UNIVERSIDADE CATÓLICA PORTUGUESA

FACULDADE DE DIREITO

ASSINATURA ELETRÓNICA E SEGURANÇA JURÍDICA ELETRÓNICA

Dissertação apresentada à Universidade Católica Portuguesa para

obtenção do grau de Doutor em Direito por

José Maria Fernandes Pires

Orientador: Professor Doutor Luis de Sousa Fábrica

Lisboa, julho de 2017

ÍNDICE

ÍNDICE DE SIGLAS UTILIZADAS 9

INTRODUÇÃO 11

1. Apresentação do tema 13
2. Objeto da investigação 15
3. Objetivo da investigação 16
4. Metodologia 17
5. Estruturação do trabalho 18
6. Obstáculos à investigação 19
7. Demonstração do interesse do trabalho 19
8. O papel da tecnologia 20
9. Agradecimentos 22

PARTE I. FUNDAMENTOS TÉCNICOS E JURÍDICOS DA ASSINATURA ELETRÓNICA 25

Capítulo I – Quadros fundamentais 27

1. Assinatura em geral: conceito e funções 27
   1.1. A função de identificação da assinatura manuscrita 28
   1.2. A função probatória da assinatura manuscrita 30
   1.3. A função de atribuição 32
2. O desafio da evolução tecnológica 32
   2.1. A digitalização da Informação 32
      2.1.1. A digitalização e o desenvolvimento da Lógica 33
         2.1.1.1. A filosofia de Leibniz 34
         2.1.1.2. A Lógica Booleana 35
      2.1.2. Digitalização, mecanização e eletrificação 36
      2.1.3. A revolução da digitalização 38
   2.2. A Internet e as redes abertas 38
   2.3. O Intercâmbio Eletrónico de Dados (EDI) 40
   2.4. As redes abertas 42
3. A insegurança jurídica dos suportes eletrónicos 43

3.1. A insegurança jurídica eletrónica anterior emergência das redes eletrónicas 43
3.2. A insegurança jurídica das redes abertas 46
3.3. Insegurança quanto aos sujeitos 47
3.4. Insegurança quanto aos documentos 49
3.5. Insegurança quanto aos sistemas 49
Capítulo II - A formação da assinatura eletrónica 53
1. A história da formação da assinatura eletrónica 53
1.1. A fase anterior às redes eletrónicas 53
1.2. O EDI e as redes fechadas 55
1.2.1. O Relatório TEDIS da Comissão Europeia 55
1.2.2. A Lei Modelo do Comércio Eletrónico (LMCE) 56
1.2.3. O papel de outras organizações internacionais 57
1.3. A fase das redes abertas 57
1.3.1. A emergência da assinatura digital 58
1.3.1.1. A lei do Utah, de 1995 60
1.3.1.2. A lei italiana de 1997 61
1.3.1.3. A lei alemã de 1997 61
1.3.1.4. A lei portuguesa de 1999 62
1.3.1.5. A lei espanhola de 1999 64
1.3.1.6. A lei inglesa de 1999 64
1.3.2. O trabalho de harmonização das organizações internacionais 65
1.3.2.1. As *Guidelines* da American Bar Association (ABA) 65
1.3.2.2. As Diretrizes sobre Política Criptográfica da OCDE 65
1.3.2.3. A diretiva europeia da assinatura eletrónica 66
1.3.2.4. A Lei Modelo da Assinatura Eletrónica (LMAE) 67
1.3.3. O Regulamento EIDAS 68
2. A criptografia como base de construção da assinatura eletrónica. 69
2.1. A criptografia de chave simétrica 71
2.2. A criptografia de chaves assimétricas ou de chave pública 72
2.2.1. O processo de criação das chaves 75
2.2.2. Demonstração da operação de encriptação e de desencriptação 77
Cap. III – O objeto da assinatura eletrónica 81

1. A formação do conceito de documento eletrónico. Os conceitos de mensagem e de registo 83
1.1. O conceito de mensagens eletrónicas da LMCE 83
1.2. O conceito de mensagem eletrónica da LMAE e da UNCUECIC 86
1.3. A generalização da utilização do conceito de documento eletrónico 86
1.4. Os documentos eletrónicos que não têm correspondência com o papel 87
1.5. A legislação da UE e a assunção do conceito de documento eletrónico 88
2. A ontologia dos documentos eletrónicos 89
3. A inteligibilidade dos documentos eletrónicos 93
4. A declaração negocial eletrónica automatizada 94

PARTE II – O PROCEDIMENTO DE ASSINATURA ELETRÓNICA ..99

Capítulo I – Os tipos de assinatura eletrónica 101
1. A Assinatura mediante digitação do nome 102
2. A Assinatura digitalizada 103
3. A autenticação por palavras-chave ou códigos secretos 105
4. Os métodos biométricos 108
5. A assinatura digital 110
5.1. A utilização da criptografia 111
5.1.1. Na vinculação de dados ao seu autor 113
5.1.2. A possibilidade de partilha livre da chave pública 114
5.1.3. A autonomização da ação do emissor e do destinatário 115
5.1.4. A função *Hash* 116
5.2. A função dos prestadores de serviços de confiança eletrónica 119
5.3. O resultado da assinatura de um documento eletrónico 121
5.4. O procedimento de verificação da assinatura eletrónica do destinatário .. 122
5.4.1. A verificação da autenticidade e da identidade 122
5.4.2. A verificação da integridade dos documentos eletrónicos. 123

Capítulo II – O conceito jurídico de assinatura eletrónica 125
1. O ponto de partida no paradigma do papel 126
2. Antecedentes do conceito de assinatura eletrónica 131
2.1. A emergência do EDI e o conceito de assinatura na LMCE 132
2.2. As limitações do regime da LMCE 133
3. O conceito de assinatura no contexto das redes abertas 135

3.1. A formação do conceito de assinatura eletrónica na LMAE e na Diretiva da UE 136
3.2. O conceito de assinatura eletrónica no Regulamento EIDAS 139
3.3. A assinatura eletrónica como um conjunto de dados 140
3.3.1. A natureza dos dados da assinatura eletrónica 141
3.3.2. A natureza da associação dos dados 142
3.3.2.1. A mera ligação de dados 142
3.3.2.2. A assinatura por associação lógica entre dados 143
3.3.2.3. A associação aos elementos da identificação 147
3.3.2.4. A abrangência da definição 147
3.4. As limitações de um conceito geral de assinatura eletrónica 148
3.5. A assinatura eletrónica qualificada 149
3.5.1. Conceito de assinatura eletrónica qualificada 150
3.5.2. Efeitos jurídicos da assinatura eletrónica qualificada 152
3.5.3. Requisitos substanciais da assinatura eletrónica qualificada 157
3.5.3.1. Requisitos substanciais da legislação da UE 163
3.5.3.1.1. Que se trate de assinatura eletrónica avançada 164
3.5.3.1.2. Que o certificado seja qualificado 166
3.5.3.1.3. Que o dispositivo de criação de assinatura seja qualificado 168
3.5.4. Requisitos formais da assinatura eletrónica qualificada 170
3.6. O conceito de assinatura na doutrina 180
3.7. O conceito de assinatura na legislação 188
Capítulo III – Funções da assinatura eletrónica 197
1. A função de identificação do titular 197
2. A função de aprovação do conteúdo das mensagens eletrónicas 200
3. A função de autenticação 205
3.1. A autenticação eletrónica nos primeiros estudos jurídicos 208
3.2. O conceito de autenticação na LMCE. 212
3.3. A autenticação e identificação nas redes abertas 218
3.4. O conceito de autenticação no Regulamento EIDAS 221
4. A função de garantia da integridade do documento 224
5. A função de não repúdio 229
5.1. A função de não repúdio na origem 231
5.2. A função de não repúdio no destino 233

6. A função de confidencialidade 238
Capítulo IV – Os certificados de assinatura eletrónica 241
1. A função dos certificados de assinatura eletrónica 242
2. O conteúdo dos certificados de assinatura eletrónica 245
3. Os tipos de certificados de assinatura eletrónica 247
4. Fiabilidade dos certificados e das assinaturas eletrónicas. Os certificados qualificados. 248
5. Revogação, suspensão e caducidade dos certificados 250
Capítulo V – Identificação eletrónica e assinatura eletrónica. O regime europeu 255
1. – Pressupostos do reconhecimento mútuo 258
2. – Sujeitos 260
3. – Fases da identificação eletrónica 262
4. – Níveis de garantia dos meios de identificação eletrónica 266
5. – Requisitos do reconhecimento mútuo pelos Estados Membros 270
5.1. – Reconhecimento facultativo 272
5.2. – Reconhecimento obrigatório 273
5.3. – Interoperabilidade 275
5.4. – Efeitos 280
Capítulo VI – A Assinatura eletrónica e os restantes serviços de confiança 283
PARTE III. CONSTRUÇÃO JURÍDICA DA ASSINATURA ELETRÓNICA 295
Capítulo I – Os princípios jurídicos da assinatura eletrónica 297
1. O princípio da inalterabilidade do direito subjacente 297
2. O princípio da equivalência funcional 298
3. O princípio da neutralidade tecnológica 307
4. O princípio da liberdade contratual 310
Capítulo II – Os sujeitos da assinatura eletrónica 315
1. Os prestadores de serviços de confiança 318
1.1. Natureza das funções de confiança 320
1.1.1. A geração e fornecimento de pares de chaves de assinatura eletrónica 324
1.1.2. A identificação dos titulares da assinatura eletrónica 326
1.2. As Infraestruturas de chaves públicas (PKI) 327
1.2.1. Organização das PKI 330

1.2.2. PKI e Estado 332
1.2.3. A supervisão e acreditação públicas. O regime da União Europeia 339
1.3. Os regimes de responsabilidade dos prestadores de serviços de certificação 347
1.3.1. Fundamentos da responsabilidade 347
1.3.2. Limites da responsabilidade 354
1.4. Reconhecimento internacional das assinaturas eletrónicas 357
1.5. O regime de reconhecimento mútuo da União Europeia 368
1.6. Os prestadores qualificados de serviços de confiança 372
2. O titular da assinatura eletrónica 375
2.1. A assinatura eletrónica de pessoas coletivas. Os selos eletrónicos. 381
2.2. A assinatura eletrónica de entidades públicas 386
2.3. A sede eletrónica 391
2.4. Responsabilidade dos titulares da assinatura eletrónica 392
3. As partes que confiam na assinatura eletrónica 397
Capítulo III – Os efeitos jurídicos da assinatura eletrónica 399
1. Documento escrito eletrónico 399
2. O carácter original dos documentos eletrónicos 406
2.1. Originalidade e autenticidade 409
2.2. Originalidade e singularidade. Os títulos transacionáveis eletrónicos 413
2.2.1. O objeto da garantia da singularidade 415
2.2.2. O instrumento de garantia da singularidade 420
3. Arquivo e conservação de documentos e comunicações eletrónicas 422
4. A admissibilidade de prova mediante documentos eletrónicos 429
4.1. Problemática 429
4.2. As soluções legislativas 436
4.3. O regime vigente em Portugal da prova por documentos eletrónicos 440
4.3.1. - O documento eletrónico como base probatória 440
4.3.2. – A eficácia probatória da assinatura eletrónica 445
4.3.2.1. – Das assinaturas eletrónicas qualificadas 446
4.3.2.1.1. – Documentos eletrónicos em forma escrita 448
4.3.2.1.2. – Documentos eletrónicos não considerados em forma escrita 451
4.3.2.2. – Das assinaturas eletrónicas não qualificadas 452
4.3.2.3. – Das convenções de autenticação eletrónica 454

4.3.3. - O documento eletrónico não assinado 455
Capítulo IV – A assinatura eletrónica na administração pública 457
1. - A assinatura e o documento eletrónico no procedimento administrativo 457
2. O efeito da assinatura eletrónica e do documento eletrónico no procedimento administrativo 466
Capítulo V – Problemas jurídicos da assinatura eletrónica 473
1. O procedimento administrativo e os serviços de confiança eletrónica 473
1.1. - O procedimento administrativo eletrónico 474
1.1.1. - O procedimento administrativo automatizado 475
1.1.2. – A programação do ato administrativo 480
1.1.2.1. – A subsunção dos factos ao programa informático 485
1.1.2.2. – A apreciação e qualificação dos elementos do procedimento 486
1.1.2.3. – A decisão final do procedimento automatizado 487
1.1.2.4. – A natureza regulamentar do programa informático 490
1.1.3. – Direitos dos interessados no procedimento eletrónico 494
1.2. O processo administrativo eletrónico 496
1.3. A assinatura eletrónica e os serviços de confiança no procedimento administrativo 502
1.4. A notificação eletrónica 506
2. Os arquivos de documentos eletrónicos 518
3. A interoperabilidade funcional 521
4. A identidade eletrónica 526
4.1. - As dificuldades adicionais da identificação eletrónica 529
4.2. – Os efeitos do regime europeu da identificação eletrónica 532
4.2.1. – No espaço da União Europeia 533
4.2.2. – No seio de cada Estado Membro 534
4.2.3. – Nas empresas privadas 536
4.3. – As limitações do regime europeu da identificação eletrónica 537
4.4. – Crítica e limitações 544
5. A entrada em vigor do Regulamento EIDAS e o regime transitório 549
5.1. – Os prestadores qualificados de serviços de confiança 549
5.2. – As assinaturas eletrónicas qualificadas 551
5.3. – Os certificados eletrónicos de assinatura eletrónica atribuídos a pessoas coletivas 552

5.4. Os dispositivos certificados de assinatura eletrónica 553
5.5. – As listas de confiança 553
5.6. – Interoperabilidade 554
5.7. – Revogação do Decreto-Lei n.º 290-D/99, de 4 de agosto 554
5.8. – Entrada em vigor do regime da identificação eletrónica 556

CONCLUSÕES 559

BIBLIOGRAFIA 583

Índice de Siglas utilizadas

ABA - American Bar Association

ADP – Automated data Process

CCC - Customs Co-operation Council

CE - Comissão Europeia

CEN – Centro Europeu de Normalização

CEA - European Insurance Committee

CEFIC - European Council of Chemical Industries Federations

CEGER - Centro de Gestão da Rede Informática do Governo

CIREDIT - Centre International de Recherches et d'Etudes du Droit de l'Informatique et des Telécommunications

CIT - International Rail Transport Committee

CMI - Comité Maritime International

CPA - Código do Procedimento Administrativo

DL – Decreto-Lei

EDI – Electrónic Data Interchange

EDICC - Electronic Data Interchange Trading Partner Agreement"

EIDAS – Regulamento Europeu Relativo à Identificação Eletrónica e aos Serviços de Confiança para as Transações Eletrónicas no Mercado Interno

ETSI - Instituto Europeu de Normas e Telecomunicações.

EUA – Estados Unidos da América

FINPRO/CMEA - Model Agreement on Transfer of Data in International Trade"

ICC - International Chamber of Commerce

IRU - International Road Transport Union

ISO - International Organization for Standardisation

JOCE - Jornal Oficial das Comunidades Europeias

LMAE – Lei Modelo da Assinatura Eletrónica

LMCE – Lei Modelo do Comércio Eletrónico

MIT - Instituto Tecnológico do Massachusetts

NZEDIA - New Zealand Electronic Data Interchange Association

OCDE – Organização para a Cooperação e o Desenvolvimento Económico

ODETTE - Organization for Data Exchange via Teletransmission in Europe

SITPROSA - Organization for Simplification of International Trade Procedures, da África do Sul

SRI - Stanford Research Institute

UNCID Rules

UNCITRAL – United Nations Commission on International Trade Law

UNCUECIC – United Nations Convention on the Use of Electronic Communications in International Contracts

UNCTADIFALPRO - Special Programme on Trade Facilitation of the United Nations Conference on Trade and Development

UNIECE - Working Party on Facilitation of International Trade Procedures on the United Nations Economic Commission for Europe

Introdução

1. Apresentação do tema

A dissertação que apresentamos de seguida tem por objeto o estudo do direito da assinatura eletrónica como instrumento fundamental de segurança jurídica dos suportes eletrónicos dos documentos e das comunicações.

Trata-se de uma disciplina jurídica jovem, que resulta da emergência da eletrónica como suporte alternativo do papel à documentação dos negócios e dos atos com relevância jurídica.

Os suportes eletrónicos são uma importante aquisição da civilização, que provavelmente terão uma importância que se aproxima do desenvolvimento da imprensa escrita por Johannes Gutenberg no século XV, no que respeita à rapidez da difusão do conhecimento, do desenvolvimento das relações jurídicas e da eficiência da atividade económica. A descoberta e o crescimento da utilização daqueles suportes é o produto da evolução do conhecimento filosófico, matemático e tecnológico e operou mediante três transformações ocorridas nas últimas décadas do século XX:

i) A digitalização da informação, dos serviços, das comunicações, dos suportes do conhecimento e da produção intelectual em geral. Todo o conhecimento humano se veicula através das infinitas combinações do

alfabeto e da escala numérica, mas os computadores operam apenas com dados, numa escala da máxima simplicidade, de apenas dois dígitos – o zero e o 1. A digitalização abriu a possibilidade de se transpor para a linguagem desses dígitos – e por isso se chama digital – toda a informação e as operações efetuadas mediante a linguagem humana. Assim nasceu a comercialização dos respetivos produtos através das redes de comunicação e se fundou o conceito de comércio eletrónico, mediante a generalização da utilização dos suportes eletrónicos na documentação e no estabelecimento das relações jurídicas. Mesmo quando se trate da transmissão de bens materiais, a generalização da digitalização veio permitir que as relações jurídicas conexas se possam desenvolver de forma digitalizada. A tecnologia da comunicação por pacotes e por fibra ótica aumentou extraordinariamente a velocidade das comunicações e a possibilidade de todos os conteúdos digitas serem transmitidos de forma praticamente instantânea;

ii) A automatização das operações internas e externas dos agentes económicos, incluindo as relações jurídicas que entre eles se estabelecem. A simplicidade com que operam os sistemas informáticos, mediante uma infinidade de combinações dos dois dígitos de base, permite a automatização e a interação entre sistemas, de forma autónoma, mediante programação. Esta automatização aumenta também a velocidade de execução das operações com relevância jurídica;

iii) O desenvolvimento da Internet como rede universal de comunicação, acessível a todos os cidadãos e empresas em todo o mundo, a custos relativamente baixos, conjugando a digitalização, a comunicação, a automatização, e a acessibilidade universal.

Estes três instrumentos, que designamos ao longo da nossa investigação como tecnologias eletrónicas, foram imediatamente adotados pelas empresas nas suas operações, dada a rapidez, economia, eficiência e eficácia que trazem ao funcionamento da economia.

Desta transformação resultou a emergência de um novo suporte de documentação das relações jurídicas, que é o suporte eletrónico, passando a existir dois

onde anteriormente existia apenas o papel. Em muito casos elas permitem a substituição do papel como suporte documental.

A nossa investigação centra-se na assinatura eletrónica como o instrumento jurídico construído por juristas, matemáticos, informáticos, agentes económicos e outros, que confere aos suportes eletrónicos idoneidade para servirem de base à documentação das relações jurídicas. Analisamos o conhecimento jurídico produzido, o seu contexto e o corpo normativo já alcançado, para depois perspetivarmos a evolução futura.

2. Objeto da investigação

As normas jurídicas que regulam os suportes documentais sedimentaram-se no paradigma do papel. O papel é um objeto físico, fáctico, sensível, imutável, um instrumento de estabilidade e um veículo fiável de registo e de transmissão. Um documento suportado em papel beneficia de todos esses atributos, que lhe conferem segurança e estabilidade jurídicas.

O suporte eletrónico não possui a robustez do papel como instrumento de segurança jurídica dos documentos. Os suportes eletrónicos são construções que se erigem de cada vez que ordenamos a um computador que as disponibilize para nossa consulta. O documento que vemos num ecrã de computador é uma construção efetuada em cada momento em que o abrimos, efetuada mediante a conversão de um conjunto de dados numa aparência que seja legível pelo entendimento humano. O que é inteligível para o Homem não é operável pelos sistemas informáticos e o que é suscetível de ser processado por estes, as sequências digitais binárias, não é compreensível pelo intelecto humano, sem que o computador o converta para a nossa linguagem. Uma letra do alfabeto no papel é essa mesma letra, mas nos suportes eletrónicos, apesar de se apresentar como uma letra, ela é uma sequência de dígitos de zero e um.

Os documentos em papel são objetos unos e estáveis, que podemos observar no estado exato em que foram gerados. E a possibilidade dessa constatação depende apenas dos nossos meios, dos nossos sentidos e do nosso entendimento. Os suportes eletrónicos não possuem esses atributos e a insegurança na sua utilização, além de ser intrínseca é quase sempre impossível de verificar com os nossos próprios meios.

Do mesmo modo as relações jurídicas estabelecidas por meios eletrónicos são mediadas por máquinas que se interpõem entre os sujeitos, sendo insegura a identificação e a vinculação, porque é incerta a identidade de quem opera com cada máquina e se perde a proximidade existencial que serve de contexto à declaração negocial e à expressão da vontade.

O objeto da nossa investigação é o estudo da idoneidade dos suportes e das comunicações eletrónicos para documentarem as relações jurídicas. A questão da sua idoneidade jurídica, da sua fiabilidade.

Trata-se de uma problemática essencial para a regulação das relações jurídicas estabelecidas mediante a utilização dos instrumentos e das comunicações eletrónicos.

A nossa investigação analisa como se formou a ordem jurídica dos documentos eletrónicos e como foi possível conferir segurança jurídica a suportes de informação estruturalmente contingentes, inseguros e facilmente manipuláveis e permeáveis à fraude. Quando o suporte não é físico nem estático, mas constituído a cada apresentação e facilmente alterável, a segurança jurídica não se pode ancorar no suporte, mas na própria informação que constitui o documento. É esse desafio de construir um sistema de vinculação assente nos dados informacionais dos documentos eletrónicos, que conferem uma segurança jurídica equivalente à dos documentos em papel, que constitui o objeto fundamental da nossa investigação.

3. Objetivo da investigação

A assinatura eletrónica é o principal instrumento de juridificação dos suportes e das comunicações eletrónicas, em especial através da Internet, e a sua criação e desenvolvimento dão resposta a uma necessidade de segurança jurídica dos agentes económicos, que é indispensável à generalização da utilização das tecnologias eletrónicas nas relações jurídicas.

O objetivo do nosso trabalho é contribuir para a consolidação desta ainda jovem disciplina do direito, analisando de forma sistematizada o corpo de conceitos e de metodologias já sedimentados, identificando domínios problemáticos que necessitam de estudo e de investigação e tentando perscrutar caminhos de futuro, contribuindo, de forma naturalmente modesta mas bem-intencionada, para a sua evolução.

Pretendemos contribuir para o desenvolvimento da reflexão jurídica acerca da confiança na utilização dos meios eletrónicos.

4. Metodologia

Iniciámos o nosso trabalho com o estudo das três transformações que estão na base dos suportes eletrónicos e do conhecimento que está na sua origem. Investigámos também o contexto histórico em que emergiram esses suportes e em que se expandiu a sua utilização pela atividade económica.

Estudámos depois as necessidades de segurança jurídica na utilização desses suportes e a adequação, ou não, das soluções jurídicas aplicáveis ao papel, para os documentos eletrónicos. Refletimos acerca das soluções que o conhecimento jurídico do paradigma do papel poderia aportar para a resolução do problema da insegurança estrutural dos suportes eletrónicos.

Estudámos cuidadosamente, como era nosso dever, o impressionante conhecimento jurídico produzido a nível internacional, em especial pela UNCITRAL, mas também por um vasto conjunto de organizações internacionais, desde a década de 1960 até a atualidade. Dedicámos especial cuidado à legislação pioneira, produzida a nível internacional, em primeiro lugar a LMCE e a LMAE, e de outros documentos do mesmo nível, bem como a chamada legislação precoce, com especial referência para a lei do estado do Utah, nos EUA sobre assinatura eletrónica e, onde se incluem também as leis portuguesa, alemã e espanhola, todas de 1999. Estudámos depois a legislação consolidada da UE, bem como as soluções legislativas posteriores às soluções tecnológicas mais avançadas de assinatura.

Tal como na assinatura manuscrita, existem vários tipos de assinatura eletrónica, assentes em tecnologias diferentes, que foram surgindo como resposta às necessidades crescentes de segurança jurídica na utilização dos meios eletrónicos que os agentes económicos foram postulando. Ao mesmo tempo evoluiu também o quadro de exigências legais de segurança jurídica e descobriram-se novos conceitos como o de identidade eletrónica, de assinatura digital, de sede eletrónica, de marcação temporal eletrónica e outros. Esses novos conceitos são construções do conhecimento humano, que recorrem a formulações gnoseológicas muitas vezes ancestrais, e multidisciplinares, incluindo a filosofia, a lógica, a matemática e a ciência jurídica.

Embora não exista uma produção doutrinária nem jurisprudencial diversificada nesta matéria, procurámos também analisar cuidadosamente aquela que existe e refletir o seu contributo no nosso trabalho.

Concluímos a fase de investigação no final do ano de 2014, pelo que todas as referências que utilizamos se reportam a esse limite temporal, salvo escassas exceções.

Numa fase avançada da nossa investigação tivemos a oportunidade de conceber e coordenar o trabalho de implementação do sistema de assinatura eletrónica num importante serviço da administração púbica portuguesa, a par de um sistema de notificações eletrónicas, que muito enriqueceu o nosso trabalho de investigação. Coordenámos também a conceção e implementação de muitos projetos de utilização de tecnologias eletrónicas em procedimentos administrativos na função tributária.

5. Estruturação do trabalho

Iniciamos o nosso trabalho com a definição do conceito geral de assinatura e, em especial de assinatura eletrónica, tentando assim delimitar o objeto da nossa investigação.

Dedicamo-nos depois a expor o problema da segurança jurídica que advém da utilização da eletrónica como suporte dos documentos com relevância jurídica. Os documentos eletrónicos possuem uma estrutura e uma ontologia distinta dos documentos em papel, que os podem tornar menos eficazes do que o papel para a função de documentação das operações jurídicas. A insegurança que daí resulta é multifacetada na sua problematicidade.

A ambição da expansão da utilização dos meios eletrónicos pelos agentes económicos forçou a procura de soluções capazes de superar essa insegurança, sendo que essas soluções evoluíram rapidamente, como expomos no capítulo referente à formação da assinatura eletrónica, onde incluímos também o estudo das formulações matemáticas que estão na origem dessas soluções.

Dedicamos a Parte II ao estudo do procedimento da assinatura eletrónica, enunciando os tipos de assinatura eletrónica disponíveis, definindo o conceito de assinatura eletrónica e elencando as funções que lhe são próprias.

Na Parte III, relativa à construção da assinatura eletrónica, analisamos a sistematização dos princípios jurídicos que enformam o respetivo regime jurídico, os

sujeitos da assinatura eletrónica e os respetivos efeitos, dedicando ainda um capítulo ao estudo da sua utilização e efeitos no procedimento administrativo.

Terminamos com as conclusões, onde elencamos os domínios em que existe ainda necessidade de aperfeiçoamento jurídico. A construção do direito da assinatura eletrónica está ainda no seu início, existindo ainda um conjunto de fatores de insegurança que necessitam de produção legislativa e doutrinária.

6. Obstáculos à investigação

No decurso da nossa investigação deparámo-nos com algumas dificuldades, em especial a escassez de desenvolvimentos doutrinais desta disciplina do direito em Portugal, e da sua escassa sistematização dogmática a nível internacional. Existe muita literatura publicada acerca da chamada revolução tecnológica, incluindo de natureza jurídica, mas muitas vezes eivada de excesso de voluntarismo que lhe retira rigor científico. Merece, porém, realce, a existência de um relevante espólio documental dos trabalhos de conceção legislativa que decorreram na instância que mais contribuiu para o desenvolvimento desta disciplina, que foi a UNCITRAL, e que em muito nos iluminou o caminho.[1]

Outra dificuldade é o elevado teor técnico da fenomenologia eletrónica, sobre o qual se erige a respetiva disciplina jurídica, e a necessidade de se associar o conhecimento das necessidades de segurança jurídica, aos dispositivos tecnológicos que permitem a sua satisfação. A utilização dos meios eletrónicos é uma exigência crescente da atividade económica, mas ela só é possível se existirem instrumentos técnicos e legislativos de segurança jurídica. A necessidade desta é tão importante como a necessidade da tecnologia. Procuramos na nossa investigação associar os domínios do conhecimento jurídico, matemático e tecnológico, para podermos compreender e analisar toda a fenomenologia do nosso tema.

7. Demonstração do interesse do trabalho

[1] As referências bibliográficas que fazemos aos documentos da UNCITRAL e da União Europeia ao longo do nosso trabalho são identificadas pelo número de documento, sendo a referenciação completada na Bibliografai.

Vivemos um contexto de transição entre o papel e o eletrónico como suporte documental do tráfego jurídico, o que poderá conduzir a que em domínios tão importantes como as atividades económicas de prestações de serviços e em vastos sectores das transmissões de bens venha a ocorrer uma completa desmaterialização das operações com relevância jurídica. Esse fenómeno terá também especial impacto no procedimento administrativo. Por essa razão dedicamos também um especial enfoque à utilização das tecnologias eletrónicas nas relações jurídicas administrativas.

Os suportes eletrónicos têm sobre o papel a vantagem da suscetibilidade de serem objeto de tratamento automatizado, bem como a rapidez de tratamento e a economia que proporcionam às partes envolvidas, tanto em termos de tempo como de meios financeiros e de comodidade. Daí o seu sucesso.

As tecnologias eletrónicas, sendo mediadas por máquinas que se interpõem nas relações pessoais, também aproximam, porque tornam as comunicações imediatas e multifuncionais. Por essa razão, a presença eletrónica e a ação humana através destes meios será cada vez maior, o que coloca a questão da identidade eletrónica e do conhecimento pessoal através destes meios.

Por outro lado a automatização dos procedimentos levanta o problema da documentação, dado que os sistemas informáticos operam apenas com dados binários, sendo que a documentação é essencial para o controlo da legalidade dos atos.

A automatização coloca ainda a questão do controlo das regras de funcionamento desses sistemas e, sendo elas aplicáveis a uma elevada quantidade de atos e procedimentos, possuem natureza quase normativa, exigindo um controlo correspondente, em especial quando se trate de procedimentos administrativos automatizados.

8. O papel da tecnologia

O entusiasmo académico com que nos dedicamos ao tema do nosso trabalho não nos permite classificar o resultado das três transformações que anteriormente enunciámos, como uma revolução ou como a emergência de um mundo novo, como muitas vezes se invoca.

Trata-se apenas de três novas técnicas inventadas pelo Homem, como tantas outras que anteriormente inventou, provavelmente com maior impacto transformador,

como foi o caso da invenção do papel, da escrita ou da imprensa. A técnica é sempre instrumental do Homem, mas é também essencial à sua existência. É instrumental porque facilita a sua ação e o Homem como ser ético realiza-se na ação. A técnica permite que o braço humano, a voz, a expressão sejam mais fortes, mais eficientes, mais rápidas, mais expressivas, que possam ir mais longe. Mas a técnica só exprime o que é essencialmente humano, portador de sentido e expressão de intencionalidade. A técnica é instrumento do Ser, mas não é o Ser, nem a sua expressão.[2]

Mas a técnica é essencial ao Homem, em face da sua natureza de ser eticizado e expressivo, de ser em ação. A humanidade é linguagem, expressividade e ação, e essa externalização exige instrumentos, que designamos como técnicas de comunicação e de conservação que têm evoluído ao longo da história, a par e como resultado da evolução do conhecimento humano e da cultura.

A tecnologia nunca substituirá as mulheres e os homens na sua essência e na sua Humanidade, porque é apenas instrumento e não essência, e essa foi uma importante conclusão que retiramos no final do percurso metodológico que empreendemos para este nosso trabalho. Não há técnica sem humanidade e não há humanidade sem cultura, sem conhecimento, sem direito.

As tecnologias eletrónicas proporcionam apenas uma maior rapidez, economia, proximidade e expressividade na ação humana.

Numa das suas mais notáveis lições, que dedicou ao tema *"A origem da Obra de Arte*", Heidegger contempla o quadro de Van Gogh intitulado *"Natureza Morta Com um Par de Sapatos Velhos*" e, depois de assinalar aos sapatos a sua natureza de utensílios, dedica-se a procurar a sua essência, dissertando acerca da essência dos utensílios, do que é "útil". Para o filósofo do Ser, essa essência está na sua fiabilidade, na sua capacidade de cumprirem a sua função. É esse o *"ser do útil"*. É essa fiabilidade e a confiança que dela emerge que, segundo Heidegger, permite à camponesa que terá utilizado esses sapatos envelhecidos pelo seu trabalho e esforço, entregar-se ao seu trabalho sobre a terra, sem se preocupar com a importância que os sapatos têm para esse fim. "*Mediante a fiabilidade a camponesa pode abandonar-se ao apelo mudo da terra,*

[2] Como afirma Urdanoz, na filosofia de Heidegger, o filósofo que mais teorizou a importância da técnica na Filosofia, *"A descrição fenomenológica do mundo parte da análise do Dasein na sua existência quotidiana (...) O Homem é um ser ativo perante as "coisas", que já os gregos designavam de 'pragmata'. A primeira preocupação do 'Dasein' perante as coisas não é a do conhecimento puro delas, mas a sua manipulação, a sua utilização e o seu emprego"*. E mais adiante, *"O homem não considera as coisas em si mesmas, mas enquanto instrumentos úteis para a sua actividade, para o desenvolvimento das suas possibilidades"*. Urdanoz, T. (1978). *História de la Filosofia, vol. VI*. Biblioteca de Autores Cristianos. Madrid., pág.s 522 e 523.

e sentir-se confiante no seu mundo em virtude da fiabilidade do útil".[3] É esta fiabilidade que está em causa relativamente às tecnologias eletrónicas, como suporte da documentação das relações jurídicas.

Numa conferência realizada em 1953 na Academia Bávara de Belas Artes, Heidegger dedica-se especificamente à tecnologia, interrogando-se acerca da sua essência, definindo-a como *"instrumento ao serviço do ser humano, um meio para a realização de fins"*.[4] A sua essência seria a da *"ex-tração"* ou da produção, consistindo num *"trazer algo do oculto para o desoculto"*.[5] E nessa medida a técnica é um instrumento de revelação do Ser e de realização do Homem.[6]

É na procura da fiabilidade dos documentos eletrónicos e da sua idoneidade para os suportes eletrónicos serem fundamento de validade e eficácia jurídica dos respetivos documentos que a assinatura eletrónica desempenha o papel de instrumento útil e portadora de juridicidade.

9. Agradecimentos

No lugar mais elevado da satisfação que o trabalho intelectual nos proporciona está a gratidão por aqueles que nos ofereceram a sua generosidade, o seu conhecimento, a sua sapiência, enfim, a sua humanidade. Em primeiro lugar agradeço ao Senhor Professor Doutor Luís Fábrica, que me deu tudo isso com exigência e rigor, sem nada me pedir em troca, a não ser a obra como resultado do trabalho árduo. Mas também a todos as Senhoras Professoras e os Senhores Professores da Universidade Católica Portuguesa que, tanto na fase do doutoramento como do mestrado, da pós-graduação e da licenciatura, me ensinaram os fundamentos da Justiça e do Direito e a utilizar o método jurídico na vida de todos os dias.

Devo também infinita gratidão a essa comunidade académica de excelência que é a Universidade Católica Portuguesa, onde me sinto sempre iluminado por uma cultura

[3] Claros, Luis Fernando Moreno; "Martin Heidegger", ADAF Ensayo, Madrid, 2002, pág. 337.
[4] *Ibidem*, pág. 377.
[5] *Ibidem, idem*.
[6] Do mesmo modo quando escrevemos uma carta, o que para nós é mais importante é o papel e a caneta, porque são esses os instrumentos que nos possibilitam realizar o nosso fim. Porém, logo que concluída a escrita, o que passa a ser decisivo são o envelope e o selo que nos permite enviá-la. O selo passa a ser o instrumento mais útil naquele momento. Os utensílios têm importância em função das necessidades que deles temos. Se não necessitamos deles não servem para nada. Se necessitamos são fundamentais. *"Nesta caso o selo é visto como algo impertinente, que obstaculiza e obstrói a acção do 'Dasein', o qual se encontra sempre imerso no útil"*. *Ibidem*, pág. 175.

de serviço aos outros e aos valores, de humildade na procura do conhecimento, de disciplina e comunhão, tanto na Escola do Porto, onde me licenciei em Direito, como de Lisboa, onde continuei os estudos.

Devo também gratidão ao Senhor Dr. Amaral Tomás, ao Senhor Dr. Paulo Macedo e ao Senhor Professor Doutor José António de Azevedo Pereira, que me concederam equiparação a bolseiro no país para desenvolver a minha investigação e me desafiaram para aplicar muito do conhecimento adquirido em projetos relevantes da administração tributária portuguesa. Ao Senhor Dr. António Nunes dos Reis devo também o incentivo e a amizade genuína, desinteressada e de todos os dias. Ao Senhor Professor Doutor Elísio Brandão agradeço o incentivo, a amizade e a serenidade do trabalho dos sábios que também me orientou nos dias de nosso trabalho. Agradeço também ao Dr. João Pedro Santos e aos meus amigos e colegas do Centro de Estudos Fiscais o apoio generoso que me deram.

Às minhas filhas, Inês e Sofia, estarei sempre grato pela sua infinita compreensão da importância das longas horas de silêncio e de estudo e do valor do trabalho, bem como pelo ânimo que sempre me deram. Elas são duas importantes luzes no meu caminho. À Graciosa, minha mulher, agradeço a ajuda permanente e sem falhas, a compreensão e o carinho e o caminho, a retaguarda e a força tranquila e sábia que sempre me transmitiu. Aos meus Pais agradeço para sempre o valor do trabalho e do esforço que me souberam transmitir com tranquilidade e exemplo.

Parte I.

Fundamentos técnicos e jurídicos da assinatura eletrónica

Capítulo I – Quadros fundamentais

1. Assinatura em geral: conceito e funções

A metodologia para o estudo da fenomenologia jurídica das assinaturas eletrónicas deve partir da análise das funções essenciais das assinaturas manuscritas. Foi a partir do diagnóstico dessas funções que se construiu o seu regime jurídico de acordo com o princípio da equivalência funcional. E essas funções fundamentais são duas:

i) A identificação de uma pessoa, aquela que criou a assinatura com a sua escrita manual;

ii) A vinculação dessa pessoa a um documento. Essa vinculação pode resultar da circunstância de essa pessoa ser o seu autor ou de subscrever o seu conteúdo. Essa vinculação é a consequência jurídica do facto de a assinatura provar a participação pessoal do autor ou subscritor no ato de assinatura do documento.[7] [8]

[7] Nos trabalhos preparatórios da elaboração da LMCE, identificaram-se ainda funções acessórias da assinatura manuscrita: *"To provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document"*. "A/CN.9/WG.IV/WP.71", par. 12. A

Nas relações pessoais e nos atos assinados mediante a presença física da pessoa que assina, a estrutura conceptual do ato de assinatura é intuitiva e aparentemente composta de um só ato mas, na verdade, essa estrutura é múltipla.

Uma assinatura manuscrita é apenas uma manifestação exteriorizada de um acontecimento que é o ato de assinar, e este ato corresponde a uma vontade de subscrever, de assumir um conteúdo informacional como seu. Essa assinatura é um instrumento que revela um acontecimento que funda uma vinculação de uma pessoa a um documento. Mas uma assinatura é uma entidade autónoma do documento do qual consta. Um instrumento transitivo entre a pessoa e o documento, no qual está incorporada. Trata-se de um instrumento, com uma função de vinculação da pessoa ao documento que dela se autonomizou. A assinatura coloca-se metodologicamente entre o autor e o documento e conexiona-os. Essa vinculação pressupõe mais duas vinculações prévias, que acrescem à função de identificação:

i) A vinculação entre uma pessoa e a sua assinatura;

ii) A vinculação da assinatura ao documento.

Normalmente estes três elementos da estrutura de uma assinatura são intuitivos, nos casos em que as partes nos negócios se conhecem, mas quando assim não é, é necessária a sua comprovação. E essa comprovação compõe-se de um conjunto de atos que é necessário praticar.

Seguindo a síntese da UNCITRAL, as três funções clássicas de uma assinatura em papel são a função identificação, a função probatória e a função atribuição, que analisamos de seguida.[9]

1.1. A função de identificação da assinatura manuscrita

definição das funções essenciais perdurou pacificamente nos trabalhos da UNCITRAL, incluindo na elaboração da UNCUECIC. "A/CN.9/608/Add.2", par. 23.

[8] São ainda associadas à assinatura manual em papel outras funções, nomeadamente a de certificar a vontade da pessoa, de i) se vincular ao conteúdo do documento, de ii) assumir a autoria de um texto, de iv) subscrever um texto cuja autoria é de outrem, de v) demonstrar a participação pessoal no ato de assinatura, em determinado local e data. "A/CN.9/608/Add.2", par. 23. Do mesmo modo, "Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)", par. 53.

[9] Essas funções são enunciadas nos documentos relativos aos trabalhos de elaboração da LMCE, nos seguintes termos: *"Signatures, in turn, perform three main functions in the paper-based environment: signatures permit to identify the signatory (identification function); signatures provide certainty as to the personal involvement of that person in the act of signing (evidentiary function); and signatures associate the signatory with the content of a document (attribution function)"*. "A/CN.9/630, annex", par. 7.

Uma assinatura é um instrumento material e objetivo, que por si só não tem valor intrínseco se não estiver associada a outros referenciais que lhe confiram valor jurídico. Ela é uma entidade relacional, que não tem uma ontologia jurídica própria e autónoma.[10] O primeiro referencial a que a assinatura deve estar conexionada é a identidade de quem assina. A assinatura é sempre um sinal de uma pessoa e não existe juridicamente se essa pessoa não for identificada. Sendo um instrumento de subjetivação de um documento, não é concebível a sua existência jurídica sem o sujeito. Por essa razão, o conhecimento da identidade da pessoa que assina é a primeira função da assinatura.

Mas essa determinação é uma função que excede a assinatura e nem sequer é própria dela, porque só tem o poder de revelar a identidade de quem assina, por reporte a outros instrumentos, que são aqueles que são próprios da identificação.[11]

A função de identificação cabe às entidades competentes, através do registo e da identificação civil, assegurando a assinatura essa determinação por reporte para os respetivos elementos, produzidos por aquelas entidades. Também aqui a assinatura é um instrumento transitivo, relacional, um símbolo que reporta a um significado.

A função de identificação que a assinatura manuscrita desempenha, perante terceiros, só pode ser garantida mediante:

i) A existência de uma entidade com competência, que emita um documento de identificação que esteja associado exclusivamente a uma pessoa;

ii) A existência de um documento de identificação da pessoa que assina, que prove a sua identidade;

iii) A observação desse documento de identificação;

iv) O confronto entre os elementos do documento de identificação e os traços físicos da pessoa, nomeadamente a fotografia, a assinatura e as impressões digitais.

É mediante a verificação desses elementos que os destinatários dos documentos podem adquirir segurança acerca dessa vinculação do seu autor.

---

[10] Como se refere nos documentos da UNCITRAL, *"Regardless of the particular legal tradition, a signature, with very few exceptions, is not self-standing. Its legal effect will depend on the link between the signature and the person to whom the signature is attributable"*. "A/CN.9/630", annex, par. 9.

[11] Este é um ponto de partida essencial na compreensão dos pressupostos da assinatura eletrónica. "*Furthermore, the authority to intervene in a transaction and the actual identity of the person in question, while important elements to ensure the authenticity of a document or signature, are neither fully demonstrated by the signature alone, nor sufficient assurance of the authenticity of the documents or of the signature"*. "A/CN.9/630", annex, par. 8.

Essa verificação pode fazer-se instantaneamente, quando existe um conhecimento pessoal entre as partes, mas envolve sempre o conhecimento dos passos antes enunciados. Porém, na relação jurídica emergente da assinatura de um documento intervêm sempre, de forma direta ou indireta, as entidades competentes para a identificação civil. Quando se pretende a máxima segurança no efeito vinculativo dos documentos, podem ter que intervir quatro sujeitos distintos – a pessoa que assina, a entidade que emitiu o documento de identificação, a entidade que autenticou a assinatura e o destinatário do documento assinado.

1.2. A função probatória da assinatura manuscrita

A assinatura é um instrumento de prova de participação direta e pessoal da pessoa que ela própria identifica, no ato de assinar. A prova dessa participação é o instrumento de vinculação jurídica da pessoa ao documento.[12] Mas essa prova não é uniforme na sua eficácia jurídica, dado que a assinatura manuscrita é um instrumento estruturalmente inseguro, tanto no que respeita à determinação da identidade do assinante como à prova da sua participação no ato de assinatura, como ainda quanto às possibilidades da sua falsificação e do conteúdo dos documentos assinados.

É essa insegurança fundamental que está na base das exigências das partes e da própria lei, nomeadamente de certificação por entidades terceiras que confiram maior confiança, como são os casos da assinatura perante testemunhas, ou da intervenção de notários, para os casos das assinaturas reconhecidas e, no nível mais elevado de certificação, para as assinaturas perante notários. Na atividade comercial, e também na atividade administrativa, é frequente a utilização de carimbos e de selos como forma de conferir segurança acrescida às assinaturas. Na atividade administrativa a assinatura das entidades com competência para a prática dos atos é também frequentemente acompanhada do selo dessa entidade.

[12] Como escreve Bazin, no paradigma do papel, a assinatura é o instrumento físico de ligação entre o papel e o sinal gráfico que a revela. E como foi escrita manualmente pelo seu autor, revela também esse ato físico da mão do autor, sendo ele que o vincula. *"In the physical world, the power of the signature is the physical link between the paper and the graphic sign put on the paper"*. Bazin, P. (2008). An Outline of the French Law on Digital Evidence. Digital Evidence and Electronic Signature Law Review. Vol 5, pág. 180.

Quando recebemos um documento assinado por uma pessoa com quem queremos estabelecer um vínculo jurídico, adotamos comportamentos diferentes, conforme conheçamos essa pessoa melhor ou pior:

i) Se conhecemos a sua identidade e a sua assinatura, consideramos, de forma quase intuitiva, que essa pessoa está juridicamente vinculada ao documento por si assinado;

ii) Se não conhecermos a pessoa tão bem, solicitamos que nos envie uma cópia do seu documento de identificação, para conferirmos o seu nome e a sua assinatura e verificarmos se a assinatura o vincula adequadamente;

iii) Se pretendermos obter um nível de segurança maior, solicitamos que assine o documento na nossa presença e pedimos o seu documento de identificação para conferirmos os mesmos dados;

iv) Se não conhecemos o autor do documento e pretendemos obter maior segurança no que respeita à sua vinculação jurídica ao conteúdo do documento, solicitamos que a sua assinatura no documento seja reconhecida por um notário;

v) Se pretendermos alcançar um nível de segurança mais elevado, solicitamos à nossa contraparte que autentique a sua assinatura, efetuando-a presencialmente num notário, e que este a autentique.

A eficácia da assinatura como instrumento de vinculação não é uniforme, sendo que existem vários tipos de assinatura manuscrita. Nas assinaturas por chancela o grau de eficácia é baixo e será mais elevado no caso das assinaturas reconhecidas por notário, e ainda mais elevado nas assinaturas efetuadas perante o notário.[13]

É o grau de eficácia da assinatura que confere aos agentes maior ou menor segurança jurídica. Em determinados negócios jurídicos, a lei exige um grau de eficácia probatória elevada, como são, por exemplo, os casos em que a lei exige a intervenção de notário. A função notarial traduz-se na emissão de uma declaração com a eficácia de fazer fé pública, de confirmação da participação do assinante no ato de assinatura. Nos casos de reconhecimento presencial da assinatura, o que a entidade notarial certifica é a

[13] Como já anteriormente referimos, o Código do Notariado distingue o reconhecimento presencial do que é feito por semelhança, sendo, naturalmente, o primeiro mais seguro (artigo 153.º do Código do Notariado).

participação pessoal e direta do titular no ato da assinatura. É essa certificação que confere ao ato uma eficácia probatória acrescida.

A função do notário envolve a emissão de duas declarações, sendo a primeira a de que efetuou a identificação da pessoa e a segunda a declaração de que a assinatura aposta no documento é a assinatura que corresponde àquela pessoa. Nos casos em que o reconhecimento é presencial, o notário declara ainda ter presenciado o ato da assinatura.

1.3. A função de atribuição

A função de atribuição do documento ao autor é uma consequência jurídica das duas anteriores funções, e consiste no vínculo que delas resulta, de uma pessoa a um documento. Embora seja uma função derivada das duas anteriores, ela representa a finalidade jurídica da função da assinatura.

A eficácia desta função depende sempre da força vinculativa da assinatura utilizada, mas ela envolve sempre a verificação da assinatura, a constatação da vinculação entre a pessoa e a assinatura e, por fim, a confirmação da vinculação entre a assinatura e o documento assinado. Só depois de terem sido efetuados estes três passos é que se pode estabelecer a vinculação entre a pessoa e o documento, atribuindo àquela os efeitos jurídicos deste.

2. O desafio da evolução tecnológica

A assinatura eletrónica emergiu como uma necessidade, em resultado da utilização dos suportes eletrónicos na documentação dos atos jurídicos. E essa utilização resultou da emergência dos suportes eletrónicos na documentação das relações jurídicas, a par do papel.

As tecnologias eletrónicas são um produto da evolução do conhecimento humano e todas as suas componentes são tributárias da sua sedimentação secular, nomeadamente nos domínios da filosofia e da matemática.

2.1. A digitalização da Informação

As tecnologias eletrónicas assentam na digitalização da informação. Os sistemas informáticos operam com o código binário, que assenta no tratamento de unidades mínimas de informação. A unidade mínima de informação na linguagem informática é o *bit*, e este corresponde a um conteúdo semântico muito simples. Um *bit* corresponde, na linguagem humana, a uma resposta "sim" ou "não", a determinado impulso. No domínio eletrónico o sim representa um ponto determinado em que ocorre passagem de energia e o não representa o impedimento dessa passagem de energia. Na programação informática o sim é representado pelo dígito 1 e o não pelo dígito zero. O código binário combina essas unidades mínimas digitais, de zero e 1 e é sobre esta escala binária simples que assenta toda a construção das bases de dados informáticas.

Toda a informação contida nos suportes eletrónicos reconduz-se, em última análise, a milhões de combinações daqueles dígitos, também designados de *bites*. A cópia de um texto em papel para um suporte eletrónico, que designamos de digitalização, consiste na sua redução a sequências de dígitos 1 e zero. A linguagem digital, que é utilizada nos sistemas informáticos, reduz toda a linguagem humana a combinações destes dois dígitos, correspondentes a dois impulsos elétricos contrários, ao contrário da linguagem humana, que funciona com base num sistema algébrico decimal (nos países ocidentais) e num alfabeto.[14]

Em 1982 Simon Nora e Alain Minc publicaram a obra *"La Informatization de la Societé"*, onde *"anunciam pela primeira vez um processo de digitalização progressiva de toda a informação"*.[15] O processo de digitalização corresponde à conversão de toda a informação contida em vários suportes (papel, filmes, gravações, imagens), na linguagem binária dos computadores. Esta obra é um importante marco histórico no caminho para a expansão da utilização dos suportes eletrónicos, porque vem revelar a capacidade de esses suportes gravarem, guardarem e transmitirem toda a informação e o conhecimento, configurando-se como a primeira alternativa ao papel.

2.1.1. A digitalização e o desenvolvimento da Lógica

[14] Esta é a estrutura básica de funcionamento dos computadores, que é muito simples. *"Computers are actually among the simplest devices that we have ever developed, doing jus tone thing: Tey allow a small electric charge to be passed from one storage cell to another"*. Barret, N. (2006). *The Binary Revolution – The history and Development of the Computer*. Weidenfeld & Nicolson. London, pág.61.

[15] Rodriguez-Margariños, F.G. (2008). *La Administración de Justicia Digitalizada. Una Necesidad Inaplazable*. Ediciones Experiencia. Barcelona., pág. 26.

O conhecimento que permitiu a digitalização da informação radica, na sua origem, na lógica aristotélica, mas em especial da filosofia de Leibniz, o fundador da Lógica Matemática.

2.1.1.1. A filosofia de Leibniz

Gottfried Wilhelm Leibniz (1646-1716) construiu um sistema filosófico assente no princípio de que todas as formulações lógicas do raciocínio humano se podem reconduzir a formulações matemáticas.[16] A aplicação do método matemático ao domínio dos conceitos e do discurso argumentativo, ou seja, da Lógica, constitui o fundamento daquela que viria a ficar conhecida na história da filosofia como a Lógica Matemática.

Para Leibniz só existem dois tipos de conceitos, os simples e os compostos, sendo que estes últimos podem ser sempre decompostos em conceitos simples. O número de conceitos simples seria muito pequeno e poderiam ser representados por um símbolo ou uma palavra, tal como na álgebra. Os conceitos simples deveriam combinar-se por diversas formas, sempre segundo as regras da matemática, podendo assim formar-se vários conceitos compostos, tornando o discurso científico universal. Este procedimento permitiria, segundo Leibniz, a unificação de todas as ciências sociais ou humanas, sendo essa a grande ambição do sistema filosófico por si construído.[17]

A matemática tornar-se-ia a base de todas as ciências, das quais seriam eliminados o erro e as disputas, pois que o método matemático é irrefutável. Tal como a *"Álgebra, que permite realizar todas as operações com um número reduzido de símbolos"*[18], todo o raciocínio lógico seria um caminho seguro para a verdade e para o conhecimento irrefutável. O raciocínio lógico tem a mesma estrutura e finalidade do cálculo matemático e é, em última análise, uma forma de cálculo, porque se trata de uma combinação de conceitos. Assim, tal como uma fórmula matemática conduz a um

[16] A aplicação do método matemático à Lógica e a todas as expressões do raciocínio humano que constitui um dos vértices da filosofia de Leibniz, não é nova na história da Filosofia. Já os filósofos pitagóricos anteriores a Parménides entendiam que *"os números são as causas da realidade das outras coisas",* como ensina Aristóteles na sua Metafísica, acrescentando que *"Os Pitagóricos, como lhe chamam, dedicavam-se à matemática, foram os primeiro a fazer progredir o seu estudo, e, por terem sido educados nela, pensaram que os princípios desta eram os princípios de todas as coisas. Visto que, de entre estes princípios, os números são por natureza os primeiros … eles supunham que os elementos dos números eram os elementos de todas as coisas."* . *Apud* Kirk, G. S., Raven, J. E. (1979). *Os Filósofos Pré-Socráticos*, Fundação Calouste Gulbenkian. Lisboa., pág.s 246 e 247.

[17] Fraile, G; (1978). *Historia de la Filosofía, vol. III – Del Humanismo a la Ilustración*. Biblioteca de Autores Cristianos, Madrid., pág. 660.

[18] Fraile, G; (1978). Op. Cit., pag. 662.

resultado sempre certo, também a raciocínio lógico conduz a uma conclusão, que deve ser sempre certa e correspondente à verdade.

Leibniz tenta construir uma espécie de *"alfabeto do pensamento"*[19] em que a cada conceito simples corresponda um símbolo, da mesma forma que na aritmética cada símbolo representa uma grandeza. O raciocínio, a argumentação e o discurso seriam apenas combinações de conceitos simples, representáveis por símbolos e verdadeiras formas de cálculo, como na matemática. Leibniz pretendia alcançar uma linguagem universal para as ciências, em que os raciocínios lógicos seriam proposições assentes em cálculos e, por isso, facilmente demonstráveis.

2.1.1.2. A Lógica Booleana

A lógica matemática de Leibniz seria desenvolvida por Gergonne (*"Os juízos ou conclusões alcançam-se com palavras, exatamente da forma que na Álgebra os cálculos se efetuam com números"*[20]) e Boole. Este último é considerado o fundador do sistema binário e da linguagem dos sistemas informáticos. Para Boole todos os raciocínios expressos em linguagem gramatical, verbal ou escrita, podem ser convertidos em fórmulas matemáticas e expressos dessa forma. Para isso estabeleceu um sistema assente em três tipos de símbolos:

i) Símbolos de conceitos (compostos por letras x, y, etc.);

ii) Símbolos de operações (+, -)

iii) Símbolos de identidade (=).

Sobre estes três tipos de símbolos se formulam, segundo Boole, os raciocínios científicos e as formulações racionais.[21]

Todas as proposições lógicas se poderiam exprimir através de fórmulas que utilizariam esses tipos de símbolos, compondo formulações e juízos com a mesma estrutura e método da álgebra.

Boole desenvolve e conclui a ambição de Leibniz de aplicação do método matemático à lógica, ao raciocínio científico e ao discurso gramatical. Como afirma com propriedade Rodriguez Margariños, *"A aritmética de Boole configura uma ponte*

[19] Bochenski, I. M., (1976). Historia de la Lógica Formal. Editorial Gredos, Madrid, pág. 290, 291.
[20] Bochenski, Op. Cit., pág. 292.
[21] Bochensky, Op. Cit., pág. 313.

entre o mundo das matemáticas e o das ideias (expresso em palavras)"[22], traduzindo as proposições gramaticais utilizando as fórmulas matemáticas.

Nas suas obras *"Mathematical Analysis of Logic"* e "*Laws of Thought"*, Boole constrói uma convenção em que o símbolo 1 corresponde a uma afirmação de verdade e o símbolo zero à falsidade.[23] Estava descoberto o caminho que viria a dar origem ao sistema binário.

2.1.2. Digitalização, mecanização e eletrificação

Alguns anos antes de Boole já Blaire Pascal (1626 – 1662) havia inventado a primeira máquina de calcular numérica, em 1642, automatizando pela primeira vez a realização de operações algébricas simples.[24] Tendo por base que as regras matemáticas são universais e que os símbolos numéricos também o são, Pascal aplicou esses princípios a uma máquina por si concebida e colocou-a a efetuar operações simples, que conduziam a resultados iguais aos apurados por cálculos mentais efetuados pelo homem.[25]

Esse sonho, que Leibniz designava de matemática universal e de *Philosophia perenis*,[26] viria a ser desenvolvido por Boole, que encontrou um método de conversão de proposições lógicas do raciocínio em formulações matemáticas. O raciocínio lógico seria veiculado através de conjunções, disjunções, negações, condições e dependências condicionais.

Com base nos fundamentos Booleanos do raciocínio lógico-matemático e do sistema binário, um dos seguidores de Boole, W. S. Jevons publicou em 1870 as suas "Elementary Lessons in Logic" e apresentou, em simultâneo, uma máquina em que as diversas combinações lógicas de Boole aparecem e desaparecem quando se carrega em teclas.[27] A simplicidade e segurança lógica do sistema de Boole tornava-o facilmente

[22] Rodriguez-Margariños, F.G. (2008), pág. 18.
[23] Kneale, W. e Kneale, M. (1980). O Desenvolvimento da Lógica. 2.ª edição, Fundação Calouste Gulbenkian, Lisboa., pág. 418 e 419.
[24] Rodriguez-Margariños, F.G. (2008); Op. Cit., pág. 17.
[25] Rodriguez-Margariños, F.G. (2008), *idem*..
[26] Na expressão de Fraile, "Com estes procedimento chegar-se-ia a converter todas as ciências em ramos da matemática e assim a matemática universal seria a ciência suprema na qual se unificariam todas as restantes". Fraile, G; (1978), Op. Cit., pag. 663.
[27] Kneale, W. e Kneale, M. (1980). Op. cit., pág. 426 e 427.

suscetível de ser operado por máquinas e reproduzível por sistemas mecânicos, e seria isso que viria a acontecer.

Alan Marquand lançou em 1885 a ideia de eletrificar a máquina de Jevons, o que viriam a fazer T. A. Kalin e W. Burkhart quando em 1947 apresentam uma máquina elétrica que aperfeiçoa a de Jevons e resolve proposições envolvendo até 12 variáveis.[28] A eletrificação da máquina de Jevons é um dos primeiros computadores da história.[29]

A mecanização e eletrificação do sistema de Boole foram possíveis fazendo corresponder as proposições lógicas a impulsos elétricos. A ligação de um interruptor, permitindo a passagem de energia, pode corresponder à afirmação, e o corte da energia, quando se desliga o interruptor pode corresponder à negação, ou à falsidade. O sistema digital de Boole passa a ser operado por impulsos elétricos. Se utilizarmos este mecanismo em vários transístores da mesma máquina, podemos elaborar várias combinações, tal como Leibniz distinguia que os conceitos compostos são combinações dos conceitos simples. Na lógica de Boole, a passagem de energia pode corresponder à afirmação, ou ao código 1 e a não passagem de energia à negação, ou código zero. É este o funcionamento do sistema binário ou digital e o fundamento da programação informática.

A programação informática consiste então na definição de várias instruções dadas pelo homem (o operador ou programador) à máquina (os sistemas informáticos), por exemplo, se A e B são afirmativos, então passamos a C, e se C coincide com F, passamos a G, e assim sucessivamente. Como explicam Wiliam e Martha Knealle, *" Se ligar um interruptor que tenha que estar num de dois estados é comparável à afirmação de uma proposição, desligá-lo é comparável à negação da mesma proposição; a combinação de dois interruptores em série pode ser comparada à conjunção de duas proposições, enquanto a disposição em paralelo pode ser comparada à conexão de duas proposições por 'ou' "*.[30]

[28] Kneale, W. e Kneale, M. (1980). Op. Cit., pág. 427.
[29] Para Rodriguez-Margariños foram John Presper Eckert e John Williams Mauchly que construíram em 1946 o primeiro computador, mas um tribunal americano reconheceu esse título a John Vincent Atanasoff, professor catedrático da Universidade de Iowa, que em 1937 inventou uma máquina de cálculo com a qual trabalhava nas suas investigações. A categoria de inventor do primeiro computador é ainda disputada por Howard Aiken, que em Fevereiro de 1944 apresentou o Mark I, uma máquina capaz de efetuar as quatro operações aritméticas fundamentais, de somar, subtrair, multiplicar e dividir, sem qualquer intervenção humana. Aiken trabalhava já para a IBM, que subsidiou a sua investigação. Rodriguez-Margariños, F.G. (2008), Op. Cit., pág. 19.
[30] Kneale, W. e Kneale, M. (1980). *Idem*.

2.1.3. A revolução da digitalização

A possibilidade de transformar as formulações escritas do raciocínio humano nos dois símbolos digitais da linguagem binária trouxe a possibilidade de traduzir para a programação informática a produção do pensamento humano, permitindo a gravação e a circulação nas redes informáticas todo o conhecimento escrito.

Esse processo expandiu-se no início da década de 80 do século XX com a descoberta da possibilidade de digitalização da voz humana, até aí efetuada através do fio de cobre com a tecnologia das ondas que reproduzem uma frequência, idêntica à que era utilizada na transmissão do sinal de rádio.[31] A sua digitalização converte-a numa sequência de bites, logo que é emitida, mediante um codificador, passando a sua transmissão a ser efetuada em forma de dados digitalizados, sendo descodificados no final pelo aparelho recetor. O procedimento é idêntico ao que ocorre na produção e envio de um documento em forma de texto.

A mesma tecnologia permitiu que, na década de 90 do século XX, se tivesse alcançado a digitalização da imagem em movimento[32], passando assim os suportes eletrónicos a poderem armazenar e comunicar todos os tipos de informação.[33]

2.2. A Internet e as redes abertas

A Internet nasceu em 1969,[34] quando se estabeleceu a primeira ligação entre computadores por linha telefónica no seio da comunidade académica e no desenvolvimento do programa ARPA,[35] O projeto teve iniciativa no Departamento de Defesa dos EUA e envolvia o Instituto Tecnológico do Massachusetts (MIT), o Stanford

[31] Rodriguez-Margariños, F.G. (2008); Op. Cit., pág. 27.
[32] Rodriguez-Margariños, F.G. (2008), Op. Cit., pág. 28.
[33] Roques-Bonnet fala de uma revolução que a digitalização proporcionou, tornando os suportes eletrónicos o instrumento essencial para o acesso ao conhecimento e à cultura. *"l'Internet conditionne l'accès à la culture et à la connaissance. Depuis la révolution numérique, jamais dans l'histoire de l'humanité l'acess à la culture n'a eté aussi facile et ouvert'"*. Roques-Bonnet, M.C. (2010). *Le Droit. Peut'il Ignorer la Révolution Numérique?*. Michalon Éditions. Paris, pág. 553.
[34] Acerca do aparecimento da Internet, Barret, N. Op. cit., págs. 193 e seguintes.
[35] Advanced Research Project Agency (ARPA): *"O objetivo que o ARPA perseguia era dispor de informação estratégica contida em diferentes computadores muito distantes entre si (...).A ARPANET pretendia criar uma rede que unisse os centros de investigação dedicados à defesa, capaz de manter o seu funcionamento mesmo no caso de um ataque nuclear")*. Blasco, J.A. (2005). Qué es Internet. Em: Mexía, P.G (Director). *Principios de Derecho de Internet*. 2.ª Edição, Tirant lo Blanch, Valencia., pag. 31 e 35.

Research Institute – SRI, da Universidade de Stanford, Universidade da Califórnia em Los Angeles (UCLA), a Universidade da Califórnia em Santa Bárbara (UCSB) e a Universidade do Utah. O objetivo do ARPA era a criação de uma rede de comunicações não hierarquizada e dispersa, que funcionasse sem nenhum centro nevrálgico. [36]

O projeto era liderado desde 1962 pelo académico do MIT, Joseph Carl Robnett Licklider, com obra publicada onde teorizava uma futura conexão entre computadores em diversos pontos do mundo,[37] estabelecendo redes de computadores, com dimensão universal, à qual todos poderiam aceder,[38] que pudesse continuar a funcionar mesmo no caso de uma eventual destruição de uma parte da rede por um eventual ataque militar inimigo, mesmo que, no limite essa rede de se reduzisse a dois computadores. [39] [40]

Um dos membros do grupo era Leonard Kleinrock, investigador do MIT, em cuja tese de doutoramento, de 1961, teorizava acerca da transmissão de dados entre computadores, em rede aberta, mediante a comutação de pacotes de dados digitalizados. Foi ele que estabeleceu a primeira ligação por linha telefónica entre os computadores da

[36] Como indica Cremades, *"A Internet nasceu de um projeto de defesa (Arpanet) auspiciado pelo Pentágono norte-americano e pela administração da Defesa dos EUA"*. Cremades, J. (2002). Cultura y Internet: Una Nueva Revolución. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., Régimen Jurídico de Internet. La Ley. Madrid, pág. 166.

[37] Uma teoria que se viria a revelar "visionária", na expressão de Kloos: *"Licklider era um cientista visionário do MIT*. Kloos, C.D.e Rubio, C.G. (2002). História de Internet. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., *Régimen Jurídico de Internet*. La Ley. Madrid. pag. 88. *"Licklider concebeu uma rede interconectada globalmente, através da qual qualquer pessoa pudesse aceder desde qualquer lugar a dados e programas."*. Leiner, Barry M.; Cerf, Vinton G.; Clark, David D.; Kahn, Robert E.; Kleinrock, Leonard; Lynch, Daniel C.; Postel, Jon; Roberts, Lawrence G.; Wolff, Stephen; Op. cit. *Idem*.

[38] O próprio Kleinrock descreve o papel visionário de Licklider: *"La primera descripción documentada acerca de las interacciones sociales que podrían ser propiciadas a través del networking (trabajo en red) está contenida en una serie de memorándums escritos por J.C.R. Licklider, del Massachusetts Institute of Technology, en Agosto de 1962, en los cuales Licklider discute sobre su concepto de Galactic Network (Red Galáctica)*.". *Ibidem*, *Idem*.

[39] O objetivo da ARPANET *"era colocar em marcha uma rede experimental de computadores sem centros nevrálgicos, na qual cada nó pudesse comunicar com qualquer outro através de mais do que uma via, e na qual a informação circulasse dividida em pacotes pequenos, de modo a garantir que a rede pudesse continuar operativa mesmo no caso de ocorrer uma suposta guerra nuclear"*. Mundet, J.R.C.P. e Peña, F.M. (2006). *Información y Documentación Administrativa*. 2.ª Edição; Editorial Tecnos. Madrid., pág. 41.

[40] Como ensina Manuel Castells, *"A Internet nasceu na encruzilhada insólita entre a ciência, a investigação militar e a cultura libertária"*, mas com uma estrutura capaz de corresponder *"às necessidades militares de sobrevivência: flexibilidade, ausência de um centro de comando e máxima autonomia em cada nó"*. Castells, M., (2004). A Galáxia Internet - Reflexões Sobre a Internet, Negócios e Sociedade. Fundação Calouste Gulbenkian, Lisboa, pág. 34. Do mesmo modo, acerca da origem militar do ARPA, Ruiz, Carlos Barriuso; "La Contratación Digital - 3.ª Edición" Editorial Dykinson, Madrid, 2006, pág. 63.

UCLA e do SRI, assim nascendo a primeira rede, a rede do ARPA, que foi designada de ARPANET.[41]

O protocolo TCP – *Transmission Control Protocol*, de intercomunicação de redes, apresentado em 1973, que haveria de dar origem ao protocolo TCP-IP[42], adotado em 1983, veio permitir ligar entre si todos os computadores e sistemas informáticos e redes fechadas já então existentes, independentemente da heterogeneidade da sua linguagem e do seu sistema operativo e viria a expandir extraordinariamente os nós ligados em rede. A ARPANET passou a ser uma rede de redes. As redes informáticas internas das universidades, das empresas e dos organismos públicos começaram a ligar-se à rede mais ampla da ARPANET e esta passou a ser uma meta-rede, uma inter-rede. Foi assim que nasceu a Internet, afinal uma rede de redes, uma rede global que liga entre si várias redes.

2.3. O Intercâmbio Eletrónico de Dados (EDI)

No início da década de 1980, a tecnologia EDI, veio permitir a comunicação entre computadores ligados, por linha telefónica, através de mensagens parametrizadas.[43] A parametrização permite que a informação seja tratada de forma imediata e automática pelos sistemas informáticos.[44] Esta tecnologia tinha a capacidade

[41] "Ligámo-nos por telefone com o SRI. Na UCLA carregámos na tecla L e perguntámos-lhes: *'Vêm a letra L?'. Responderam: 'Sim, vemos'. Carregámos então na tecla O. 'Vêem o O?'. 'Sim, vemo-lo'. Então carregámos na tecla G e o sistema caiu. Foi desta forma que nasceu uma revolução".* É assim que descreve Kleinrock como nasceu a Internet, em 1969, ao ligar um computador do MIT, onde trabalhava, com outro do SRI, utilizando a linha telefónica. Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C.; Postel, J.R., Lawrence G., Wolff, S. (1989). Op.cit. *Idem*.

[42] Tomás Friedman descreve a importância do protocolo TCP/IT da seguinte forma: *"O protocolo TCP/IT funcionava como uma canalização básica da Internet, ou os carris de base de uma via férrea, sobre os quais se movimentava tudo o resto"*. Friedman, T.L. (2005). *O Mundo é Plano - Uma História Breve do Século XXI*. Actual Editora, Lisboa, pag. 73.

[43] A definição de EDI do ABA, transcrita pela UNCITRAL é a seguinte: *"Electronic data interchange 'EDI' is the method by which business data may be communicated electronically between computers in standardized formats (such as purchase orders, invoices, shipping notices and remittance advices) in substitution for conventional paper documents. . . . Technically stated, EDI is the transmission, in a standard syntax, of unambiguous information between computers of independent organizations"*. A/CN.9/WG.IV/WP.53), par. 27.

[44] A primeira forma de comunicação eletrónica foi o telégrafo, inventado na década de 1830 por Samuel Morse. A primeira linha telegráfica ligou Washington a Baltimore, em 1844, tendo a primeira mensagem sido: "*What hath God wrought*!" (Que obra fez Deus!). http://www.reformation.org/what-hath-god-wrought.html (última consulta efetuada em 20/1/2016). O telégrafo era utilizado nas transações comerciais, nomeadamente no domínio financeiro, mas tinha a desvantagem da falta de sistematicidade do conteúdo das mensagens que, não sendo parametrizadas, davam origem a erros de interpretação pelas partes. Como se refere no Projeto de Guia Legal Sobre a Transferência Eletrónica de Fundos, de 1984, *"Credit transfers in electronic form have been widely used for over a hundred years in the form of*

de fazer substituir o papel pelos suportes eletrónicos nas operações negociais das empresas, de forma universal, desmaterializando assim a documentação das transações entre empresas e, tão importante como isso, o tratamento automatizado das operações entre as empresas.[45] [46] [47] Fica aberta, assim, a possibilidade de dispensa da intervenção humana no tratamento de dados, uma vez que todas essas operações são efetuadas pela interação dos sistemas informáticos de ambos os intervenientes.[48] [49]

A UNCITRAL identifica as seguintes caraterísticas definidoras do EDI:[50]

i) A transmissão de dados negociais;

ii) Efetuada entre computadores;

iii) Operada por diferentes empresas;

Telegraphic transfers". A/CN.9/250 and Add.1 to 4), pág. 123. Em Portugal o artigo 379.º do Código Civil considera os telegramas como documentos particulares, desde que se demonstre que os respetivos originais haviam sido assinados pelo seu autor. Do mesmo modo o Código Comercial já estabelecia no artigo 97.º a admissibilidade da correspondência telegráfica como fonte probatória. Sob o título *"Admissibilidade da correspondência telegráfica e seu valor"*, este artigo 97.º estabelece, no § 1.º uma norma idêntica ao artigo 397.º do Código Civil, acrescentando o § 3.º que *"o mandado e toda a prestação de consentimento, ainda judicial, transmitidos telegraficamente com a assinatura reconhecida autenticamente por tabelião são válidos e fazem prova em juízo"*.

[45] Segundo o CMI, o EDI consiste no *"intercâmbio de dados negociais através de teletransmissão"*. *"The interchange of trade data effected by teletransmission"*. "CMI Rules for Electronic Document Interchange (EDI), Appendix A, 13 Octobber 1999", http://web.uct.ac.za/depts/shiplaw/cmi/cmirules.htm (consulta em 27/6/2015).

[46] A definição de EDI dada por Helmut Kracmar e outros é a seguinte: *"Electronic data interchange is the inter-company computer-to-computer communication of standard business transactions in a standard format that permits the receiver to perform the intended transactions"*. Kracmar, H., Bjorn-Andersen, N. e O' Callaghan, R. (1995). *EDI in Europ*, John Wiley & Sons. Chichester., pág. 2.

[47] A importância e a variedade de funcionalidades proporcionadas pelo EDI é evidenciada no Relatório TEDIS nos seguintes termos: *"Enables companies to improve both the quality and cost of inventory management and to shorten the 'order / product delivery or provision t of services / billing / Payment' cycle"*. E mais adiante: *"Transfer trade documents relating to orders and their confirmation, delivery and reception of goods, and invoicing of products and services provided. It is also used in the case of so-called "interactive" transactions, such as in travel, hotel and theatre reservations or banking or money transfer operations. Of more recent date is the application of EDI to electronic points of sale (EPOS), to direct debit payment systems, to electronic funds transfer (EIT), to financial credits, or to computer-assisted trading systems (CATS)"*. "TEDIS - The Legal Position of the Member States With Respect to Electronic Data Interchange". Commission of the European Communities. Final Report". September 1989, pág. 28 e 30, respetivamente.

[48] O EDI permite a programação dos sistemas informáticos para que sejam efetuadas, recebidas e processadas ordens de encomenda sem intervenção humana, dado que os sistemas informáticos podem ser programados para emitir essas ordens em determinadas circunstâncias de facto que eles próprios detetam, mediante programação. *"A purchaser's computer may be programmed to send purchase orders under certain circumstances, and the supplier's computer may be programmed to act upon the orders it receives, both without human intervention"*. A/CN.9/333, par. 61.

[49] *"The ultimate goal of EDI is that the receiving computer applications accept and process the data transmitted without additional human intervention. This implies that the data be coded in some pre-established format"*. Kracmar, H., Bjorn-Andersen, N. e O' Callaghan, R. (1995), Op. Cit., pág. 17.

[50] *"Although they differ slightly as to their wording, most definitions of EDI contained in existing model interchange agreements seem to rely on a combination of two or more of the following elements: the transmission of trade data; between computers; operated by different trading partners; by reference to a standardized syntax or format; through the use of electronic means"*. "A/CN.9/WG.IV/WP.53", pág.s 365 a 382, par. 27.

iv) Mediante formatos pré definidos; [51]

v) Através de meios eletrónicos.[52]

A importância e o impacto do EDI nas operações comerciais deu origem ao conceito de mercado eletrónico.[53]

2.4. As redes abertas

Enquanto o EDI era um sistema fechado, que exige uma prévia conexão, a Internet é uma rede aberta de redes, a que podem aceder qualquer cidadão e empresa, de forma simples e com baixos custos. Enquanto o EDI exigia uma convenção prévia entre agentes económicos, a Internet não a pressupõe, que permitiu a comunicação com um universo infinito de destinatários que até aí não se conheciam.

A generalização da digitalização permitiu que através da rede das redes passassem a poder realizar-se praticamente todos os tipos de atividades económicas.[54]

A generalização da utilização da Internet nas relações comerciais e a universalização do acesso dos cidadãos à rede criou pela primeira vez um mercado global sem fronteiras, substituindo o tradicional conceito de mercado como um local físico onde se efetuam transações em determinados horários.[55] Aumentaram

[51] É por essa razão que o EDI não inclui as comunicações por correio eletrónico nem comunicações em texto livre. Não inclui também a transmissão de imagens nem de quaisquer conteúdos que não respeitem rigorosamente o formato pré-definido e rígido dos sistemas EDI. Como refere o SITPROSA, a definição de EDI *"does not include facsimile transmissions, electronic mail or other forms of free formatted text or images"*. A/CN.9/WG.IV/WP.53, par. 29.

[52] O Relatório TEDIS define EDI como *"Electronic Data Interchange, commonly abbreviated to EDI, differs from conventional methods of transmitting data to the extent that it allows direct computer-to-computer transfer of structured and standardised data"*. "TEDIS Report", pág. 27.

[53] *"Networks with multiple suppliers and multiple participants ... can develop into electronic markets".* Kracmar, H., Bjorn-Andersen, N. e O' Callaghan, R. (1995), Op. Cit., pág. 5.

[54] Como explicam Velasco e Castejón, *"A revolução em curso baseia-se na digitalização, ou seja, na transformação de todo o tipo de informação (imagens, sons, grafismos) num código de símbolos (dígitos) que se expressa numa base binária utilizando unicamente o zero e o um. Isso tornou possível, por um lado, a explosão de uma oferta informativa sem precedentes na história e, por outro lado, abriu a perspectiva da convergência entre as redes, as infra-estruturas e os aparelhos terminais e receptores".* Velasco, M.M.P e Castejón, J.C. (2002). Regulación Versus Autorregulación en Internet y los Nuevos Servicios de Comunicación. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., Régimen Jurídico de Internet. La Ley. Madrid, pág. 121.

[55] Essa universalização é reconhecida como o principal fator de eficiência económica da rede. Esse é o principal fundamento invocado na proposta de Diretiva da UE relativa ao quadro comum das assinaturas eletrónicas, apresentada pela CE ao Parlamento Europeu em 13/5/1998: *"As redes eletrónicas abertas, como a Internet, têm uma importância crescente nas comunicações à escala mundial. Oferecem a possibilidade de comunicações interactivas entre partes que até aí não tinham estabelecido relações"*. COM(1998) 297 final.

substancialmente as possibilidades de crescimento das transações para os agentes económicos.[56]

3. A insegurança jurídica dos suportes eletrónicos

Os instrumentos jurídicos de segurança na vinculação dos documentos foram construídos no paradigma do papel, sendo nesse contexto que se formaram os conceitos de escrita, documento e assinatura. A emergência dos suportes eletrónicos altera esse paradigma, e apesar de se tratar apenas de uma mudança de suporte, a utilização destes novos meios exige um conjunto de ajustamentos legais que garantam a solidez do eletrónico.[57] É essa a problemática central do regime jurídico da assinatura eletrónica.

3.1. A insegurança jurídica eletrónica anterior emergência das redes eletrónicas

A utilização dos meios eletrónicos pelos agentes económicos ocorreu inicialmente numa base informal, apenas para a execução de procedimentos rotineiros e instrumentais, sem relevância jurídica e, quando envolviam comunicações externas, ocorriam entre agentes económicos que se conheciam mutuamente e operavam no contexto de uma relação de confiança.[58] Mas o EDI veio permitir a desmaterialização e a automatização de todas as comunicações entre empresas, incluindo todas as declarações negociais. E a Internet e as redes abertas expandiram as possibilidades de as empresas estabelecerem relações jurídicas com pessoas que até aí lhes eram

[56] Como se refere na Resolução do Parlamento Europeu sobre o projeto de regime da assinatura eletrónica, *"o comércio eletrónico pode transformar-se num dos motores do desenvolvimento da sociedade de informação planetária; este novo espaço económico «virtual», de grande potencial para a criação de empregos, encontra-se, no entanto, ameaçado pela falta de segurança e confiança nas redes abertas"*. (COM(97)0503 C4-0648/97); JOCE nº C 292 de 21/09/1998 p. 0217, par. 23.

[57] Isto não quer dizer que concordemos com os autores que entendem que nos suportes eletrónicos desaparecem aqueles três elementos essências da segurança jurídica que enunciámos. *"The sudden arrival of the screen in business life has made three of the essencial rules of the perfect evidence disappear: the rule of writing –a paper medium; the rule og the original document – only one document, and the rule of the signature: only hand-signed document".* Bazin, Philippe; *op. cit*, pag. 180.

[58] As comunicações eletrónicas expandiram-se inicialmente nos mercados financeiros, numa base de confiança informal entre os agentes. Como se refere no relatório do Secretário Geral de 17/5/1982, *"electronic funds transfer systems have developed in a partial legal vacuum"*, acrescentando-se, de seguida, que os pressupostos técnicos e jurídicos necessários a garantir a garantir a segurança eram ainda muito incipientes. *"Electronic funds transfer systems, especially those based on computer-to-computer transmissions, are still in their infancy"*. A/CN.9/221, pág. 23.

desconhecidas. A digitalização criou ainda as condições para que o comércio eletrónico se alargasse à generalidade das atividades empresariais e aos procedimentos administrativos.

Onde anteriormente existia apenas o papel como suporte para a documentação dos negócios e dos atos jurídicos, passaram a existir também os suportes eletrónicos. Ora, as normas legais que regulam essa documentação haviam sido concebidas para o papel e podem não ser linearmente transpostas para os suportes eletrónicos. E nessa transição, os problemas que se colocavam eram, fundamentalmente os seguintes:[59]

i) O problema da prova mediante documentos eletrónicos, bem como a admissibilidade da sua utilização nos procedimentos administrativos, em especial perante as entidades aduaneiras, e fiscais no que respeita à documentação contabilística e fiscal.[60]

ii) O problema da própria validade jurídica dos documentos e dos registos eletrónicos. A legislação não previa a utilização dos suportes eletrónicos no comércio jurídico. [61] Esta incerteza obrigou as empresas a manterem a sua documentação duplicada nos suportes eletrónicos e de papel.[62] Os custos desse armazenamento eram um constrangimento para

[59] Hatfield e Casamento enunciam cinco fatores de insegurança na utilização dos meios eletrónicos nas atividades empresariais. O risco de autenticação, que designam como o risco da falsificação da identidade, o risco de repúdio, como a possibilidade de o autor negar a autoria posteriormente, o risco de admissibilidade, ou seja, de o destinatário impugnar a validade e eficácia do atos constantes dos documentos em suporte eletrónico, o risco de cumprimento, nos casos em que a utilização dos meios eletrónicos não cumpra normas especificas da legislação dos países onde a sua eficácia é requerida, e finalmente o risco de adoção, que consiste no custo que os agentes económicos teriam que suportar pelo risco de utilização dos meios eletrónicos. Casamento, G. e Hatfield, P. (2009). The Essential Elements of an Effective Electronic Signature Process. Digital Evidence and Electronic Signature Law Review. Vol 6: pag. 84.

[60] A UNCITRAL separava três tipos de documentação com valor jurídico, necessários à atividade das empresas – i) a que consiste na comprovação da realização de operações comerciais, como contratos e outros; ii) registos diários de operações; e iii) resumos diários de operações. *"(1) originals or copies of transaction documents, (2) chronological records of transactions or (3) summary records of those transactions"*. "A/CN.9/265", par. 4.

[61] *"In certain cases, existing legislation imposes or implies restrictions on the use of modern means of communication. While a few countries have adopted specific provisions to deal with certain aspects of EDI, there exists no legislation dealing with EDI and related means of communication as a whole. This may result in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper-based document"*. A/CN.9/426, par. 22.

[62] Esse facto levava as empresas a reservar a utilização de meios eletrónicos para as operações comerciais mais rotineiros e com menor relevância jurídica. *"In order to store computer records in a form which could not be altered, some enterprises have stored authenticated and dated hard copies of all significant records"*. "A/CN.9/265", par. 26.

a utilização dos meios eletrónicos.[63] Esse facto era agravado pela inexistência de soluções legislativas sólidas que os evitassem.[64]

iii) O problema da originalidade e singularidade dos títulos transacionáveis, em que a respetiva posse titula a propriedade. Como se pode garantir que não existe duplicação quando os títulos são eletrónicos?

iv) O problema do arquivo dos documentos eletrónicos, nomeadamente a garantia da manutenção da integridade desses documentos ao longo do tempo, e a garantia da sua legibilidade futura;

v) A validade jurídica das declarações negociais emitidas automaticamente pelos sistemas informáticos, sem intervenção humana imediata e sua eficácia na vinculação das pessoas, que terão que ser sempre os sujeitos de uma relação jurídica?[65]

vi) A responsabilidade em caso de erro na emissão daquelas declarações negociais; [66]

vii) A validade e eficácia jurídica dos documentos eletrónicos nos casos em que a legislação interna dos países exige documentos formais, designadamente os documentos notariais. [67]

A adoção de mecanismos jurídicos de segurança nas transações eletrónicas era uma necessidade cada vez mais urgente e reconhecida.[68] A falta dessa regulação era um

---

[63] Esta é uma das preocupações reveladas no Guia Legal da Transferência Eletrónica de Fundos, de 1987, nomeadamente quando se reconhece que *"The volume of electronic funds transfers and the sums involved suggest that the potential losses could exceed the losses experienced with paper-based funds transfers"*."UNCITRAL Legal Guide on Electronic Funds Transfer", pág. 48.

[64] A falta de soluções juridicamente adequadas era uma preocupação da UNCITRAL, que a reconhecia em vários textos. *"There remain a surprising number of unanswered questions in many legal systems"*. "UNCITRAL Legal Guide on Electronic Funds Transfer", pág. 48.

[65] *"... Remaining uncertainties in a number of countries as to whether contracts can validly be concluded by electronic means. The need for such a provision results from the doubt that may exist in many countries as to the validity of contracts concluded through the use of computer because the data messages expressing offer and acceptance may be generated by computers without immediate human intervention, thus raising doubts as to the expression of intent by the parties".* Essa incerteza incluía a natureza escrita dos documentos eletrónicos. *"Another reason for such uncertainty is inherent in the mode of communication and results from the absence of a paper document"*. "A/CN.9/426", par. 102.

[66] As questões jurídicas emergentes do EDI foram elencadas, embora apenas a título exemplificativo, pela primeira vez pela UNCITRAL, no relatório de 1992. *"There existed a need for legal norms to be developed in the field of EDI. (...) Examples of such issues included: formation of contracts; risk and liability of commercial partners and third-party service providers involved in EDI relationships; extended definitions of "writing" and "original" to be used in an EDI environment; and issues of negotiability and documents of title"*. "A/CN.9/360", par. 129.

[67] *"Such forms include notarization and other requirements for "writings", and might respond to considerations of public policy, such as the need to protect certain parties or to warn them against specific risks"*. "A/CN.9/426", par. 105.

[68] Essa necessidade intensificou-se no final da década de 1980. Como refere, em 1988, o Grupo de Trabalho sobre os Pagamentos Internacionais da UNCITRAL. *"There was general agreement that the*

entrave cada vez mais sensível à utilização dos meios eletrónicos no comércio internacional.[69] A ausência dessa regulação conduziu as organizações empresariais a criarem regras uniformes de carácter contratual, mediante convenções.[70]

Foi nesse contexto que se iniciaram os trabalhos de conceção da LMAE, destinada, em primeiro lugar, a eliminar as barreiras jurídicas à utilização do suporte eletrónico nas relações contratuais e a conferir aos documentos eletrónicos o mesmo valor probatório dos documentos em papel.[71][72]

3.2. A insegurança jurídica das redes abertas

A utilização das redes abertas na atividade comercial exige segurança jurídica.[73] Mas pressupõe também o estabelecimento de relações com agentes económicos desconhecidos, o que aumenta a insegurança no que respeita à identidade e vinculação das partes.[74] A rede das redes não foi concebida como meio para a prática de

---

preparation of Model Rules for electronic funds transfers was both important and urgent. The rapid growth in international funds transfers and the entry of foreign parties into domestic financial system increased the need for clear rules". A expansão da utilização das comunicações eletrónicas havia já chegado às relações comerciais entre as empresas e os consumidores, envolvendo também, já nessa época, aquisições internacionais. *"Modern technology made it possible for a customer or a group of a customers to effect related funds transfers successively in different markets and in different time zones, thereby increasing the importance of having harmonized legal rules governing those various funds transfers."* A/CN.9/317, pág.s 42 e 43.

[69] Essa preocupação é também assinalada na Recomendação da UNCITRAL sobre o valor jurídico dos registos informáticos, nos seguintes termos: "*A more serious legal obstacle to the use of computer records and computer-to-computer telecommunications in international trade arose out of the requirements that documents had to be signed or be in paper form"*. "UNCITRAL Recommendation on the Legal Value of Computer Records (1985)".

[70] A insuficiência dos modelos contratuais de regulamentação era reconhecida nos relatórios publicados da UNCITRAL. *" The contractual approach is limited in that it cannot overcome any of the legal obstacles to the use of EDI that might result from mandatory provisions of applicable statutory or case law. (...) Another limitation to the contractual approach results from the fact that parties to a contract cannot effectively regulate the rights and obligations of third parties"*. A/CN.9/426, 24 April 1996, par. 17.

[71] O atraso na criação dessa legislação é reconhecido em vários textos, até da segunda parte da década de 90 do século passado. *"It has been suggested by the Norwegian Committee on Trade Procedures (NORPRO) in a letter to the Secretariat that "one reason for this could be that the 1985 UNCITRAL Recommendation advises on the need for legal update, but does not give any indication of how it could be done""*. "A/CN.9/426", par. 6.

[72] O objetivo da LMCE era abranger qualquer tipo de comunicação eletrónica. *"It should be noted, however, that the aim of the uniform rules is to enable, and not to impose, the use of EDI and related means of communication"*. "A/CN.9/426", par. 18.

[73] Como afirma Garnacho, *"A segurança (...) é a pedra angular da qual dependem as novas tecnologias da informação cujo limiar estamos ainda a tentar entrar."*. Garnacho, A.R. (2002). *Sistema de Certificación: La Firma y el Certificado Digital. Regimen Jurídico de Internet*. Editorial La Ley. Madrid., pág. 1314.

[74] Como refere Dan Kaminsky, *"Internet nunca fue diseñado para ser seguro, sino para funcionar; era el terreno de juego de un puñado de frikis como nosotros"* acrescentando que *"Todos somos un objetivo*

atos de natureza jurídica.[75] E o seu poder, que reside mesmo em cada um dos milhões de utilizadores e não em qualquer unidade central de gestão,[76] é também a principal causa da sua insegurança.[77]

Nadal assinala às redes abertas quatro riscos fundamentais de insegurança – a facilidade de simulação da identidade (o designado roubo de identidade), a adulteração do conteúdo dos documentos, a rejeição pelo titular, de um documento por si emitido e o perigo de violação da confidencialidade.[78]

Apesar disso a Internet cresceu e converteu-se numa espécie de praça pública da sociedade da informação, uma nova espécie de Acrópole cibernética, onde os cidadãos discutem os problemas da sua comunidade, se informam sobre eles e exercem a sua opinião.[79] Expandiu-se também à atividade económica e converteu-se num mercado aberto, apesar do seu caráter inseguro.[80]

3.3. Insegurança quanto aos sujeitos

hacker" e "la economia global depende de Internet". http://www.huffingtonpost.es/2015/08/03/kaminski-seguridad-online_n_7924008.html (consulta em 3/8/2015).

[75] No mesmo sentido Velásquez: *"A segurança da Internet não é suficientemente consistente para suportar o peso do que transporta. A Internet não foi desenhada para ser aquilo que é actualmente"* Velásquez, Raúl Rubio; Sal, Carlos Rodriguez; Muñoz, Ramiro Muñoz; Velásquez, Raúl Rubio; Sal, Carlos Rodriguez; Muñoz, Ramiro Muñoz; "La Firma Digital - Aspectos Legales e Técnicos", Ediciones Experiência, Barcelona, 2004, pág. 172.

[76] Assim o afirma também Castells: *"A cultura da Internet radica na tradição académica da investigação científica partilhada, na reputação obtida graças ao prestígio académico, na avaliação por parte dos colegas e na abertura e publicidade das investigações, outorgando a merecida consideração aos autores de cada descoberta"*. Castells, M., Op. Cit., pág. 60.

[77] Como afirma Barriuso Ruíz, *"A Internet em si mesma é um canal inseguro, já que não foi concebida para certas aplicações, pelo que é necessário criar medidas suficientes de segurança e confidencialidade."* Ruíz, C.B. (2006). *La Contratación Electrónica.* 3.ª Edição. Editorial Dykinson. Madrid., pág. 603.

[78] Nadal, A.G. (2009). *Comentarios a la Ley 59/2003 de Firma Electrónica*. 2.ª edição, Civitas Aranzadi, Thomson Reuters. Pamplona., pág. 53.

[79] Roques-Bonnet compara a Internet a uma espécie de *ágora* que estava na base da polis da antiga Grécia, ou de república eletrónica. *"L'Internet offre la perspective d'une sorte d'agora, une place publique, como dans la polis grécque où chacun descendait quando bon lui semblait pour discuter avec le tout-venant des affaires de la cité, et où se formait la l'opinion des citoyens"*. Roques-Bonnet, M.C. (2010). Op. cit, pág. 135.

[80] É esse sentido inicial que capta Velásquez de forma exemplar, quando afirma que *"A segurança sempre foi entendida como um factor residual, principalmente porque segurança significa custos e incomodidades e um retorno de investimento que nunca é imediato (...) mas a utilização de medidas de segurança proporcionadas define claramente a maturidade tecnológica de uma empresa".* Velásquez, Raúl Rubio; Sal, Carlos Rodriguez; Muñoz, Ramiro Muñoz; Op. Cit., pág. 171.

A principal causa de insegurança é a falta de conhecimento pessoal dos agentes económicos que praticam negócios e atos jurídicos na Internet.[81] Nas relações estabelecidas através da Internet não releva a localização geográfica das partes, nem é necessário o conhecimento prévio, que eram caraterísticas essenciais do paradigma do papel e das redes fechadas.[82]

Nesse contexto a dissimulação da identidade e a falsificação dos conteúdos documentais são fáceis, mas incompatíveis com a segurança jurídica.[83] [84] Do mesmo modo a determinação da identidade e da autoria dos documentos é essencial para se a segurança da vinculação jurídica. Em sentido inverso, o repúdio da autoria de um documento é relativamente fácil se não houver mecanismos seguros de vinculação.[85]

A ordem jurídica pressupõe confiança, que a rede inicialmente não podia proporcionar.[86] [87]

A Internet tem o poder de colocar em contacto um universo de pessoas, de informação e de conhecimento que anteriormente se julgava impossível, mas é um instrumento técnico limitado, porque efetuado por máquinas e à distância. Não é um

---

[81] Esse mesmo desconhecimento pessoal é destacado por Velasco e Castejón: *"A estrutura descentralizada da rede torna completamente inoperante o esquema tradicional de imputar a responsabilidade ao autor ou difusor da informação. (...) Qualquer usuário, em qualquer parte do planeta, pode converter-se em difusor de informação dirigida a usuários de todo o mundo"*.Velasco, M.M.P e Castejón, J.C. (2002); Op. Cit, pág.s 122 e 123.

[82] Nas redes abertas as "*pessoas que nunca haviam mantido nenhuma relação previamente possam manter uma comunicação interactiva*". Más, F.J.G. (2004). *Comercio y Firma Electrónicos. Análisis Jurídico de los Servicios de la Sociedad de la Información*. 2.ª Edição, Editorial Lex Nova. Valladolid., pág. 36.

[83] *"A natureza aberta da rede, conatural à sua própria existência, torna possível a intercepção das comunicações por terceiros e a alteração das mensagens (...) tornando possível a simulação da identidade do primeiro ou a negação, por um ou por outro, da emissão e da receção da mesma"*. Llovet, E.G. (2002). Acreditación. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., *Régimen Jurídico de Internet*. La Ley. Madrid., pág. 373.

[84] Assim o sustenta também Garcia Lhovet, quando afirma que *"A garantia da segurança das transações, da personalidade dos contraentes, do conteúdo dos contratos e do tempo de celebração dos mesmos é, em última análise, a garantia de viabilidade da rede como espaço de comércio"*. Llovet, E.G. (2002). Op cit. pág. 373.

[85] Essa preocupação é também referida por Gamero Casado: *"O principal problema que se coloca no intercâmbio telemático de informação é a insegurança das transações (...), podendo ocorrer que se altere a mensagem, que se simule a personalidade do recetor, que o seu destinatário negue tê-la recebido, etc.."*. Casado, E.G., (2005). *Notificaciónes Telemáticas y Otros Médios de Notificación Administrativa en el Procedimiento Administrativo Comúm*. Editorial Bosch, Barcelona, pág. 119.

[86] Como afirmam Calvo-Sotelo e Coello, *"A rapidez e o volume de negócios exigem que se disponha de um sistema seguro, mas a rede é vulnerável e é suficientemente reconhecido por todos o défice de segurança na Internet";* Calvo-Sotelo, A.C. e Coello, M.C.L., (2002). La Firma Electrónica. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., Régimen Jurídico de Internet. La Ley. Madrid., pág. 1379.

[87] Nesse mesmo sentido Ortega Diaz: *"A existência de um espaço virtual absolutamente livre e sem regras, implica uma panaceia libertária que não tem espaço na economia de mercado"*. Díaz, J.J.O. (2008). *La Firma y el Contrato de Certificación Electrónicos*. Thomson – Aranzadi. Pamplona, pág. 17. Do mesmo modo Andrés Blasco: *"A evolução que a Internet sofreu, converteu-a num magma ingovernável"*. Blasco, J.A. (2005), Op. Cit., pág. 72.

espaço vivencial pleno, de convivência real, no sentido de encontro existencial e físico.[88] E por essa razão não permite que operem os ancestrais fatores de confiança fundados na relação pessoal direta. A confiança económica, de que a segurança jurídica é um instrumento essencial, é um processo volitivo, não apenas racional e objetivo, mas antes fundamentalmente subjetivo e pessoal, ou mesmo ético.[89]

É a perceção desta insegurança estrutural que está na base do direito da assinatura eletrónica.

3.4. Insegurança quanto aos documentos

Os documentos em papel são entidades físicas, materiais e incindíveis, onde não é possível separar o próprio documento do seu suporte. Nos documentos eletrónicos a sua composição em bites é uma realidade diferente da aparência com que se apresenta nos écrans dos computadores, para ser lido e interpretado pelo entendimento humano.[90] Esta separação entre o interface visual e o substrato de dados torna os documentos eletrónicos vulneráveis a alterações e falsificações, de difícil deteção.[91]

3.5. Insegurança quanto aos sistemas

Na Internet, os agentes económicos apresentam-se em forma de sítios *web*, que são, na verdade, equipamentos informáticos. Um instrumento fundamental de segurança

---

[88] Como dizia o filósofo Entralgo, *"perceber o outro é viver ameaçadora e prometedoramente um nós inseguro e incerto em razão de um movimento expressivo que está perante mim"*. Entralgo, P.L. (1983). *Teoría y Realidad del Otro*. Alianza Editorial. Madrid., pág. 429.

[89] Ainda Entralgo: *"no lapso temporal compreendido entre a minha perceção do outro e a resposta que lhe dou, adquire o seu constitutivo cariz ético – 'etifica-se' – o momento físico do encontro"*. Entralgo, P.L. (1983). Op. Cit., pág. 455.

[90] Essa facilidade é consequência da digitalização da informação. Nesse sentido, Velásquez: *"A digitalização comporta um grave perigo. A possibilidade de manipulação generalizada da imagem aumenta o risco de falsificação*. Velásquez, Raúl Rubio; Sal, Carlos Rodriguez; Muñoz, Ramiro Muñoz; Op. Cit., pág. 28. A qualidade que a digitalização proporciona na falsificação de documentos é destacada por Garnacho: "*Lamentavelmente, quando os dados estão em suporte digital são suscetíveis de ataques muito mais numerosos, subtis e insidiosos do que quando se encontram num substrato convencional*". Garnacho, Artur Ribagorda; Op.cit., pág. 1314.

[91] Com afirma a UNCITRAL*"The potential for fraud is considerable, due to the ease of intercepting and altering information in electronic form without detection, and the speed of processing multiple transactions"*. A/CN.9/WG.IV/WP.88, par. 30. Também Garnacho, *"A natureza digital do documento eletrónico torna-o susceptível de ser manipulado fraudulentamente"*. Garnacho, A.R. (2002); Op. Cit., pág. 1320.

jurídica é a garantia da vinculação das entidades que são titulares desses sistemas às operações efetuadas por seu intermédio.

São frequentes as operações de simulação de páginas na Internet denominadas por *"sproofing"* conduzindo o utilizador a operar com um delinquente que falsificou o original.[92]

É também frequente o designado *spam*, envio generalizado de mensagens de correio eletrónico não solicitadas, que pode, no limite, produzir situações de bloqueio que impedem a receção de comunicações digitais solicitadas ou desejadas.[93]

São conhecidos usos indevidos do correio eletrónico, nomeadamente o *Internet Worm*[94], o *Cancel Bot*[95] e o *Butter overflow*[96]. O mesmo autor cita alguns exemplos de vírus que ficaram conhecidos na história da informática pela sua especial danosidade.[97] A pirataria informática é também um dos mais importantes fatores de insegurança e mesmo de criminalidade na Internet.[98]

Do mesmo modo o *phishing*, que consiste na tentativa de obter informações de caráter crítico e confidencial junto dos visados pela fraude, para dessa forma, e na posse dessa informação, os agentes fraudulentos a utilizarem para fins ilícitos.[99]

---

[92] O *sproofing "Consiste em que o atacante detecta e cria uma cópia de todas as páginas que visita o usuário interceptado (...). Assim, através deste meio, o atacante pode monitorizar todas e cada uma das visitas da vítima assim como aceder a toda a informação que esta insere na web"*. Díaz, J.J.O. Op. Cit., pág. 179. Essa informação assim recolhida pode ser a relativa a palavras-passe ou outra, que permite aos agentes da fraude efetuar depois operações ilícitas com esses dados.

[93] O *spam* é o *"envio massivo de correio eletrónico não solicitado"*. Blasco, Javier de Andrés; Op. Cit., pág. 83. Blasco refere que o Spam nasceu como um problema quando em *"12 de Abril de 1994 a sociedade de advogados Canter e Siegel levou a cabo o envio indiscriminado de mensagens publicitárias através do serviço news"*. *Ibidem*, pág. 51.

[94] *"Um programa criado por Robert Morris que em 2 de Novembro de 1988 aproveitou uma vulnerabilidade no sistema de correio eletrónico, colocou fora de serviço 6.000 dos 60.000 computadores que estavam ligados à Internet."* Blasco, Javier de Andrés; Op. Cit., pág. 51.

[95] *"Um programa designado CancelBot eliminou cerca de 25.000 mensagens do sistema de news mundial. Acredita-se que essa eliminação era selectiva e destinada a fazer desaparecer determinadas mensagens referentes a uma série de temas em concreto"*. Blasco, Javier de Andrés; Op. Cit., pág. 51.

[96] Trata-se do envio através da rede, de vírus que irrompem nos computadores dos destinatários visados e *"que permitem executar programas de computador de um usuário sem que este possa fazer nada para evitá-lo"*. Blasco, Javier de Andrés; Op. Cit., pág. 83.

[97] São os casos do vírus que ficou conhecido como "CIH (mais conhecido como Chernobyl), *"que em 26 de Abril de 1999 afectou milhares de máquinas e foi o primeiro a afectar o hardware"*, bem como dos vírus "*Melissa*" e "*I love you*", dois vírus que *"foram particularmente prejudiciais, ocasionando graves problemas em computadores de todo o mundo"*. Blasco, Javier de Andrés; Op. Cit., pág. 51.

[98] Blasco enuncia alguns exemplos de pirataria informática, "*Cooko's egg",* em que *"piratas alemães se infiltraram em numerosas instalações do governo dos EUA. O motivo da intrusão era a espionagem"*, bem como o caso do russo Vladimir Levin, de São Petesrburgo, que em 1995 *"aproveitou a Internet para roubar milhões de dólares à banca, através de uma agência do Citibank"*. Blasco, Javier de Andrés; *Op. Cit*., pág. 51.

[99] Um exemplo de phishing é dado pela notícia seguinte: http://economico.sapo.pt/noticias/clientes-do-montepio-alvo-de-tentativa-de-fraude_98136.html (consulta efetuada e, 1/09/2010).

São ainda relevantes as *"cookies"*, ou sistemas espiões que são aplicações inseridas, via Internet, nos computadores dos utilizadores, para efetuar operações determinadas pelos responsáveis pela sua colocação. A Diretiva n.º 2009/136/CE, de 25/11/2009, alterou o n.º 3 do art.º 5.º da Diretiva n.º 2002/58/CE, no sentido de a colocação dessas aplicações depender sempre do consentimento dos destinatários.[100]

[100] Uma enunciação dos diversos tipos de intrusão eletrónica é efetuada por Roques-Bonnet, M.C. (2010).. Op. Cit, pag. 450 e ss.

Capítulo II - A formação da assinatura eletrónica

1. A história da formação da assinatura eletrónica

A formação do direito da assinatura eletrónica é a resposta à insegurança técnica e jurídica dos suportes eletrónicos.[101] E nesse processo separam-se 3 fases:

1.1. A fase anterior às redes eletrónicas

A primeira vez que o suporte eletrónico foi introduzido numa previsão normativa, embora convencional, foi em 1978, nas Hamburg Rules, que admite a possibilidade de os documentos de transporte por via marítima, designado

[101] A confiança dos agentes económicos na utilização das tecnologias eletrónicas é o fundamento da criação do direito da assinatura eletrónica. Como se refere na exposição de motivos da proposta de regulamento sobre a identificação eletrónica, da CE, *"Criar confiança no ambiente em linha é fundamental para o desenvolvimento económico"*; COM(2012) 238 final, ponto 2 da Exposição de Motivos.

conhecimento de embarque (*bill of lading*), serem assinados por meios eletrónicos.[102] Em 1977 a Convenção para Facilitação do Tráfego Marítimo Internacional admitiu os suportes eletrónicos, sob a condição de se apresentarem em forma legível.[103]

O Protocolo de Montreal admitia a sua utilização no transporte aéreo desde que se garanta a sua conservação.[104]

A primeira vez que os suportes eletrónicos são referidos em textos relativos a procedimentos administrativos, foi na recomendação do CCA, de 16 de junho de 1981, relativa à declaração aduaneira de bens por meios eletrónicos.[105]

A UNCITRAL desenvolveu um papel fundamental na construção do direito da assinatura eletrónica, que se iniciou em 1985, com o relatório do Secretário-Geral acerca do valor jurídico dos documentos eletrónicos.[106] Esse relatório exorta os estados, para o que releva do nosso tema, a: [107]

i) Eliminarem entraves legais à admissibilidade da prova efetuada através dos registos eletrónicos;[108]

ii) Eliminarem entraves legais à utilização dos registos eletrónicos nos procedimentos administrativos.[109]

iii) Analisem os requisitos de autenticação dos registos eletrónicos;[110]

Embora não existissem soluções conhecidas para estabelecer um mínimo de requisitos observáveis, para a validade e a eficácia jurídica dos documentos eletrónicos,

[102] United Nations Convention on the International Carriage of Goods by Sea", 1978, Hamburg, 31 March 1978, citado em A/CN.9/221, pág. 20.
[103] Parte final do ponto 2.15 do Anexo I, introduzido em novembro de 1977 da Convention on Facilitation of International Maritime Traffic, disponível em http://www.ifrc.org/Docs/idrl/I258EN.pdf (consulta em 26/5/2015).
[104] N.º 2 do artigo 5.º da Convention For The Unification Of Certain Rules For International Carriage By Air, na versão constante da emenda do art.º III do Protocolo de Montreal, de 25/9/1975. Disponível em http://nasamer.ku.edu.tr/sites/nasamer.ku.edu.tr/files/mevzuat/conventions/montreal-convention.pdf (consulta efetuada em 26/5/2015).
[105] A/CN.9/221, pág. 21.
[106] A proposta de resolução consta como conclusão a esse relatório. "A/CN.9/265", pág. 24.
[107] A recomendação está disponível em http://www.uncitral.org/pdf/english/texts/electcom/computerrecords-e.pdf (consulta efetuada em 20/6/2015).
[108]Disponível em http://www.uncitral.org/pdf/english/texts/electcom/computerrecords-e.pdf (consulta efetuada em 20/6/2015).
[109] *"to review legal requirements that documents for submission to governments be in writing and manually signed with a view to permitting, where appropriate, such documents to be submitted in computer-readable form to those administrative services which have acquired the necessary equipment and established the necessary procedures".* http://www.uncitral.org/pdf/english/texts/electcom/computerrecords-e.pdf (consulta efetuada em 20/6/2015).
[110]Disponível em http://www.uncitral.org/pdf/english/texts/electcom/computerrecords-e.pdf (consulta efetuada em 20/6/2015).

a sua utilização pela atividade económica já se havia expandido e tornado irreversível.[111]

1.2. O EDI e as redes fechadas

Foi o EDI, pela sua importância na atividade das empresas, que desencadeou o movimento legiferante em matéria de assinaturas eletrónicas.

1.2.1. O Relatório TEDIS da Comissão Europeia

O Relatório TEDIS é o primeiro documento produzido pela então Comunidade Económica Europeia que inventaria os constrangimentos legais à generalização da utilização da tecnologia EDI.[112] O seu objetivo é o de promover a sua eliminação.[113]

Analisando o quadro legal dos diversos países, enunciam-se como obstáculos legais a exigência legal de forma escrita, a necessidade de assinatura e do seu reconhecimento, e ainda os requisitos de forma, nomeadamente para fins probatórios e para efeitos administrativos e fiscais.[114]

Essas exigências advinham da durabilidade do papel, que permitia manter registo para o futuro, das declarações negociais, bem como verificar eventuais alterações e determinar com rigor a data e o local de celebração dos contratos.[115]

---

[111] Como se refere logo no primeiro considerando da recomendação, a Comissão havia *"Noting that the use of automatic data processing (ADP) is about to become firmly established throughout the world in many phases of domestic and international trade as well as in administrative services".* http://www.uncitral.org/pdf/english/texts/electcom/computerrecords-e.pdf (consulta efetuada em 20/6/2015).

[112] Esse propósito era enunciado no próprio documento. *"The study contributes to 'research into legal issues which might hinder the development of trade EDI and to ensuring that regulatory constraints in matters of telecommunications should not impair the development of trade EDI'".* E mais adiante: *"The legal obstacles which could frustrate development of European EDI are many and varied"*. "TEDIS Report", pág. 39.

[113] *"Europe continues to lag relatively far behind in this respect, particularly by comparison with the United States of America"*. "TEDIS Report", pág. 31.

[114] *"The key legal obstacles to EDI result from the priority accorded to written document in Member States national law, and the concommitant requirement in national law to prepare, issue, send and store documents in signed hard-copy form, either to ensure compliance with provisions in respect of validity or negotiability of the document per se, or for reasons of accounting or fiscal regulations or for use as evidence."* "TEDIS Report", pág. 32.

[115] *"To fulfil a function comparable to writing, a computerized record must be capable of being a stable and durable medium - to satisfy the need for perpetuation - and reliable and unalterable to satisfy the need for security"*. "TEDIS Report", pág. 304.

Conclui que são esses os principais atributos que a tecnologia deve garantir aos documentos gerados e comunicados por via eletrónica.

1.2.2. A Lei Modelo do Comércio Eletrónico (LMCE)

A LMCE foi elaborada como resposta à necessidade de segurança jurídica na utilização do EDI, mas ela é o primeiro instrumento normativo com a ambição de criar um regime jurídico aplicável às transações eletrónicas, conferindo-lhe o mesmo nível de segurança, validade e eficácia das transações documentadas em suporte de papel.[116] O projeto de LMCE foi concluído pela UNCITRAL em 1993.[117]

A LMCE consagrou os conceitos jurídicos fundamentais do direito da segurança eletrónica, nomeadamente os seguintes:

i) De mensagem eletrónica.[118] Trata-se do conceito de base do posterior conceito de documento eletrónico, ainda influenciado pela designação da tecnologia EDI então dominante.[119] Mas é um conceito fundamental para o reconhecimento da validade e eficácia jurídicas dos suportes eletrónicos.[120]

ii) O reconhecimento expresso da validade e da eficácia jurídica das mensagens eletrónicas;

iii) A equivalência das mensagens eletrónicas a documentos escritos e a originais;

iv) A equivalência das mensagens eletrónicas aos requisitos de conservação e arquivo dos documentos em papel;

---

[116] É em 1992 que os textos da UNCITRAL referem, pela primeira vez, a necessidade de se regularem os aspetos jurídicos do EDI. *"The time might now be appropriate for considering the preparation of detailed rules regarding some other aspects of the use of EDI"*. "A/CN.9/360", par. 24.

[117] O projeto faz parte do A/CN.9/387 e seria revisto e apresentado em A/CN.9/WG.IV/WP.60.

[118] Como refere a UNCITRAL, *"The fundamental issue at the heart of all aspects of the legal admissibility of digitally transmitted and processed data and information is that of the legal reliability of information and communication technology"*. "A/CN.9/333", par. 58.

[119] *"Among the means of communication encompassed in the notion of "electronic commerce" (...): communication by means of EDI defined narrowly as the computer-to-computer transmission of data in a standardized format; transmission of electronic messages involving the use of either publicly available standards or proprietary standards; transmission by electronic means of free-formatted text"*. A/CN.9/373, par. 12.

[120] Como se refere num estudo do Ministério das Finanças Britânico, citado pela UNCITRAL, *"Identification, verification and authentication technologies and techniques which are, or may become, as legally acceptable as the conventional trust and comfort of a manual signature written in ink on paper'"*. "A/CN.9/333", par. 58.

v) A abrangência a todos os tipos de tecnologias eletrónicas e não apenas ao EDI, [121] estabelecendo o princípio da neutralidade tecnológica.[122] [123]

1.2.3. O papel de outras organizações internacionais

A relevância do EDI para a atividade económica fez envolver várias organizações internacionais de caráter empresarial a estudarem a adoção de soluções que promovessem a utilização desta nova tecnologia nas respetivas atividades comerciais, mediante a celebração de convenções.[124]

Merecem referência, em especial, os trabalhos da CCC, do CMI da CIT (que criou o título de transporte ferroviário eletrónico), do IRU (título de transporte rodoviário eletrónico), bem como da ABA.

No que respeita às relações administrativas, releva a importância do Guia CCC, de comunicação eletrónica de dados entre as empresas e as administrações aduaneiras. Trata-se da primeira convenção de cumprimento de obrigações de natureza administrativa por via eletrónica.[125]

1.3. A fase das redes abertas

A emergência das redes abertas aumentou as exigências de segurança jurídica dos suportes eletrónicos, em face dos fatores acrescidos de insegurança a que já nos referimos. É nesse contexto que nasce a assinatura digital, em 1990.

---

[121] Embora a definição de EDI adotada pelo projeto seja muito reduzida (*'EDI', means the computer-to-computer transmission of business data in a standard format"*), a definição de dados negociais eletrónicos é mais abrangente, sendo esse o âmbito de previsão do projeto. *"'Trade data message' means a set of trade data exchanged (or stored)by means of electronic data exchange (EDI), telegram, telex, telecopy or other (analogous) means of teletransmission (or storage) of (digitalized) data, (to the exclusion of purely oral communication) which (inherently) provides a complete record of data"*. "A/CN.9/387", par. 29.

[122] *"No communication technique is excluded from the scope of the Model Law since future technical developments might need to be accommodated"*. A/CN.9/WG.IV/WP.64, par. 31.

[123] *"The objectives of the Model Law, which include enabling, or facilitating, the use of EDI and related means of communication and providing equal treatment to users of paper-based documentation and to users of computer-based information".* "A/CN.9/426", par. 24.

[124] Para uma análise exaustiva dos trabalhos efetuados e das organizações intervenientes, "A/CN.9/350".

[125] "A/CN.9/350", par. 64.

1.3.1. A emergência da assinatura digital

No início da década de 1990 emergiu a tecnologia das assinaturas digitais, concebida especificamente para corresponder às necessidades de segurança jurídica dos suportes documentais eletrónicos. Os documentos da UNCITRAL referem-se a ela pela primeira vez em 1990, relevando a utilização da criptografia e de chaves de encriptação e de desencriptação.[126] Em 1992 eram referidas como *"complexas assinaturas digitais"*, que permitiam verificar *"tanto a fonte das mensagens eletrónicas, como a conformidade da mensagem recebida com a mensagem emitida"*.[127] Em 1993 a tecnologia da assinatura digital é referida como instrumento de autenticidade, de integridade e de não repúdio.[128]

Em 1996 foi efetuada uma apresentação técnica ao grupo de trabalho que elaborou a LMCE.[129] O relatório dessa sessão refere-se à assinatura digital como o resultado combinado de *"códigos matemáticos"* que garantem a autenticação, a integridade e o não repúdio das mensagens eletrónicas.[130] Apesar disso, era ainda escasso o conhecimento da nova tecnologia no ano de 1996, quando o tema foi retomado.[131] E desde logo se assumiu que a importância da assinatura para a segurança jurídica eletrónica,[132] incluindo no que respeita aos títulos negociáveis.[133]

---

[126] Esta primeira referência é a seguinte: *"An algorithm can be used for the coding of the text, the reading of which requires application of the corresponding decoding key"*. E mais adiante:*"Techniques combining several keys can also be used as a means of identifying the operator of the sending machine"*. "A/CN.9/333", par. 54.

[127] O documento acrescentava: *"The methods ranged from a technically simple verification of the address of the owner of the computer that had sent or received a message to sophisticated "digital signatures". Some of those methods were designed to verify only the source of the message, while others could verify both the source of the message as well as whether the message received was identical to the message sent"*. "A/CN.9/360", par. 114.

[128] O conceito de integridade é apresentado do seguinte modo: *"This technique involves the partial or total encryption of a message in order to verify that it is from the purported sender and that it has not been altered, and could be used by the recipient to prevent the sender from denying transmission of the message"*. "A/CN.9/WG.IV/WP.55", par. 68.

[129] É assim descrita essa apresentação: *"The Working Group heard a presentation on "digital signatures", i.e., mathematical codes used in electronic communications in order to ensure: that a particular data message originated from a particular person (authentication function); that the data message had not been altered since its creation and transfer (verification of integrity function); and that the recipient could not alter the message received (non-repudiation function)"*. "A/CN.9/421", par. 49.

[130] Essa asserção é apresentada do seguinte modo:*"The digital signature was the result of a combination of a mathematical code created by the originator to secure the uniqueness of a particular message and of the private and public keys of the originator"*. "A/CN.9/421", par. 51.

[131] A necessidade de obter conhecimento das assinaturas eletrónicas era reconhecida pelo grupo de trabalho. *"With a view to providing more information to the Working Group as to how digital signatures and various other authentication techniques might operate, a number of presentations of a technical nature were made"*. A/CN.9/446, par. 88. Do mesmo modo,*"The Working Group considered the*

Em 1996 foi criado um grupo de trabalho específico para estudar e elaborar um possível regime jurídico das assinaturas digitais.[134] Em 1997, foi apresentado o primeiro estudo preliminar.[135]

Ainda no ano de 1997 é apresentado o primeiro esboço de um regime jurídico da assinatura eletrónica.[136] Estabelecia-se, entre outros, os princípios jurídicos fundamentais, uma graduação da eficácia e dos efeitos jurídicos dos vários tipos de assinaturas, um conjunto de normas que regulavam as relações jurídicas emergentes da autenticação dos documentos eletrónicos entre o emissor e o destinatário, e também a previsão do regime de responsabilidades dos prestadores de serviços de certificação.[137] Essa rapidez na apresentação deste primeiro esboço revela a importância e a urgência que então se fazia sentir na aprovação de uma lei modelo da assinatura eletrónica.[138] Nesse contexto temporal haviam já sido publicadas as Guidelines da ABA e o estado do Utah havia já publicado a sua lei sobre assinatura digital.[139] A proliferação legislativa era já uma das preocupações da UNCITRAL, em especial pelos efeitos da adoção de

---

functioning of possible security devices and mechanisms, such as the use of time-stamping, cryptography, access keys, and digital signature". "A/CN.9/421", par. 78.

[132]Nos termos seguintes: *"The establishment of digital signature laws, together with laws recognizing the actions of "certifying authorities" (hereinafter referred to as "certification authorities"), or other persons authorized to issue electronic certificates or other forms of assurances as to the origin and attribution of messages "signed" digitally, was regarded in many countries as essential for the development of electronic commerce"*. A/CN.9/WG.IV/WP.71, par. 2.

[133] Era assim referida a importância da assinatura digital neste domínio: *"It was pointed out that the ability to rely on digital signatures would be a key to the growth of contracting as well as the transferability of rights to goods or other interests through electronic media"*. "A/CN.9/WG.IV/WP.71", par. 2.

[134] Esta proposta foi adotada no relatório da mesma sessão em que o Grupo de Trabalho sobre o Comércio Eletrónico assistiu, pela primeira vez, a uma apresentação acerca da assinatura digital. *"Among the topics possibly to be considered for future work by the Commission in the area of electronic communications, the Working Group considered the following: possible standards for digital signatures; issues of registries; incorporation by reference; rights and obligations of service providers; and review of existing international conventions"*. "A/CN.9/421", par. 109.

[135] Esse estudo vem anexo ao documento "A/CN.9/WG.IV/WP.71", Op. Cit.

[136] A/CN.9/WG.IV/WP.73.

[137] Era assim delimitado o primeiro âmbito de abrangência do projetado regime: *"The Uniform Rules might (...)be restructured in three parts as follows: (a) an introduction acknowledging the principle of party autonomy; (b) a set of rules dealing with the relationship between parties communicating with each other (based on the presumptions and liability provisions currently contained in the Uniform Rules); and (c) a set of provisions dealing with the liability of service providers that undertake to assist in the identification of parties in an electronic environment"*. A/CN.9/454, par. 137.

[138] Uma enunciação de outros países onde essa legislação foi publicada consta da nota 15 do reporte "A/CN.9/630/Add.2".

[139] As Guidelines da ABA são reportadas pelo grupo de trabalho. *"Moreover, the study draws on the work of other organizations, in particular the draft Uniform International Authentication and Certification Practices being prepared by the International Chamber of Commerce (ICC) and the Digital Signature Guidelines published by the American Bar Association"*. "A/CN.9/WG.IV/WP.71", par. 10.

regimes jurídicos diversos em cada país.[140] Preocupavam os prejuízos resultantes dessa diversidade de regimes jurídicos para o comércio internacional.[141]

1.3.1.1. A lei do Utah, de 1995

A Lei do Utah é a primeira que consagra a assinatura digital como o modelo de assinatura eletrónica, estabelecendo também o princípio da equivalência funcional entre a assinatura digital e a assinatura manuscrita. Como estabelece o seu n.º 46-3-402, *"Um documento assinado digitalmente é tão válido como se tivesse sido escrito em papel"*.[142] A associação dos efeitos da assinatura eletrónica ao da assinatura manuscrita foi a forma pragmática de conferir confiança nas transações eletrónicas e de promover a sua utilização generalizada.

São definidos, pela primeira vez num instrumento legislativo, os conceitos relacionados com a assinatura eletrónica, adota-se assinatura digital como a assinatura eletrónica legalmente reconhecida, o princípio da equivalência funcional com a assinatura manuscrita e a regulação da atividade dos prestadores de serviços de certificação.

A Lei do Utah tem, porém, a limitação de só dar relevo jurídico às assinaturas digitais, excluindo a relevância jurídica das restantes formas de assinatura, nomeadamente das palavras passe e dos métodos biométricos.

---

[140] *"The widespread use of digital signatures and the risk that diverging legislative approaches be taken in various countries with respect to digital signatures may suggest that uniform legislative provisions are needed as a specific legal framework for that authentication technique"*. "A/CN.9/WG.IV/WP.71", par. 47.

[141] Essa preocupação era já reportada no relatório de 1999, que assinalava já ter conhecimento da publicação de leis reguladoras do regime jurídico das assinaturas eletrónicas na Alemanha, em 1997, em Singapura, em 1998, e nos estados do Illinois (1998), Minnesota (1997) e Missouri (1998), dos EUA. *"Drawing on the many legislative instruments already in force or currently being prepared in a number of countries, these draft provisions aim at preventing disharmony in the legal rules applicable to electronic commerce"*. "A/CN.9/WG.IV/WP.88", par. 13. Esta preocupação era particularmente sensível para a UNCITRAL, cuja missão era a adoção de medidas de uniformização legislativa que facilitassem e promovessem o comércio internacional. *"The objectives of the Model Law, which include enabling or facilitating the use of electronic signatures and providing equal treatment to users of paper-based documentation and users of computer-based information, are essential for fostering economy and efficiency in international trade"*. "A/CN.9/WG.IV/WP.88", par. 5.

[142] Este documento está disponível em http://www.jus.unitn.it/users/pascuzzi/privcomp97-98/documento/firma/utah/udsa.html, (última consulta efetuada em 29/2/2016).

1.3.1.2. A lei italiana de 1997

Em 15/3/1997 foi publicada em Itália a primeira lei que regula os *"Atos, contratos e documentos em forma digital"*, que se refere à assinatura digital, definindo-a como *"il risultato della procedura informatica che rende manifesta e consente di verificare la riferibilità soggettiva e l´integrità di un documento informatico o di un insieme di documenti informatici"*,[143] uma formulação muito próxima da que havia sido adotada na Lei do estado do Utah e muito inspirada nas Guidelines da ABA. É uma lei pioneira em toda a Europa, definindo também o conceito de assinatura digital e de documento eletrónico.

Do mesmo modo que a Lei do estado do Utah, consagra-se a assinatura digital como a assinatura eletrónica na respetiva ordem jurídica e estabelece a equivalência com a assinatura manuscrita, considerando também que os documentos eletrónicos assinados com a assinatura digital possuem a mesma validade e eficácia jurídicas dos assinados com a assinatura manual (art.º 10º).

1.3.1.3. A lei alemã de 1997

A Alemanha publicaria a sua Lei Federal de assinatura eletrónica em 1 de Agosto de 1997.[144] Essa lei está contida na *Lei que Estabelece as Condições Gerais de Informação e Serviços de Comunicações (Informations und Kommunikationsdienste-Gesetz)* e adota também a assinatura digital como o modelo de referência para a assinatura eletrónica.

A lei define a assinatura digital, designando-a de "carimbo" ou "selo", gerado pela aplicação de uma chave privada que garante a identidade do titular da assinatura e a integridade dos dados (§ 2, (1), do art.º 3.º), uma definição muito próxima da assinatura digital, que exclui do regime legal todas os restantes tipos de assinatura.[145]

---

[143] Este importante documento está disponível no site http://www.marcosdacosta.adv.br/ (última consulta efetuada em 21/7/2014).

[144] Lei da Assinatura Digital de aprovada pela Lei Federal de 1/8/1997 (Signaturgesetz Sigg).

[145] A redação é a seguinte: *"For the purposes of this Act "digital signature" shall mean a seal affixed to digital data which is generated by a private signature key and establishes the owner of the signature key and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority or the authority according to §3 of this Act."*. Tradução para inglês disponível em http://germanlawarchive.iuscomp.org/?s=digital+signature+act&submit= (última consulta efetuada em 28/1/2016).

Outro instrumento estrutural da legislação alemã era o da configuração formal do sistema de geração das chaves privadas que são utilizadas na assinatura dos documentos eletrónicos. A lei estabelece um controlo administrativo da emissão dos certificados de assinatura eletrónica e das chaves privadas, centrando numa autoridade pública as competências de emissão de licenças de autorização do exercício da atividade pelos prestadores de serviços de certificação (§ 3.º).[146]

Esta relevância pública do sistema de geração de chaves privadas e certificados seria revertida na legislação posterior à Diretiva 1999/93/CE, mas correspondia já a uma opção que abriria um debate acerca da natureza, pública ou privada, dos sistemas de identificação eletrónica.

1.3.1.4. A lei portuguesa de 1999

No dia seguinte ao da publicação da lei alemã, é publicado em Portugal o Decreto-Lei n.º 290-D/99, de 2 de Agosto, que aprova o regime jurídico do documento eletrónico e da "*assinatura digital*". A lei portuguesa tem uma inovação relativamente àquelas que anteriormente citámos, ao distinguir entre assinatura eletrónica e assinatura digital. As definições desses conceitos, constantes das alíneas b) e c) do art.º 1.º, não são substancialmente diferentes, mas é de relevar a perfeição da definição do conceito de assinatura digital, próximo das *Guidelines* e dos trabalhos que decorriam na UE, tendentes à uniformização do regime jurídico da assinatura eletrónica no espaço Europeu.

A lei portuguesa restringe a eficácia do princípio da equivalência funcional à assinatura digital, considerando que só os documentos com esse tipo de assinatura produzem os mesmos efeitos dos que são assinados com assinatura autografa, nos termos do seu art.º 7.º, e do n.º 3 do art.º 3.º, na versão original. O carácter restritivo desta equiparação retirou eficácia à lei e não permitiu a expansão da utilização da assinatura eletrónica em Portugal, porque não foram criadas as condições necessárias para a emissão dos indispensáveis certificados de assinatura eletrónica.

[146] Essa entidade seria a *"regulatory authority for telecommunications and posts"*, dependente do governo federal (§ 66 da Telekommunikationsgesetz, TKG). Versão em inglês disponível em http://germanlawarchive.iuscomp.org/?s=telecommunications+act&submit=#66 (última consulta efetuada em 28/1/2016).

Na verdade o art.º 8.º determinava, e bem, que quem pretendesse utilizar uma assinatura digital deveria possuir, além de um par de chaves assimétricas, um *"certificado da respetiva chave pública emitido por entidade certificadora credenciada nos termos do presente diploma"*.

Esta norma continha uma terminologia menos rigorosa, dado que o certificado não é apenas da chave pública, mas do par de chaves, como o mesmo diploma legal determinava na alínea p) do art.º 2.º, onde se definia certificado como "*o documento eletrónico que liga os dados de verificação da assinatura ao seu titular e confirma a identidade desse titular*".[147]

O problema é que a lei não viria a permitir que se se emitissem certificados eletrónicos nos termos nela previstos, porque a autoridade credenciadora que haveria depois de habilitar as entidades certificadoras a prestarem os seus serviços só viria a ser criada em 2006 pelo Decreto-Lei n.º 116-A/2006, de 16 de Junho, que no seu art.º 8.º estabeleceu que essa entidade é a Autoridade Nacional de Segurança. Antes disso havia sido designada autoridade de credenciação o Instituto das Tecnologias de Informação da Justiça pelo Decreto-Lei n.º 234/200, de 25 de Setembro, mas por falta de condições técnicas e de regulamentação, não exerceu efetivamente essas funções.

Na versão inicial do Decreto-Lei n.º 290-D/99, de 2 de Agosto, o exercício da atividade de prestação de serviços de certificação dependia de autorização administrativa emitida pela autoridade de credenciação, um regime que mais tarde viria a ser abandonado.

Este carácter restritivo da equivalência apenas à assinatura digital, praticamente impediu a sua aplicação no nosso país, valendo apenas a utilização de certificados emitidos por entidades não residentes, por força da equivalência internacional constante do art.º 37.º do referido Decreto-Lei.

A lei portuguesa, assente na dualidade entre a assinatura eletrónica e a assinatura digital, permitia ainda que outros "*meios de comprovação da autoria e integridade de documentos eletrónicos*" (n.º 4 do art.º 3.º) servissem para autenticar documentos eletrónicos, passando a existir, na verdade, não dois mas três tipos de assinatura eletrónica – a digital, a eletrónica e os restantes meios de comprovação da autoria e da integridade dos documentos. Esta distinção só tinha importância para a assinatura digital, porque só os documentos assinados com ela eram suscetíveis de

[147] A redação do artigo 8.º viria depois a ser alterada pelo DL n.º 62/2003, de 3/4, que passou a falar apenas em certificado, sem se referir já à chave pública.

possuir a força probatória prevista no art.º 376.º do Código Civil (n.º 2 do art.º 3.º). Quanto aos restantes documentos eletrónicos, a sua força probatória seria apreciada nos termos gerais (n.ºs 4 e 5 do art.º 3.º). Não tinha, pois nenhuma especificidade nesta lei a chamada assinatura eletrónica.

1.3.1.5. A lei espanhola de 1999

A lei espanhola foi publicada em 17 de Setembro de 1999, definindo, pela primeira vez, dois tipos de assinaturas eletrónicas – a assinatura eletrónica e a assinatura eletrónica avançada. Esta diferenciação refletia já os trabalhos de preparação da Diretiva 1999/93/CE que viria a consagrar essa distinção.

Esta distinção destinava-se a admitir no âmbito do regime jurídico da assinatura eletrónica outros tipos de assinatura eletrónica que não a digital, como era o caso das estantes que antes enunciámos. Foi por essa razão que a lei espanhola passou a considerar assinatura eletrónica avançada a assinatura digital e assinatura eletrónica os restantes tipos de que falámos atrás.[148]

Com essa distinção a lei espanhola equiparou os documentos assinados com assinatura eletrónica avançada aos documentos assinados em papel e deixou sujeitos às regras da livre apreciação da prova os restantes documentos eletrónicos, tendo porém, o cuidado de prever que não se negarão efeitos jurídicos a um documento só pode facto de possuir uma assinatura eletrónica, qualquer que ela seja, só pelo facto de ser eletrónica (n.º 2 do art.º 3.º do Real Decreto-Lei 14/99, de 17 de Setembro).

1.3.1.6. A lei inglesa de 1999

Em 18 de Novembro de 1999 é publicada em Inglaterra a *Electronic Comunications Bill*, que define no seu n.º 7 que a assinatura digital é a modalidade consagrada de assinatura eletrónica, e que confere validade jurídica aos documentos eletrónicos assim assinados idêntica à dos documentos em papel com assinatura manuscrita.

[148] Era também essa distinção que o legislador português pretendia consagrar com a distinção entre assinatura eletrónica e assinatura digital, mas, como se viu, não foi esse o resultado que se veio a produzir.

1.3.2. O trabalho de harmonização das organizações internacionais

O direito da assinatura eletrónica nasceu no seio das instâncias de harmonização jurídica do comércio internacional, primeiro numa base convencional, mas rapidamente evoluiu com a criação de normas gerais na legislação nacional. Essa produção legislativa é sequencial à tecnologia da assinatura digital, que resulta da associação do conhecimento jurídico, matemático e tecnológico.

As organizações internacionais desenvolveram também um importante trabalho na harmonização dos regimes jurídicos nacionais de assinatura eletrónica.

1.3.2.1. As *Guidelines* da American Bar Association (ABA)

A American Bar Association (ABA), uma associação americana de advogados e juristas, publicou, em 1 de Agosto de 1996, as *Guidelines* da assinatura digital. Trata-se do primeiro trabalho jurídico sobre assinaturas eletrónicas, que descreve o modo de funcionamento da assinatura digital, incluindo a definição de todos os conceitos jurídicos necessários à construção dos sistemas jurídicos de assinatura digital, e a sua capacidade de produzir confiança e segurança jurídica nas transações efetuadas por meios eletrónicos.[149] Foi nas *Guidelines* que os primeiros documentos legislativos internacionais se fundaram.

1.3.2.2. As Diretrizes sobre Política Criptográfica da OCDE

Em Março de 1997 a OCDE publicou o Relatório com as Diretrizes sobre Política Criptográfica em que recomenda aos Estados a adoção de legislação que regule

[149] Esse documento foi publicado e tinha como título "*Digital Signature Guidelines*", e por objetivo *"facilitar as discussões conducentes ao desenvolvimento de uma legislação adequada e boas práticas em matéria de assinaturas digitais como uma ferramenta que conduza ao comércio eletrónico seguro."*American Bar Association; "Digital Signature Guidelines", pág. 23. Disponível em http://www.americanbar.org/content/dam/aba/events/science_technology/2013/dsg_tutorial.authcheckdam.pdf (última consulta em 20/7/2015).

de forma harmonizada em termos tecnológicos os regimes de assinatura eletrónica.[150] Nele se analisa, de forma detalhada, a importância da informação nas sociedades modernas e da harmonização dos regimes de assinatura eletrónica para a economia internacional.[151]

A OCDE recomenda a todos os países a adoção da assinatura digital como referência central no regime legal de assinatura eletrónica, na mesma linha das iniciativas correntes nessa época, como era o caso das Guidelines da ABA.

1.3.2.3. A diretiva europeia da assinatura eletrónica

Em 13 de Dezembro de 1999 foi aprovada a Diretiva 1999/93/CE do Parlamento e do Conselho sobre Assinatura Eletrónica, estabelecendo importantes princípios que iriam ser determinantes na configuração da legislação dos países da União, bem como no seu exterior, nomeadamente os seguintes:

1. - A segmentação de três tipos de assinatura eletrónica diferenciados – a assinatura eletrónica, a assinatura eletrónica avançada e a assinatura eletrónica qualificada, correspondendo a primeira à assinatura digitalizada e às palavras-passe, bem como às assinaturas assentes em dados biométricos, e a assinatura eletrónica avançada à assinatura digital. A assinatura eletrónica qualificada é uma construção jurídica destinada a garantir os mais elevados níveis de segurança jurídica. Esta segmentação resulta de duas circunstâncias fundamentais:

a. A necessidade de conferir validade jurídica a todos os tipos de assinatura eletrónica e não apenas da assinatura digital, em face da expansão, que havia ocorrido, da assinatura digitalizada e das palavras-passe, que as legislações anteriores excluíam, por só admitirem a assinatura digital;

b. A necessidade de eliminar a obrigatoriedade de sujeição a autorização administrativa a autorização para o exercício da atividade dos prestadores de serviços de certificação, tornando-a de livre acesso;

[150] Este documento está disponível em http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm (última consulta efetuada em 21/7/2015).

[151] Lê-se, nomeadamente, no 2.º par. do n.º 1 do Relatório que "*O fluxo livre da informação é um elemento fundamental da democracia*".

2. – O princípio da equivalência funcional entre a assinatura eletrónica qualificada e a assinatura manuscrita reconhecida por notário, com o mais elevado nível de fé pública;

3. – A não discriminação negativa das restantes assinaturas eletrónicas, garantindo-se que em caso algum uma assinatura seja considerada menos válida só pelo facto de estar em forma eletrónica;

4. – A criação de um novo tipo de assinatura eletrónica – a assinatura eletrónica qualificada, que proporciona garantias de segurança e fiabilidade mais elevadas e que, por isso, é equiparada à assinatura manuscrita legalmente reconhecida;

5. – O princípio da equivalência internacional, reconhecendo-se as assinaturas que sejam válidas noutro Estado-Membro e não discriminando as assinaturas eletrónicas certificadas em países fora a União, havendo acordos bilaterais.

6. – O princípio do livre acesso à atividade certificadora por entidades terceiras, que veio romper com uma tendência inversa que constava das legislações europeias anteriores, como era o caso da Alemã, da Espanhola e da Portuguesa (art.º 3.º);

7. - A possibilidade de submissão das empresas privadas que desenvolvam atividades de certificação, a um regime voluntário de reconhecimento de que os serviços que prestam são da mais elevada segurança e qualidade, bem como de controlo. Essa submissão é importante para que essas empresas possam emitir certificados de assinatura eletrónica qualificada;

1.3.2.4. A Lei Modelo da Assinatura Eletrónica (LMAE)

Em Janeiro de 2002 foi aprovada a LMAE, que tinha como objetivos promover o comércio eletrónico incluindo a nível internacional, mediante a utilização das tecnologias eletrónicas, conferindo-lhe relevo jurídico mediante a assinatura eletrónica.[152]

[152] Esses objetivos são enunciados, de forma sintética, no seguinte trecho: *"Amongst the general principles on which the Model Law is based, the following non-exhaustive list may be found applicable: (1) to facilitate electronic commerce among and within nations; (2) to validate transactions entered into by means of new information technologies; (3) to promote and encourage in a technology-neutral way the implementation of new information technologies in general and electronic signatures in particular; (4) to promote the uniformity of law; and (5) to support commercial practice. While the general purpose of the*

A LMAE funda-se em quatro princípios fundamentais:

i) Da neutralidade tecnológica, nos termos do qual se deve deixar aos particulares a liberdade de decisão de utilização de um qualquer tipo de assinatura eletrónica, dando relevo a todos, sem prejuízo das diferenças nos efeitos jurídicos diferenciados em função da segurança e eficácia de cada um desses tipos (art.º 3.º da LMAE);

ii) Da liberdade de convenção, pelas partes, do tipo de assinatura eletrónica para efeitos da sua vinculação jurídica (art.º 5.º da LMAE);

iii) A diferenciação entre assinatura eletrónica em geral e a assinatura que cumpra todos os requisitos de identidade, autenticação, integridade e não repúdio (art.º 6.º da LMAE);

iv) O princípio da equivalência internacional das assinaturas eletrónicas (art.º 12.º da LMAE).

1.3.3. O Regulamento EIDAS

Regulamento EIDAS é um marco legislativo na formação da disciplina jurídica da assinatura eletrónica.[153] Nele se assume, pela primeira vez, o relevo público desse bem jurídico mais importante da disciplina da segurança jurídica eletrónica, que é a confiança.

Enquanto a diretiva de 1999, e a generalidade das iniciativas legislativas que se lhe seguiram, postulavam a segurança jurídica eletrónica no domínio do direito privado, este Regulamento assume essa confiança como um bem jurídico e, além disso, confere-lhe uma natureza de carácter público.

Embora se admita a existência de vários tipos de assinaturas eletrónicas e seja livre o acesso ao mercado da prestação de serviços de certificação eletrónica, faz-se depender a atribuição de eficácia jurídica traduzida na presunção de fiabilidade das assinaturas, no reconhecimento prévio, por parte das entidades de supervisão, que dependem das administrações públicas, de que os prestadores de serviços cumprem os

Model Law is to facilitate the use of electronic signatures, it should not be construed in any way as imposing their use". "A/CN.9/WG.IV/WP.88", par. 109.

[153] Regulamento Europeu Relativo à Identificação Eletrónica e aos Serviços de Confiança para as Transações Eletrónicas no Mercado Interno, que designaremos doravante como Regulamento EIDAS.

requisitos legais de segurança e que os dispositivos de criação das assinaturas são certificados.

Por outro lado são criados e regulados novos serviços de segurança jurídica eletrónica, que vão para além da assinatura eletrónica, como são o caso dos selos eletrónicos das entidades coletivas, públicas e privadas, que constituem uma espécie de assinatura eletrónica destas entidades, bem como dos serviços de entrega e de correio eletrónico certificado, da certificação dos *sites* e da criação dos selos temporais.

A relevância pública do sistema de assinatura eletrónica e dos meios de segurança jurídica e confiança nos meios eletrónicos corresponde a um progressivo reconhecimento da importância das redes eletrónicas, e em especial da Internet como um espaço público e de exercício da cidadania ao ponto de se considerar esse acesso como um direito de todos os cidadãos. Nessa linha, o direito à identificação eletrónica assume uma relevância próxima do direito à identificação presencial ou nas relações estabelecidas em suporte de papel.[154] A identificação dos cidadãos e a prestação dos serviços de confiança nos meios tradicionais de identificação é uma função de relevância pública, assumida pelos órgãos próprios da administração, incluindo os serviços de registo e de identificação. A expansão da utilização das redes eletrónicas à generalidade das dimensões da vida em sociedade transporta para o domínio público a relevância da identificação eletrónica. Do mesmo modo, sendo as redes eletrónicas abertas instâncias abrangentes de expressão das relações sociais, a segurança dos cidadãos na sua utilização, incluindo a segurança jurídica, releva cada vez mais do domínio do interesse público.

O Regulamento não exclui o acesso à prestação de serviços de certificação por parte de agentes privados, sendo esse acesso sempre possível e concorrencial, mas tem carácter inovador a atribuição de funções e de responsabilidades aos órgãos da administração pública em matéria de segurança eletrónica.

2. A criptografia como base de construção da assinatura eletrónica.

[154] A natureza pública do direito de acesso às redes e a sua proximidade dos direitos constitucionais é teorizada em especial em França por Roques-Bonnet, que defende, nomeadamente que *"Parce qu'il conditionne le développement économique autant que le développement personnel, les relations de l'administré avec l' administration autant que la démocratie, l'accès aux infrastrutures du réseau este en passe d'acquérir valeur fondamentale"*. Roques-Bonnet, M.C. (2010). Op. Cit, pág. 403 e 404.

A criptografia é a ciência da encriptação, ou seja da ocultação da informação.[155] Trata-se de um ramo da matemática,[156] historicamente utilizado para garantir o sigilo da informação transmitida através de um canal de comunicação, garantindo apenas o acesso a ela pelo destinatário. [157] [158]

A origem da criptografia perde-se na História, tendo-se desenvolvido em especial para fins militares, nomeadamente para fazer chegar as instruções dos comandos militares à frente de combate.

A criptografia opera mediante algoritmos matemáticos de encriptação que convertem, de forma lógica, a informação em algo ininteligível para quem não conheça a chave que desencripta o documento.[159]

---

[155] A palavra Criptografia *"deriva etimologicamente do grego 'Kriptos', que significa 'oculto' e de 'grafia', que significa 'signo' ou 'escrita', pelo que o seu significado é o de 'escrita oculta'. Por isso podemos definir criptografia como a disciplina que estuda os princípios, métodos e meios de ocultar a informação contida numa mensagem"*. Ruíz, C.B. (2006). Op. Cit., pág. 609. O autor acrescenta que a criptografia é o conceito que se utiliza para se falar da encriptação de dados gráficos alfanuméricos ou imagens, mas que também se podem encriptar dados sonoros ou audíveis, a voz humana e o som, caso em que falaremos de "*criptofonia*". *Ibidem*.

[156] Segundo Perales, *"a criptografia é um ramo da matemática"*. Perales, J.M.A.M. (2005). La Nueva Administración Pública Electrónica, Las Relaciones Electrónicas Entre la Administración y el Ciudadano. Especial Referencia a la Firma Electrónica. Em: Moraleda, J.P., *Administraciones Públicas e Nuevas Tecnologías*. Editorial Lex Nova. Valladolid, pág. 96. Do mesmo modo, Mahillo, S.R.R. (2004). La Seguridad de los Protocolos Criptográficos. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid..

[157] Ortega Diaz define a criptografia do seguinte modo: *"A criptografia é a ciência que se ocupa de transformar mensagens, aparentemente ininteligíveis e devolvê-las ao seu estado original, mediante o uso de chaves ou cifras. O acto de transformar a mensagem em algo ilegível chama-se 'encriptar'; à operação inversa chama-se 'desencriptar'"*. Díaz, J.J.O. Op. Cit., pág. 44. Garnacho define-a como sendo *"a ciência que estuda os princípios, métodos e meios de ocultar o significado de uma mensagem, ou seja, de garantir a sua confidencialidade. O processo que consiste em encobrir a informação (que normalmente requer o conhecimento de uma informação secreta designada 'chave') designa-se cifrar [encriptar], designando-se descifrar [desencriptar] o processo inverso (que, a não ser que se realize de forma fraudulenta, se faz também mediante o conhecimento da mesma ou outra informação secreta [chave]"*. Garnacho, A.R. (2002). Op. Cit., pág. 1316.

[158] Couto Calviño define a *"criptografia moderna como a técnica que se ocupa da protecção de dados mediante a transformação matemática dos mesmos num formato ilegível, mediante a aplicação de algoritmos ou chaves que só são conhecidas pelo emissor e o recetor da mensagem"*. Esta definição é, porém, limitada a uma das formas de criptografia, a chamada criptografia de chave simétrica. Calviño, R.C., (2008). Servicios de Certificación de Firma Electrónica y Libre Competencia. Editorial Comares, Granada, pág. 32.

[159] López Lucena define algoritmo como *"uma sequência finita e ordenada de instruções elementares que, dados os a partir dos valores de entrada de um problema, consegue finalizar e resolver a solução em determinado momento"*. O autor acrescenta, de seguida que *"a criptografia depende, em grande parte da Teoria dos Algoritmos, dado que, por um lado é necessário assegurar que o usuário legítimo, que possui a chave, pode encriptar e desencriptar a informação de forma rápida e cómoda, enquanto que, por outro lado, é necessário garantir que um atacante [terceiro] não disporá de nenhum algoritmo eficiente capaz de comprometer a segurança do sistema"*. López, M.J.L. (2009). Criptografía y Seguridad en Computadores, Versión 4-0,7,53. Universidad de Jaén. Consultado a 2014/07/03 em: http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.Lcripto, pág.s 59 e 60.

2.1. A criptografia de chave simétrica

O algoritmo de encriptação mais antigo e mais conhecido é o chamado *"algoritmo de César"*[160], utilizado pelo imperador romano Júlio César para enviar mensagens às suas legiões em campanha. Esse algoritmo consistia em converter todas as letras de um determinado texto na segunda letra seguinte do alfabeto (um algoritmo matemático que poderíamos representar pela expressão por n+2).[161] Cada letra do texto era substituída por outra, aquela que no alfabeto está duas posições acima. A letra A seria substituída pela letra C, a letra B pela D e assim por diante, de modo que, por exemplo, a palavra "homem", depois de lhe ser aplicado esse algoritmo de encriptação, passaria a ter a configuração de "jqogo". Um documento com este conteúdo poderia circular por qualquer canal de comunicação sem que ninguém pudesse suspeitar que com ele nos estávamos a referir ao conceito de homem. Quando essa palavra assim cifrada chegava ao seu destinatário, este, conhecedor do código de encriptação (o algoritmo matemático n+2), aplicava-o de novo, agora de forma inversa (n-2) sobre o conteúdo codificado e obtinha a palavra original, perfeitamente legível. Se tivéssemos um texto mais extenso, aplicava-se a mesma regra.

A criptografia foi desenvolvida na segunda guerra mundial, em especial pelo exército alemão, que aperfeiçoou a descoberta de Arthur Scherbius, que mecanizou a sua utilização através da máquina "*Enigma*", que encriptava à medida que as letras iam sendo escritas pelo utilizador.[162]O método de encriptação viria a ser descoberto pelos países aliado, já quase no final da guerra.[163]

A criptografia antiga e a que era utilizada na segunda guerra mundial era a chamada criptografia de chave simétrica, em que o autor do texto e o destinatário

---

[160] Calviño, R,C.C.; Op. Cit., pág. 33; Guzmán, A.M. (2004). *Criptografía de Clave Pública.* Em: Ministerio de Economia. Administración Electrónica y Procedimiento Administrativo. Real Casa de la Moneda. Madrid., pág. 214; Garnacho, A.R. (2002). Op. Cit., pág. 1314; Velásquez, R.R., Sau, C.R. e Muñoz, R.M. (2004). *La Firma Electrónica - Aspectos Legales e Técnicos*. Ediciones Experiencia. Barcelona, pág. 179; Ortega Díaz apresenta um extracto da obra de Plutarco "A Vida de Lisandro", onde descreve como Lisandro de Esparta utilizava já um sistema criptográfico rudimentar para enviar mensagens às suas tropas durante a guerra entre Esparta e Atenas no século V a. c. Díaz, J.J.O. Op. cit., pág. 44.

[161] Lopéz de Lucena refere que o algoritmo de César consistia em adiantar não duas, mas três letras do alfabeto a cada letra de um texto ou de uma mensagem. López, M.J.L. (2009). Op. cit.; pág. 128.

[162] Calvo-Sotelo, A.C. e Coello, M.C.L., (2002). Op. cit., pág. 44.

[163] Foi Alan Turing desenvolveu uma máquina que conseguiu essa descodificação, que ficou conhecido como a 'Bomba de Turing'. López, Manuel José Lucena, Op. cit.; pág. 134. A esse propósito Lucena López revela um episódio pouco conhecido mas curioso de Hitler ter oferecido a Franco vinte máquinas ENIGMA, *"que foram utilizadas para comunicações secretas até ao início dos anos de 1950, supomos que para regozijo dos serviços de espionagem britânico e norte-americano"*. *Ibidem*, pág. 135.

partilham o conhecimento da chave de encriptação. Com a mesma chave, o emissor do texto codifica-o (ou encripta-o) e o destinatário descodifica-o (ou desencripta-o).

A segurança do sistema criptográfico depende da capacidade daqueles que partilham o segredo acerca da fórmula da chave, de manterem esse segredo. A vantagem deste método é a sua simplicidade e facilidade de aplicação.

A criptografia de chave simétrica viria a revelar-se falível, porque assenta num segredo que tem que ser partilhado, pelo menos pelo emitente e pelo destinatário, com os riscos correspondentes, que são exponenciados quando se trate de várias pessoas. Por outro lado os atuais sistemas informáticos conseguem, por tentativas sucessivas e automatizadas, descobrir essas chaves. Finalmente a criptografia simétrica exige o estabelecimento de uma convenção criptográfica prévia entre as partes que enviam e recebem mensagens, o que prejudica a sua utilização sempre que as partes não possuam um conhecimento mútuo prévio. Estas limitações não recomendam a utilização deste modelo de encriptação nas redes abertas, como é a Internet.[164]

2.2. A criptografia de chaves assimétricas ou de chave pública

Em 1976, Martin Hellman, e Whitfield Diffie, da Universidade de Stanford publicaram um artigo sob o título *"New Directions in Cryptography"*[165] onde apresentaram uma solução criptográfica inovadora.[166] Através do seu sistema, Diffie e Hellman demonstraram que era possível transmitir uma mensagem encriptada de um emissor para um destinatário, sem necessidade de este último conhecer a chave de encriptação.

Os autores defendiam que seria possível a um destinatário de uma mensagem efetuar a sua desencriptação com uma chave criptográfica que fosse do seu exclusivo conhecimento e sem necessidade de conhecer a chave que a encriptou.

Esta descoberta era inovadora porque assentava em duas chaves, servindo uma para encriptar e a outra para desencriptar.

---

[164] A insegurança da criptografia simétrica é confirmada por Baygual, porque "*não parece ser uma tecnologia adequada para o processo de assinatura, porquanto uma mesma chave pode ter que ser utilizada por uma multiplicidade de pessoas, o que elimina a possibilidade de autenticação e, portanto, o efeito de não repúdio"*. Baygual, F.A. (2002). El Protocol SET. Em: Cremades, J., Ordonhez, M.F.A, Illescas, R. *Régimen Jurídico de Internet*, La Ley. Madrid., pág.s 1284.

[165] Hellman, M. e Diffie, W. (1976). *New Directions in Cryptography*. Consultado a 14/10/2015 em: http://www-ee.stanford.edu/~hellman/publications/24.pdf .

[166] Guzmán, A.M. (2004). Op. Cit., pág. 216; Garnacho, A.R. (2002), pág. 1318.

A outra inovação era a descoberta de que era possível, através de um modelo matemático, estabelecer uma conexão matemática entre duas chaves, de tal forma que além de ser possível a uma desencriptar aquilo que a outra encriptou, ambas as chaves podiam encriptar qualquer documento, e ambas as chaves podiam desencriptar, mas cada uma delas só era capaz de desencriptar aquilo que a outra encriptou.

Suponhamos que uma pessoa (A) necessita de receber mensagens confidenciais de várias pessoas (B, C e D, por exemplo, vários fornecedores de A).

A possibilidade de existirem duas chaves com funções idênticas permite a A guardar para si uma chave, que mantém sempre em segredo e no seu controlo exclusivo (que designaremos por chave privada) e divulgar por cada uma das pessoas de quem recebe essas mensagens (B, C e D), a outra chave, que designaremos então por chave pública, porque passava a ser conhecida dos seus fornecedores.

Quando os fornecedores (B, C ou D) enviam mensagens sigilosas ao destinatário (A), aplicam sobre cada uma delas a chave pública de A. Com essa aplicação, cada mensagem fica encriptada e pode circular por qualquer canal de comunicação, dado que a partir desse momento, só a chave privada de A a pode desencriptar. Partindo do pressuposto de que quem encriptou a mensagem foi B e a enviou assim a A, a partir do momento em que foi efetuada a encriptação, nem B nem C nem D, nem qualquer terceiro, podem desencriptar a mensagem. Ela só poderá ser desencriptada pela chave privada de A. Está assim garantida a confidencialidade.

Isso só é possível porque ambas as chaves estão matematicamente relacionadas, sendo essa relação que assegura que aquilo que uma encripta, a outra desencripta.

A última descoberta destes autores foi a de que uma chave não podia ser descoberta por derivação a partir da outra. Esta descoberta garantia segurança na confidencialidade do documento encriptado.

Estava assim aberta a possibilidade de uma pessoa receber mensagens encriptadas que só ela podia desencriptar, sem que, com isso tivesse que vulnerabilizar o seu segredo acerca da forma de desencriptação. Neste modelo existe segurança de que mais ninguém acede a uma mensagem encriptada.

Este procedimento é seguro porque:

i) Só uma chave pode desencriptar o documento;

ii) Essa chave não necessita de ser partilhada;

iii) Para desencriptar não é necessária a chave de encriptação;

iv) O remetente e o destinatário operam de forma independente;

v) A parte que encripta não consegue descobrir a chave de desencriptação;

vi) Uma mensagem que é encriptada por uma chave, não pode ser desencriptada por essa mesma chave, nem por qualquer outra, a não ser por aquela que está com ela relacionada de forma matemática;[167]

vii) Uma mensagem desencriptada com a chave privada pode voltar a ser encriptada por esta, mas esse processo não é a reversão da desencriptação. O resultado da sua encriptação será diferente do da primeira. E isto ocorre porque ambas as chaves são assimétricas, ou seja, são inversas uma da outra;

viii) Não é possível derivar uma chave a partir da outra. Não é possível ao remetente que aplicou uma chave de encriptação determinar qual é a chave que está matematicamente relacionada com ela, para assim poder voltar a fazer a desencriptação. É certo que ambas as chaves estão matematicamente relacionadas, mas essa relação não é suscetível de ser determinada, descobrindo-se uma chave a partir da outra. Esta foi a descoberta de Diffie e Hellman, que abriu as portas do conhecimento à construção da assinatura digital, como veremos de seguida. Para se estabelecer a relação entre ambas as chaves, são utilizados números primos aleatórios muito grandes que tornam inviável a derivação em tempo útil, mesmo mediante a utilização de tentativas sucessivas com programas informáticos de elevada capacidade computacional. Para isso, atualmente, são usadas chaves de 254 dígitos.[168]

Foram desenvolvidas técnicas matemáticas diferenciadas, que aperfeiçoam a resistência contra a derivação das chaves privadas a partir das chaves públicas, nomeadamente a utilização da criptografia das curvas elípticas.[169] Esta tecnologia, desenvolvida mais recentemente,

---

[167] E se a pessoa que encriptou com a chave pública a tentar usar para desencriptar, consegue reverter o processo ? A resposta a esta questão é crítica, porque se for positiva, não existirá segurança acerca da origem dos documentos. Essa resposta é negativa.

[168] Como afirma Ortega Diaz, "*as chaves assimétricas têm um carácter unidireccional, o que, em síntese, significa que a obtenção de uma das chaves a partir da outra é matematicamente impossível"*. Esta segurança, segundo o Autor *"deriva de uma importante característica dos números primos, segundo a qual, uma vez obtido um produto resultante de uma multiplicação de fatores, constituídos pelos números primos, é impossível determinar, a partir do referido produto quais foram os números primos empregues no cálculo"*. Díaz, J.J.O. Op. Cit., pág. 47.

[169] Que é referida pela UNCITRAL*"Other mathematical techniques are currently used or under development, such as cryptosystems relying on elliptic curves, which are often described as offering a*

reforça a inviabilidade computacional da obtenção da chave privada a partir da chave pública.

2.2.1. O processo de criação das chaves

Ambas as chaves devem ser geradas ao mesmo tempo, porque têm que estar matematicamente relacionadas. O processo da sua criação compõe-se de um conjunto de procedimentos matemáticos, que utiliza operações sobre números primos.[170]

O algoritmo mais utilizado na criação de chaves assimétricas, que segue os princípios da criptografia de chaves assimétricas de Diffie and Helman, foi apresentado em 1977 por Ron Rivest, Abi Shamir e Len Adleman no *Massachusetts Institute of Technology* (MIT), passando a ser conhecido por sistema Rivest-Shamir-Adleman através das iniciais RSA.[171] Desde então, o algoritmo RSA é o mais utilizado na criptografia da chave pública.[172]

Analisamos, de seguida, o processo de criação de um par de chaves assimétricas. O processo de criação utiliza três conceitos fundamentais:[173]

i) Os números primos;[174]

ii) Os números co-primos;[175]

---

high degree of security through the use of significantly reduced key-lengths". A/CN.9/493, par. 39. E mais tarde, *"The concept of public key cryptography, as discussed here, does not necessarily imply the use of algorithms based on prime numbers. Other mathematical techniques are currently used or under development, such as cryptosystems relying on elliptic curves, which are often described as offering a high degree of security through the use of significantly reduced key-lengths"*. A/CN.9/630/Add.1, nota de rodapé 1.

[170] *"The most common algorithms for encryption through the use of public and private keys are based on an important feature of large prime numbers: once they are multiplied together to produce a new number, it is particularly difficult and time-consuming to determine which two prime numbers created that new, larger number"*. "A/CN.9/493", par. 38.

[171] López, M.J.L. (2009). Op.cit., pág. 182.

[172] Stallings, W. (2011). *Cryptography and Netwook Security, Principles and Practice*. 5.ª Edição, Pearso Education, Pearson Hall. New York, pág. 277.

[173] Seguimos a metodologia de Stallings na exposição do processo de criação de chaves Stallings, W. (2011). Op. cit., pág.s 280 e seguintes.

[174] Números primos são números que só são divisíveis por si próprios e pela unidade. Por exemplo o número 7 só pode ser dividido:

i) Por 7, dando 1;

ii) Por 1, dando 7.

Exemplos de outros números primos são o 1, o 2 (o único número primo que é par), o 3, o 5, o 11, o 13, o 17. É claro que podemos dividir o número 7 por 3 e teremos 2, mas sobra 1 como resto. Números primos são os que, sem deixar resto, só são divisíveis por si e pela unidade.

[175] Números co-primos são números cujo único divisor comum entre eles é a unidade. Por exemplo o 6 e o 7. O seis é divisível por 2, por 3 e por 1. O 7 é divisível por 1 e por 7. Então o 6 e o 7 têm como único divisor comum a unidade.

iii) A função mod.[176]

A metodologia matemática de criação do par de chaves é um processo que tem os seguintes passos:

1. Em primeiro lugar escolhem-se dois números primos quaisquer. No processo real esta escolha recai em números primos muito extensos, mas no nosso exemplo vamos escolher números pequenos, para mais fácil demonstração. Por isso, escolhemos, por exemplo, o 3 e o 11. Designamos o primeiro por ***p*** e o segundo por ***q***. (p=3 e q=11)

2. De seguida multiplicamos *p* por *q* e calculamos **33.** (p*q é igual a 3*11, ou seja, 33). Desta operação resulta a determinação do coeficiente ***n***.

3. O terceiro passo é o cálculo da **função Euler de Totiente (*n)***, que designamos abreviadamente por **função T(*n*).** Esta função é igual ao resultado da multiplicação de *p*-1 por *q*-1. Ora, *p*-1 é igual a 3-1, que é 2. E *q*-1 é igual a 11-1, que é 10.

Assim, 2 * 10 = 20. **A função T(*n*) é 20**. T(n) = (p-1) * (q-1) = 20.

4. No quarto passo escolhemos o coeficiente ***e***, que deverá ser um número tal que seja simultaneamente co-primo e mais pequeno do que a **função T(*n*)** que acabámos de apurar, ou seja, do que 20. Escolhemos então o 7.[177] Assim, ***e* = 7. Esta é uma das chaves.**

5. O quinto passo destina-se a determinar o coeficiente ***d***. Este coeficiente deve cumprir os requisitos de o resultado da sua multiplicação por ***e*** ser um valor tal, que uma vez dividido por 20, desse um resultado com o resto de 1. Ora, já sabemos que ***e*** corresponde a 7. Sabemos também que a função *mod* corresponde ao resto de uma divisão de um número pelo outro. Assim, o produto da multiplicação de *e* por *d* (7), dividido por 20, deve dar um resto igual a 1. Ou seja, deve cumprir-se a seguinte fórmula: (E * D) mod 20 = 1.

Por exemplo vamos tentar *d* = 2

(7*2) mod 20. Ora, 7*2 = 14. E 14/20 dá como resto 14, pelo que o 2 não obedece à fórmula, dado que não produz um resto igual a 1.

Vamos tentar com *d* = 3

[176] Função *mod* é o resto da divisão de um número pelo outro. Por exemplo, no caso anteriormente referido, em que dividimos 7 por 3 e o resultado é 2, mas sobra 1. A função 7 mod 3 é então 1. A função 8 mod 3 é igual a 2. Se dividirmos 8 por 3 teremos como resultado 2 (8/3=2), sobrando como resto 2. A função 5 mod 2 é 1. Na verdade 5 a dividir por 2 dá 2, mas sobra 1.

[177] Escolhemos o 7, que só é divisível por 7 e por 1. O 20 é divisível por 1, 2, 4 e 5. Assim, dos divisores de 7 e de 20, o único que é comum a ambos é o 1. Por isso, 7 e 20 são números co-primos.

(7*3) mod 20. Ora, 7*3 = 21, e o que nós pretendemos é que (E * D) mod 20 = 1, ou seja, que 21/20 dê resto 1. E é isso que acontece, dado que o resultado dessa divisão é 1, sobrando 1.

Encontrámos, assim, o valor de ***d. D=3.*** Esta é a outra chave.

Temos assim encontradas ambas as chaves.

A primeira chave é ***e,n***, ou seja, **(7,33)** e a segunda chave é ***d,n***, ou seja, **(3,33)**.

2.2.2. Demonstração da operação de encriptação e de desencriptação

Sendo já conhecedores de duas chaves assimétricas muito simples, vamos proceder à demonstração de uma encriptação e de uma desencriptação.

Devemos anotar que com uma chave vamos alterar o teor de um documento e com outra, que é diferente, vamos retroceder essa operação. A importância da descoberta de Diffie e Hellman está nessa possibilidade de os métodos de conversão da informação, que na verdade são as chaves, serem diferentes, mas uma fazer regredir ao conteúdo original aquilo que a outra alterou, e essas chaves não serem iguais, nem se poderem deduzir uma da outra.

Vamos considerar um documento que tem apenas o texto "8". Designaremos este texto original por "M". Vamos proceder à sua encriptação. Após a encriptação, teremos o produto encriptado, que designaremos de "C".

Para proceder à encriptação utilizaremos a primeira chave que encontramos, a chave (7,33).

Para obtermos o texto encriptado C, utilizamos a seguinte fórmula:

$C = M^e \bmod n$.

Ora, $8^7 \bmod 33 = 2$

Temos assim que o texto "8", depois de encriptado pela chave privada, passou a ter a aparência 2. Este texto pode assim circular em qualquer rede, sendo seguro que ninguém pode deduzir dele que, na verdade, se trata do texto com a mensagem "8", a não ser a pessoa que possua a outra chave.

Em resultado dessa operação, e porque o algoritmo é uma fórmula matemática, uma vez aplicado àqueles dígitos, produz um novo produto, que na verdade é um novo documento.

Vamos agora considerar que essa pessoa somos nós, e com a nossa chave pretendemos proceder à desencriptação. O procedimento é idêntico, mas utilizamos a segunda chave, que seria então a chave privada (3,33). Para desencriptar e obter o texto M fazemos:

M = C^d mod n

M = 2^3 mod 33 = 8. Temos então o documento desencriptado.

Quando se aplica a segunda chave, ele encripta também os dados sobre que opera. Mas como se aplica sobre o documento que foi gerado pela encriptação efetuada pela primeira chave, o que resulta dessa operação, de segunda encriptação, é a desencriptação do documento e o regresso à sua versão original.

Assim, ambas as chaves podem encriptar e ambas podem desencriptar, mas cada uma delas só pode desencriptar aquilo que a outra encriptou. Essa desencriptação, sendo aplicada sobre o resultado da encriptação da primeira chave redunda na desencriptação e no regresso ao documento original. A encriptação que o algoritmo faz mediante a utilização da primeira chave é revertida pela aplicação do algoritmo com a segunda chave sobre o resultado da encriptação da primeira.

Na verdade, cada uma das chaves executa só uma operação, que consiste na encriptação do documento sobre que é aplicada. Quando esse documento a que é aplicada uma chave é já, em si mesmo, o resultado da operação da encriptação da outra chave, então esta segunda encriptação redunda na desencriptação desse documento e, portante, no regresso ao documento inicial, revertendo-se a primeira operação.

Chamamos desencriptação à operação de reversão que a segunda chave faz sobre o produto que resultou da aplicação da primeira chave, mas essa operação mais não é que uma segunda encriptação. Dela resulta aquela reversão, apenas porque ambas as chaves estão matematicamente relacionadas.

Estas operações podem ser feitas indistintamente por uma e a outra chave, ou seja, ambas encriptam e ambas desencriptam, mas cada uma delas só desencripta o que a anterior encriptou.

Vamos agora inverter as chaves. Vamos encriptar com a chave que utilizámos anteriormente para desencriptar, e depois desencriptaremos com a chave com que anteriormente encriptámos. No pressuposto de que alguém nos está a enviar um texto encriptado, vamos considerar que a chave que utiliza essa pessoa (chave pública) é (3,33) e que a chave que nós utilizamos para desencriptar (chave privada) é (7,33).

Vamos ver se conseguimos. O texto é o mesmo. “8”. Assim:

Para obtermos o texto encriptado C, utilizamos a seguinte fórmula:

C = M^e mod n.

Ora, 8^3 mod 33 = 17

Temos assim que o texto "8", depois de encriptado pela chave privada, passou a ter a aparência 17. Recebemos assim uma mensagem com a aparência de "17", que necessitamos de desencriptar para conhecermos o seu real conteúdo.

O procedimento é idêntico, mas utilizamos como chave de desencriptação a outra, que seria então a chave privada (7,33). Para desencriptar e obter o texto M fazemos:

M = C^d mod n

M = 17^7 mod 33 = 8. Temos então o documento desencriptado.

Como vemos ambas as chaves encriptam, e ambas desencriptam. Mas ambas encriptam qualquer documento e cada uma delas apenas desencripta o que a outra encriptou. Ambas têm a virtualidade de devolver ao seu conteúdo original, um documento encriptado pela outra.

Cap. III – O objeto da assinatura eletrónica

Uma assinatura manuscrita aplica-se sobre um documento em papel. É esse o objeto material da assinatura. O efeito da assinatura é a vinculação do seu autor ou subscritor ao conteúdo informacional, composto pela escrita e pelo suporte físico do papel que constituem o documento. O papel serve apenas de suporte a esse conteúdo informacional que constitui o documento.

Um documento é a expressão, materializada num suporte, de um facto ou de uma intencionalidade humana, que pode consistir numa declaração de vontade, numa declaração de ciência, num contrato, num negócio jurídico, num ato jurídico ou numa outra forma de expressão de um pensamento ou de uma vontade, mas que se separou do seu autor, depois de exteriorizado, num suporte que agora lhe confere autonomia e identidade. O objeto intencional de uma assinatura é sempre um conteúdo informacional materializado num suporte onde perdura.

A função da documentação dos atos é a de os materializar, e essa materialização tem como objetivo resgatá-los à extrema finitude que é própria, por exemplo, da expressão verbal da vontade humana. Essa expressão, se não for registada num suporte documental, desaparece no próprio momento em que as ondas sonoras das

palavras que a veicularam se desvanecem no ar. O registo documental grava essa expressão e preserva-a para o futuro como que cristalizando no tempo esse momento criador inicial. Essa documentação não elimina essa finitude, mas prolonga no tempo o testemunho da sua existência e da forma como foi manifestada aquela expressão, permitindo, assim, que outras pessoas possam aceder à informação produzida, em tempo diferente daquele em que foi expressa.

Quando uma expressão de vontade ou de um facto se autonomiza num documento, torna-se um objeto com uma identidade diferente do seu autor, porque se separa dele. A sua expressividade pode ser observada por terceiros, mesmo na ausência do seu autor.

A função da assinatura é manter essa conexão entre o suporte documental e a pessoa que o produziu, como que prolongando no tempo o vínculo naturalístico essencial e inicial entre o conteúdo da informação, que resultou da sua expressão verbal e a pessoa que a exteriorizou. O seu objeto é essa intencionalidade que se expressou e autonomizou num documento e que passou a ser informação.

O documento e a sua assinatura são duas manifestações separadas da vontade humana, de resistir à finitude, à contingência e à volatilidade que são caraterísticas próprias e intrínsecas da sua natureza. Ambas são apenas tentativas temporárias e imperfeitas, como a própria natureza humana o é. Mas ambas são formas de criar estabilidade, previsibilidade e paz social, no final de contas o objeto do Direito.

Nos documentos eletrónicos a volatilidade e a contingência são maiores que nos documentos em papel, dado que o papel é um objeto estático, tal como a tinta que nele grava a expressão da vontade ou de um acontecimento. Os documentos eletrónicos não são objetos, mas processos complexos e relacionais, porque se trata de combinações de dígitos operadas por máquinas, que necessitam de ser transformadas para poderem ser inteligíveis e objeto de cognoscibilidade jurídica.

O conceito de documento eletrónico como suporte de informação é a base da fenomenologia da assinatura eletrónica, dado que é ele o objeto da assinatura. O documento eletrónico é uma entidade independente da assinatura eletrónica, dado que a sua existência jurídica não depende necessariamente da assinatura. Esta serve só para conferir certeza da vinculação de uma pessoa ao documento, mas essa vinculação também se pode alcançar por outros meios, nomeadamente a prova testemunhal ou uma declaração do próprio. Existem casos em que a lei exige a assinatura dos documentos

como requisito de validade ou de eficácia, mas o documento existe sempre para além da assinatura.[178]

O documento é uma entidade prévia à sua qualificação jurídica e existe para além das exigências legais de assinatura, mas também de forma escrita, de autenticação, de originalidade e de integridade. Todos estes atributos podem existir, ou não num documento e são posteriores a ele. A construção do conceito de documento eletrónico foi uma necessidade e um pressuposto fundamental para a formação do quadro jurídico da segurança eletrónica e da assinatura eletrónica. Mas, como veremos mais adiante, o documento eletrónico não esgota as formas de manifestação do tráfego jurídico eletrónico, dado que nem todas as transações necessitam se ser documentadas, tal como ocorre nas relações estabelecidas em contextos não eletrónicos.

1. A formação do conceito de documento eletrónico. Os conceitos de mensagem e de registo

O conceito de documento eletrónico é relativamente recente e tem a sua origem nos conceitos de mensagem eletrónica utilizada pela tecnologia do EDI.

1.1. O conceito de mensagens eletrónicas da LMCE

O instituto da assinatura eletrónica nasceu da necessidade de conferir eficácia jurídica às mensagens comunicadas por EDI. É nessas mensagens que se funda o conceito de documento eletrónico.[179] Uma mensagem comunicada por EDI para fins comerciais consiste, normalmente, uma declaração negocial.[180] Embora a LMCE utilize

[178] Nos trabalhos de elaboração da UNCUECIC, a delegação argentina chamou a atenção para o interesse de não se prever a necessidade da assinatura como requisito universal de validade, e de, em alternativa, se respeitar sempre a vontade das partes, no sentido de poderem utilizar os métodos de autenticação que entendam. *"The recommendation is that the validity of an electronic communication should not be made conditional upon the electronic signature requirement"*. A/CN.9/578/Add.9, par. 3. Mas a questão releva da própria identidade do conceito de documento, que possui uma identidade própria, que precede a assinatura, sendo que esta é apenas um instrumento de autenticação, a par de outros.

[179] Como se refere nos trabalhos preparatórios da LMCE, um documento jurídico que foi ditado pela necessidade de regular o regime jurídico do EDI, *"... the initial focus of the uniform rules should be EDI messages"*. "A/CN.9/373", par. 26.

[180] Também assim era entendido nos documentos preparatórios:*"Such legally relevant messages included, for example, pre-contractual communications, various types of notifications or requests made during the performance of contracts, and claims arising from the breach of contracts"*. "A/CN.9/373", par. 28.

o conceito de mensagem e não de documento, alarga a definição da sua abrangência a outros tipos de suportes, nomeadamente os seguintes:

i) As mensagens que se reportem a outras mensagens, incluindo as que têm por finalidade a sua revogação ou alteração.[181] Também elas são suportes eletrónicos suscetíveis de produzir efeitos jurídicos;[182] [183]

ii) Os registos, eletrónicos internos das empresas.[184] Estes registos são relevantes para efeitos probatórios, contabilísticos, de auditoria;

iii) Toda a informação, mesmo não estruturada, em suporte eletrónico.[185] Toda a informação gerada, emitida, recebida gravada por meios eletrónicos, pode possuir relevância jurídica que deve ser salvaguardada;[186]

iv) Os documentos em suporte eletrónico, que resultaram da transposição de documentos em papel, necessitam também de possuir validade e eficácia jurídica; [187]

v) A inclusão das versões preliminares dos documentos eletrónicos, dado que não existe, como no papel, o conceito de rascunho e de documento

[181] Também assim se reconhecia nos trabalhos preparatórios: *"The definition of "data message" is also intended to cover the case of revocation or amendment".* "A/CN.9/426", par. 46.

[182] *"It was generally felt that, provided that the revocation or amendment was itself contained in a data message, it would be covered by the existing definition"*. A/CN.9/40, par. 134.

[183] Esta abrangência do conceito de mensagem eletrónica às comunicações revogatórias ou de alteração de anteriores manteve-se até muito recentemente, nos documentos preparatórios da UNCUECIC: *"Lastly, the definition of "data message" is also intended to cover the case of revocation or amendment"*. "A/CN.9/608/Add.1", par. 53.

[184] *"EDI messages should be understood as a broad concept that included, in addition to communications transmitted between parties, also records created by a party but not transmitted to another party"*. "A/CN.9/373", par. 27.

[185] *"On the one hand, the concern was expressed that the word "message" might suggest the exclusion of data that was merely stored, while on the other hand the word "record" might be read as excluding data that was communicated. Another concern was expressed that the word "record" might cause some uncertainty in some languages and it was suggested that it should be replaced by the word "message""*. "A/CN.9/406", par. 133.

[186] *"The reference to "similar means" is intended to reflect the fact that the Model Law was not intended only for application in the context of existing communication techniques but also to accommodate foreseeable technical developments"*. "UNCITRAL Model Law on Electronic Commerce Guide to Enactment with 1996 with additional article 5 as adopted in 1998". United Nations, New York, 1999, par. 31.

[187] *"There may exist situations where digitalized information initially dispatched in the form of a standardized EDI message might, at some point in the communication chain between the sender and the recipient, be forwarded in the form of a computer-generated telex or in the form of a telecopy of a computer print-out. Such situations are intended to be covered by the Model Law"*. "A/CN.9/WG.IV/WP.64", par. 31.

"passada a limpo".[188] O conceito de mensagem da LMCE admite no seu seio todas as formas, incluindo as versões preliminares.[189]

O conceito jurídico de mensagem eletrónica é mais vasto do que o conceito técnico de mensagem de EDI, dado que abrange todos os tipos de documentos eletrónicos. Embora a LMCE não utilize expressamente o conceito de documento eletrónico é dele que se compõe o conceito de mensagem de dados, que se centra na informação em forma de mensagem de dados.[190] Do mesmo modo a própria definição de mensagem de dados tem como objeto de referência a informação.

Verifica-se, assim, que desde logo na própria LMCE o conceito de mensagem de dados é claramente insuficiente para o universo factual que o legislador lhe atribuiu como referencial, dado que uma mensagem é sempre uma comunicação, e aquele conceito vai muito além das comunicações, abrangendo potencialmente todo o universo daquilo a que se passou a designar de documentos eletrónicos.

É à volta deste conceito de mensagem de dados que se estrutura todo o regime da LMCE, sendo sobre esta base que se funda a sua norma mais importante, que é o art.º 5.º, que consagra o reconhecimento jurídico das mensagens de dados. Esta norma adota o princípio de equivalência funcional, no sentido do qual as mensagens eletrónicas não terão menor relevo jurídico do que aquelas que estão suportadas em papel, só pelo facto de o seu suporte ser o eletrónico.[191]

Trata-se de um nível mais baixo de equivalência, destinado a impedir a discriminação dos documentos eletrónicos só pelo mero facto de se apresentarem nesse suporte. Será sobre esta base que depois se estruturarão outros instrumentos de segurança das mensagens eletrónicas, como maios tarde analisaremos.

---

[188] A questão foi levantada pelo Japão, nos comentários à definição do conceito de mensagem de dados do projeto de LMCE. *"In an EDI environment, the same information could be recorded in different forms at one time, as well as at different times. In such an environment, what does "its final form" mean?".* "A/CN.9/409", pág. 2.

[189] *"'Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy"*. (alínea a) do artigo 2.º da LMCE). "Guide to Enactment LMCE (1996)", pág. 4.

[190] Artigo 1.º da LMCE, sob o título "Sphere of application": *"This Law applies to any kind of information in the form of a data message used in the context of commercial activities*"". "UNCITRAL Model Law on Electronic Commerce …", *idem*.

[191] O artigo 5.º da LMCE tem a seguinte redação: "*Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message"*. "UNCITRAL Model Law on Electronic Commerce Guide to Enactment with 1996 with additional article 5 as adopted in 1998". United Nations, New York, 1999.

1.2. O conceito de mensagem eletrónica da LMAE e da UNCUECIC

A LMAE não se refere ao conceito de mensagem de dados nem de documento eletrónico, pelo que não apresenta, nessa matéria, qualquer inovação, provavelmente para garantir uniformidade na sua aplicação e na interpretação do conceito.[192] A manutenção do conceito sem alterações reflete também o sucesso da opção da LMCE, de garantir uma formulação aberta da sua definição, por forma a garantir a sua capacidade de acolhimento de novos tipos de suportes eletrónicos.[193] Do mesmo modo na UNCUECIC a definição constante da alínea c) do art.º 4.º mantém a mesma redação, dado que se entendeu que já era suficientemente abrangente e garantia uniformidade.[194]

1.3. A generalização da utilização do conceito de documento eletrónico

A expansão das redes abertas, rapidamente abriu a necessidade de alargar o conceito, criando a figura jurídica do documento eletrónico *("electronic record"* no original em Inglês, em contraposição com *"data message"*). Essa necessidade só foi sentida, nos trabalhos de conceção da Convenção das Nações Unidas sobre Contratos para a Internacional Transporte de Mercadorias Total ou Parcialmente por Mar, que foi publicada em 2009, que criou, pela primeira vez, os conceitos de documento de transporte eletrónico[195] e de título eletrónico de transporte.[196] Essa definição seria mais

---

[192] Essa preocupação ficou expressa nos documentos dos trabalhos preparatórios: *"The Working Group decided that, to ensure consistent interpretation of the two texts, those definitions should be strictly identical. Subparagraph (d) was adopted unchanged"*. "A/CN.9/483", par. 69.

[193] Essa abrangência do conceito de mensagem de dados é observada no Guia de Transposição da LMAE como uma das suas principais caraterísticas. *"The aim of the definition of "data message" is to encompass all types of messages that are generated, stored or communicated in essentially paperless form. For that purpose, all means of communication and storage of information that might be used to perform functions parallel to the functions performed by the means listed in the definition are intended to be covered by the reference to "similar means", although, for example, "electronic" and "optical" means of communication might not be, strictly speaking, similar"*. "UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001", par. 98.

[194] Nos trabalhos preparatórios da UNCUECIC refere-se esse facto, mas também se utiliza pela primeira vez o conceito de "record", mais próximo do de documento eletrónico. *"The notion of "data message" is not limited to communication but is also intended to encompass computer-generated records that are not meant for communication. Thus, the notion of "message" includes the notion of "record""*. É a primeira vez que se utiliza este conceito nos documentos de trabalho da UNCITRAL. "A/CN.9/608/Add.1", par. 53.

[195] A definição contida no n.º 18.º do artigo 1.º é a seguinte: *""Electronic transport record" means information in one or more messages issued by electronic communication under a contract of carriage by a carrier, including information logically associated with the electronic transport record by attachments or otherwise linked to the electronic transport record contemporaneously with or subsequent to its issue*

tarde também acolhida nos trabalhos de conceção de uma eventual Lei Modelo dos Documentos Eletrónicos Transferíveis, que ainda decorrem.[197]

O conceito de documento é mais adequado ao seu enquadramento como elemento de prova, bem como na aplicação a este tipo de suporte, de todos os atributos legais que a ordem jurídica confere aos documentos, independentemente do seu suporte. Do mesmo modo que na LMCE, também aqui o que é essencial aos documentos eletrónicos é o seu conteúdo informacional e o suporte eletrónico. Tende-se, assim, para uma conceção de documento eletrónico como abrangendo qualquer conteúdo de informação, registado num qualquer suporte eletrónico.

1.4. Os documentos eletrónicos que não têm correspondência com o papel

Esta generalização do conceito de documento eletrónico a toda a informação que conste de um suporte eletrónico faz com que esse conceito vá muito para além do de documento em suporte de papel. Nas comunicações eletrónicas a necessidade de autenticar documentos idênticos aos de papel, alarga-se também à necessidade de confirmar a própria informação acerca da identificação das pessoas. E a repetição e rapidez que se exige nas operações nas redes abertas obriga a que essa autenticação seja efetuada em todas as operações.

A maioria dos sítios *web* exigem aos utilizadores que se identifiquem e autentiquem para realizarem uma sessão segura. Em muitos casos o utilizador menciona a sua identidade e insere uma senha de acesso. Idêntica operação se faz nos terminais de

---

by the carrier, so as to become part of the electronic transport record, that: (a) Evidences the carrier's or a performing party's receipt of goods under a contract of carriage; and (b) Evidences or contains a contract of carriage". "United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea"; United Nations Commission on International Trade Law; United Nations, Vienna, 2009, pág. 17.

[196] A definição contida no n.º 18.º do artigo 1.º é a seguinte: *""Negotiable electronic transport record" means an electronic transport record: (a) That indicates, by wording such as "to order", or "negotiable", or other appropriate wording recognized as having the same effect by the law applicable to the record, that the goods have been consigned to the order of the shipper or to the order of the consignee, and is not explicitly stated as being "non-negotiable" or "not negotiable"; and (b) The use of which meets the requirements of article 9, paragraph 1*". "United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea"; *ibidem*.

[197] A redação é a seguinte: *""electronic record" means information generated, communicated, received or stored by electronic means [, including, where appropriate, all information logically associated or otherwise linked [together] [thereto] [so as to become part of the record], whether generated contemporaneously or [not] [subsequently]]"*. "A/CN.9/WG.IV/WP.130", par. 21.

levantamento automático de dinheiro.[198] Os dados inseridos pelo utilizador são informação, que fica registada nos suportes eletrónicos das respetivas entidades. Essa informação é, na sua essência, um documento eletrónico ou uma mensagem eletrónica. Basta que exista informação registada num suporte eletrónico, para que se considere estarmos perante uma mensagem eletrónica.[199]

O trabalho da UNCITRAL na definição do conceito de mensagem eletrónica seria muito importante na criação das condições de contexto para a formação do conceito de documento eletrónico. O conceito de documento eletrónico ocupa um lugar central na dogmática relativa à assinatura eletrónica, bem como a toda a disciplina do direito da eletrónica.

No paradigma do papel, a identificação das pessoas e a certificação dessa identificação são efetuadas sem necessidade de recurso à assinatura, dado que é sempre possível a identificação presencial, mas essa possibilidade não existe no paradigma eletrónico, pelo que, dada a sua inerência às funções da assinatura, a identificação é frequentemente obtida através dos seus mecanismos.

Por outro lado, a definição de documento e de mensagem eletrónica que temos vindo a analisar, tem uma importante limitação, resultante do facto de se referir apenas a informação. Trata-se de um conceito restritivo, formatado à semelhança dos documentos em papel e às mensagens EDI. Não se abrangem outros tipos de conteúdos dos documentos, como é o caso de obras de arte, de imagens e de som, que a digitalização permitiu que se suportassem também em forma eletrónica.

1.5. A legislação da UE e a assunção do conceito de documento eletrónico

[198] Frequentemente os *sites* solicitam aos seus utilizadores que se autentiquem previamente. Porém, o objeto da autenticação não são as pessoas, mas a informação relativa à sua identidade. É também isso que acontece nos contextos não eletrónicos, como é o caso da entrada num serviço público ou num local de aceso restrito. Nesses casos é solicitado a identificação da pessoa, ou seja, a disponibilização dos elementos informativos que revelam a sua identidade. Mas isso normalmente não basta para que o acesso seja permitido imediatamente. É necessário que esses dados informativos sejam autenticados, o que se faz mediante a exibição de um documento emitido por uma entidade terceira, em quem todos os agentes confiam, que certifica aquela identidade. Esse documento é normalmente, no nosso país, o Cartão do Cidadão. Assim, a permissão da entrada depende da resposta adequada a duas perguntas: Qual a sua identidade? E como pode prová-la? A resposta à primeira serve para apresentar os elementos informativos da identificação, e a segunda para autenticar esses elementos.

[199] Como se refere num dos textos da UNCITRAL, *"the notion of "message" includes the notion of "record""*, acrescentando-se que *"The notion of "data message" is not limited to communication but is also intended to encompass computer-generated records that are not intended for communication"*. "A/CN.9/426", par. 45.

A Diretiva 1999/93/CE, não contém uma definição de mensagem de dados nem de documento eletrónico. Refere-se ao objeto da assinatura eletrónica como sendo "dados", pelo que o seu âmbito de aplicação é mais abrangente, porque estarão em causa qualquer tipo de dados, desde que em forma eletrónica.[200]

O conceito de documento eletrónico viria a ser consagrado na legislação da UE, no n.º 35.º do art.º 3.º, do Regulamento (UE) n.º 910/2014, de 23 de julho de 2014 da forma mais abrangente, já não se referindo a dados, nem a informação, mas a qualquer conteúdo.[201] Todos os dados que existam em suporte eletrónico podem constituir um documento eletrónico.

Esta definição do regulamento é importante, porque o seu âmbito de aplicação é mais abrangente que o da assinatura eletrónica, aplicando-se também à autenticação dos sítios web e às comunicações eletrónicas.[202]

Fica assim, com o Regulamento, ultrapassada a diferença semântica entre documentos eletrónicos e mensagens eletrónicas, sendo que o primeiro destes conceitos abrange todos os conteúdos em suporte eletrónico.

2. A ontologia dos documentos eletrónicos

Um documento em suporte eletrónico não equivale, em termos estruturais, a um documento em suporte de papel. O papel é um objeto onde se grava a informação que constitui um documento, sendo de observação direta e imediata. Um documento eletrónico não é um objeto, mas uma composição complexa de vários elementos estruturais de natureza tecnológica, informacional, matemática, digital e lógica.

Essa estrutura complexa não é imediatamente acessível nem apreensível pelo entendimento humano, dado que a sua inteligibilidade depende de um processo de transformação dos seus dados fundamentais para que possam ser analisados e

---

[200] Por exemplo, na definição do conceito de assinatura eletrónica avançada, a alínea d) do n.º 2 do artigo 2.º refere-se ao objeto a que é aplicada a chave privada como "dados" ("*estar ligada a dados*"). Do mesmo modo, na alínea a) do n.º 1 do artigo 5.º, refere-se a "*dados em forma digital*".

[201] Textualmente: *"«Documento eletrónico»: qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual"*.

[202] Como se refere n.º 63 dos considerandos que o antecedem, *"O presente regulamento deverá estabelecer o princípio segundo o qual não podem ser recusados efeitos legais a um documento eletrónico pelo facto de se apresentar em formato eletrónico garantindo que que nenhuma transação eletrónica é rejeitada pelo facto de o documento se apresentar em formato eletrónico"*. Esse propósito é consumado no artigo 46.º, que constitui a única disposição do capítulo consagrado ao "documento eletrónico": *"Não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a um documento eletrónico pelo simples facto de se apresentar em formato eletrónico"*.

compreendidos pela inteligência humana. Por essa razão, não são facilmente transponíveis para o suporte eletrónico os instrumentos jurídicos que são aplicáveis aos documentos em suporte de papel.

As principais caraterísticas do papel são a sua durabilidade, sendo essa uma das razões fundamentais da exigência de documento escrito de muitas jurisdições nacionais. O papel preserva a vontade expressa, mais do que a palavra, que se volatiliza com a sua própria expressão, permitindo evidenciar a manifestação de vontade de o seu autor a ele se associar, mediante a assinatura. O papel também permite a transmissão dessa expressão e a sua reprodução para que terceiros a possam consultar e delas extrair efeitos. Permite também a preservação da sua integridade e o respeito pela forma como foi expressa, porque garante que um determinado documento não é alterado após ter sido gerado ou que, sendo-o, seja possível observar essa alteração, e finalmente a sua legibilidade.[203]

Ora, estes cinco atributos dos documentos em suporte papel (autenticação, conservação, transmissão, integridade e legibilidade), não são facilmente transponíveis para o suporte eletrónico com as mesmas caraterísticas de unidade e inseparabilidade do papel, nem com a simplicidade com que podem ser apreciáveis pelos sentidos humanos.

Os documentos eletrónicos não são uma unidade, mas uma dualidade composta. Não são um objeto, mas um processo de composição complexa.[204] Eles são sempre o resultado de um processamento, efetuado por máquinas e apresentado com uma determinada configuração, sendo, porém, que essa apresentação não é a essência do documento. Embora os computadores tenham sido criados pela inteligência humana, a sua linguagem não é igual à dos seres humanos, porque opera com o código binário e não com o alfabeto nem o sistema decimal.[205]

---

[203] Nos trabalhos preparatórios da UNCUECIC foram enunciadas as cinco funções do papel: a legibilidade, a integridade, a possibilidade de reprodução, a possibilidade de autenticação e a validade probatória. *"To ensure that a record would be legible by all; to ensure that a record would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts"*. "A/CN.9/608/Add.2"6, par. 5.

[204] Como se refere nos documentos da UNCITRAL,*"Because of its physical characteristics, the traditional paper document is accepted as evidence. It is durable, and changes or additions will normally be clearly visible. The electronic document is quite different. It takes the form of a magnetic medium whose data content can be changed at any time. Changes or additions will not appear as such"*. A/CN.9/WG.IV/WP.53, páginas 365 a 382, Annex, III.

[205] Como refere David Silva Ramalho, "*A ilusão de tridimensionalidade que encontramos nos ecrãs dos sistemas informáticos é o produto de um processo de leitura de dados de origem elétrica e meramente virtual e que, sem meios técnicos que permitam aceder, recolher ou inerceptar a prova digital, esta não é fisicamente apreensível*". Ramalho, D. S. (2017). *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Edições Almedina. S. A. Coimbra, pág. 105.

Essa estrutura digital serve apenas para ser processada por sistemas informáticos e é ininteligível ao entendimento humano.[206] Apesar de ela existir em todos os documentos, ela não possui, por si só, as caraterísticas de um documento, porque se trata apenas de dados em bruto, com uma lógica interna, cuja organização não é, em si mesma, suscetível de compreensão humana. Mas é esse suporte digital o elemento radical que distingue o documento e que assegura essa identidade e estabilidade.

O elemento fundamental de um documento é a informação que veicula e não os dados que lhe servem de suporte. Os dados digitais que estruturam em termos lógicos a base informática de um documento enquanto, não são conhecimento. Esses dados só proporcionam conhecimento se forem suscetíveis de ser interpretados, o que só ocorre se veicularem informação e forem legíveis. Para isso, esses dados necessitam de ser transformados, dado que, por si só não são informação. Um documento eletrónico que não seja inteligível não pode ser objeto de conhecimento jurídico, e portanto não pode produzir efeitos jurídicos.

É este o segundo elemento da dualidade dos documentos eletrónicos. A sua transposição para uma versão inteligível. E para isso é necessário um interface que, operando sobre esses dados, os converta num suporte legível pelas categorias do entendimento humano. Essa operação de conversão tem que ser efetuada através de uma máquina e de um processamento efetuada por um programa informático que são externos ao próprio documento.[207] [208]

---

[206] Como se refere num dos documentos de trabalho de preparação da UNCUECIC, *"Indeed, while paper-based documents are readable by the human eye, electronic communications are not—unless printed to paper or displayed on a screen"*. "A/CN.9/608/Add.1", par. 7.

[207] Na memória dos computadores, os documentos, sejam eles textos, fotografias, filmes, gravações de voz ou som, etc.., estão gravados em forma se sequências de bites, impercetíveis aos sentidos e ao entendimento humano. São os sistemas operativos dos computadores que os convertem no aspeto gráfico dos documentos, de forma a poderem ser interpretados pelas pessoas. Mas uma coisa é o registo informático, a base de dados, outra diferente é a aparência com que esses dados são apresentados visualmente no écran do computador, no som que ele emite ou no papel impresso. *"One of many distinctions between EDI messages and paper-based documents, namely, that the latter were readable by the human eye, while the former were not so readable unless reduced to paper or displayed on a screen"*. "A/CN.9/407", par. 32.

[208] Cremades compara os dados eletrónicos ao material da pintura, que não se confunde com a obra, o resultado, o interface. Uma coisa são os materiais com que a obra foi criada, outra coisa diferente é a criação *"Historicamente o artista realizava um obra única utilizando um meio determinado. A obra em si mesma e a forma como esta chega ao usuário (o interface) constituem uma mesma coisa: um quadro é apenas um quadro e dificilmente pode separar-se da tela ou das cores que o formam. O mundo digital é diferente. A informação relativa aos objetos que formam uma obra de arte, quer sejam palavras, cores, formas ou sons, estão gravadas em bases de dados. Tão importante como os objetos, os dados em si mesmos, é o interface, ou seja, o meio pelo qual se tem acesso aos mesmos"*. Cremades, Javier; Op. Cit., pág. 162.

Uma vez aqui chegados, uma questão se coloca inevitavelmente. O documento eletrónico é a estrutura de dados ou a sua versão legível apresentada no écran de um computador?

Se o documento não é o suporte de dados, dada a sua ininteligibilidade humana, também não podemos dizer que seja a apresentação que os computadores dela para ser visualizada, uma vez que essa apresentação deverá ser sempre igual, independentemente do computador que a efetue. Essa visualização não é mais do que o resultado de um processamento informático que é aplicado ao conjunto de dados organizados de determinada forma – a tal sequência de dígitos de zero e um que, essa sim constitui a estrutura fundamental e essencial do documento eletrónico. É essa estrutura que, na sua consistência, é irrepetível, substancial e radical, e confere identidade ao documento.

A natureza de um documento eletrónico é composta pela associação integral de todas as suas componentes informativas, lógicas, digitais, tecnológica, bem como pela sua apresentação legível numa plataforma eletrónica. Um documento eletrónico só poderá ser considerado como tal se for suscetível de avaliação jurídica e, por exemplo, em caso de litígio, ser suscetível de ser avaliado por um tribunal como elemento de prova, para o que é necessário o requisito da cognoscibilidade, dado que só é suscetível de ser objeto de avaliação jurídica o que é suscetível de ser conhecido.[209]

Assim, poderíamos concluir que um documento eletrónico é um qualquer suporte lógico suscetível de significado, ou seja, de ser lido e interpretado pelo conhecimento humano.

Mas este requisito da cognoscibilidade de um documento, sendo muito importante, necessita ainda de duas precisões, sendo a primeira relativa à inteligibilidade dos documentos eletrónicos e a outra às declarações eletrónicas automatizadas.[210]

---

[209] Nos trabalhos de elaboração da LMCE foi ponderada a adoção de vários conceitos nesta matéria, nomeadamente os de acessibilidade, legibilidade e de suscetibilidadede interpretação. *"The use of the word "accessible" was meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained"*. "A/CN.9/407", par. 56.

[210] Nos suportes eletrónicos a informação assenta sempre em dados. E o que é significante para fins jurídicos é a informação, sendo que os dados, como suporte essencial à informação, são a base sem a qual não existe informação. Por isso, não podemos afirmar que aos dados são um elemento não jurídico e só a informação o é. São ambos, porque não se podem separar. Como refere Cecílio, "*tecnicamente, dato y información no son conceptos sinónimos, en verdade, información es la representación simbólica, cuantificada o cuantificable, de la información, siendo um concepto puramente objetivo*". Cecílio, L. R.

3. A inteligibilidade dos documentos eletrónicos

A expansão da utilização das tecnologias eletrónicas conduziu a que muitas operações que produzem efeitos jurídicos passassem a ser estabelecidas mediante comunicações eletrónicas diretas e automatizadas entre sistemas informáticos. Estas comunicações são apenas interações eletrónicas entre sistemas, que desencadeiam a produção automatizada de efeitos jurídicos sem necessidade operacional de produção de quaisquer documento legível e inteligível.[211] [212] Estas mensagens não necessitam de ser lidas por qualquer pessoa para que possam produzir efeitos jurídicos.[213] Por essa razão o conceito de mensagem da LMCE é abrangente, dispensando o requisito da legibilidade e centrando-se no requisito essencial da acessibilidade para posterior consulta.[214] Este conceito abrange então a legibilidade pelo entendimento humano e a suscetibilidade de essas mensagens produzirem efeitos nos sistemas informáticos de destino.

Essa formulação abrange todos os suportes eletrónicos de informação que sejam suscetíveis de produzir efeitos jurídicos, sendo neutra relativamente à tecnologia utilizada.[215]

Na legislação da UE, o Regulamento (UE) N.º 910/2014 consagra já, como vimos no capítulo anterior, o conceito de documento eletrónico, englobando claramente este tipo de transações eletrónicas.

(2015) Política Criminal el Ciberespacio: Crítica al Concepto de Crimen Informático". *Fodertics 3.0. Estúdios Sobre Nuevas Tecnologias e Justícia*. Editorial Comares. Granada, pág. 217.

[211] *"It was also stated that the word "usable" was not intended to cover only human use but also computer processing"*. "A/CN.9/407", par. 56.

[212] *"Such notions as "readability" or "intelligibility", which might constitute too subjective criteria"*. "A/CN.9/407", par. 56.

[213] Merece relevo o comentário de Singapura ao projeto de LMCE nesta matéria: *"In many EDI systems, the processing of data messages is automated with little or no human intervention. This means that the data message may not be displayed to any person at all nor is there a need to do so"*. "A/CN.9/409", pág. 5.

[214] O n.º 1 do artigo 6.º da LMCE tem a seguinte redação: *"Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference"*. "Guide to Enactment LMCE (1996)", pág. 5.

[215] Essa definição consta da alínea b) do artigo 2.º, com a seguinte redação*: "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy"*. "Guide to Enactment LMCE (1996)", pág. 4.

4. A declaração negocial eletrónica automatizada

O EDI permitiu automatizar muitos procedimentos de gestão empresarial, incluindo a emissão de declarações negociais e a celebração de contratos.

Essa automatização incluía a programação de sistemas que desencadeiam a emissão de pedidos de fornecimento de novas mercadorias em forma de encomendas, inseridas pelo sistema de comunicações nos respetivos sistemas informáticos dos fornecedores.[216] Estes, por sua vez, mediante a automatização dos seus procedimentos internos, passaram a poder desencadeado, também de forma automática, o procedimento de fornecimento das mercadorias solicitadas.[217]

Neste contexto tecnológico é possível a celebração de contratos sem intervenção humana, direta e imediata.[218] Ora, a essencialidade dos contratos consiste na expressão da vontade humana de cada uma das partes, e sempre se colocará a questão de saber se uma mensagem eletrónica emitida automaticamente por um sistema informático pode ser considerada uma declaração negocial, e se será possível conceber-se um contrato entre duas partes sem intervenção humana. Pode haver declarações negociais emitidas por computadores ? E sendo a resposta positiva, quem fica vinculado por essas declarações ? Pode um contrato ser celebrado pela interação de duas máquinas ou de dois sistemas informáticos? E mesmo que a redação do contrato e a sua impressão

---

[216] *"Another example of the possible conclusion of a contract without specific and express agreement was the situation in which the computer of the supplier was programmed to investigate the inventory records of the buyer and to dispatch automatically a certain quantity of goods when the quantity held by the buyer went below a certain limit. In such a situation, the supplier's computer, upon establishing that the requirements for the formation of a contract had been met, proceeded automatically to an act of execution of the contract"*. "A/CN.9/360", par. 85.

[217] *"It was observed that it was technically feasible to program a computer so that it would automatically react to an offer by sending a message of acceptance or by adopting any other conduct that amounted to acceptance (e.g., delivery of the goods). It was generally admitted that such pre-programming should constitute a presumption that the programming party had intended to approve the sending of a message"*. "A/CN.9/360", par. 83.

[218] Utilizamos a expressão "*de forma direta e imediata*", porque não existe vontade nas máquinas, ainda que informatizadas. O que as máquinas podem fazer é processamentos repetidos perante situações tipificadas, através de mecanismos de causa e efeito. Se mediante programação se determinar a uma máquina eletrónica, que emita uma determinada mensagem, com um conteúdo e forma previamente determinado, para outra máquina ou para uma pessoa, sempre que se verifique determinado pressuposto (por exemplo a uma determinada hora ou quando ocorra outra qualquer circunstância), ela procederá sempre dessa forma. Trata-se de um automatismo linear. Em alguns casos esse automatismo pode ser simultâneo com outros ou possuir uma maior complexidade, que levará algumas pessoas mais entusiasmadas a designar essas operações de inteligência artificial. Trata-se, porém, de procedimentos mecânicos, que são sempre determinados pela vontade humana. A execução pode ser efetuada por máquinas, mas a vontade é sempre humana, como não podia deixar de ser. Os computadores e os sistemas informáticos são instrumentos técnicos que o Homem utiliza para melhor operar a sua conduta, como tantos outros instrumentos que descobre e utiliza desde a origem dos tempos.

em papel seja automatizada, podemos chamar-lhe um acordo de vontades validamente expresso?[219]

Alguma doutrina jurídica, especialmente italiana, partindo da capacidade de processamento eletrónico e de transmissão da informação que os sistemas informáticos possuem, designa-os como sistemas inteligentes capazes de praticarem atos com relevância jurídica. [220] Esta doutrina considera que esses sistemas possuem mesmo uma *"vontade autónoma e totalmente independente dos contraentes" e* consistiriam em verdadeiros representantes dos seus titulares, que os poderiam substituir nas relações jurídicas estabelecidas por meios eletrónicos.[221]

Nos trabalhos preparatórios da LMCE analisou-se a natureza dessas mensagens, tanto quando se trata de propostas como da sua aceitação ou de declarações de consentimento. Discutia-se se pode um consentimento enviado por um desses sistemas ser considerado uma declaração de vontade e, se sim, de quem e de que natureza. Uma das questões que se colocava era se essa declaração era apenas a mera comunicação de uma necessidade ou se poderia também considerar-se que se tratava de uma manifestação de vontade capaz de ter como efeito a celebração de um contrato.[222]

Defendeu-se a necessidade da revisão dos conceitos tradicionais de declaração negocial e de consentimento, bem como da eficácia dos contratos celebrados apenas mediante a emissão de mensagens eletrónicas por máquinas ou sistemas informáticos automatizados. Partiu-se da preocupação de que não deveria ser admissível a existência de declarações negociais expedidas por computadores programados para o fazer com *"liberdade total para enviarem automaticamente declarações de oferta e de aceitação de contratos"*.[223] Considerou-se a possibilidade de se consignar na lei a obrigação de

---

[219] *"EDI creates new opportunities for the automation of the decision-making process. For example, a purchaser's computer may be programmed to send purchase orders under certain circumstances, and the supplier's computer may be programmed to act upon the orders it receives, both without human intervention"*. "A/CN.9/333", par. 61.

[220] Giannantonio, E. (1986). *Trasferimenti Elettronici dei Fondi e Autonomia Privata*. Univ. di Salerno, A. Giuffré. Milano; pags. 10 e 28.

[221] Clarizia, R. (1988) Informática e Conclusione del Contratto. 1ª edición, Colección Diritto dell"informática 5. Milán, pag. 26.

[222] *"The computer that had been programmed to react automatically to an offer by an act of acceptance was not, in fact, consenting to the formation of the contract but merely establishing that the will of the offering party had meshed with the will of the accepting party"*. "A/CN.9/360", par. 85.

[223] *"It was risky to allow full freedom to program computers to trigger contract offers and acceptances automatically"*. "A/CN.9/373", par. 133.

antes de se iniciar a execução de um contrato assim formado, a parte ter que informar previamente do início dessa execução a outra parte.[224]

Sugeriu-se que a LMCE deveria referir-se às declarações negociais eletrónicas emitidas por sistemas automatizados para lhes conferir expressamente validade e eficácia jurídica, com capazes de produzir a celebração de contratos.[225]

Mas essas doutrinas não tiveram sequência, em face do carácter instrumental dos sistemas informatizados, mesmo quando automatizados. Esses sistemas não possuem vontade própria e por isso não lhe podem ser imputadas declarações negociais, nem são sujeitos de direitos. São apenas instrumentos de expressão e de transmissão da vontade dos seus titulares, executando tarefas que lhe são determinadas em face da programação que é determinada pelos respetivos autores.[226]

Como qualquer máquina, o sistema informático, executa operações de acordo com as instruções de quem com eles opera e é por eles responsável. O caráter automatizado das operações não muda em nada esse princípio.

A criação de máquinas que são capazes de executar tarefas que anteriormente só podiam ser executadas por pessoas é um fenómeno que acompanha ancestralmente a humanidade. O aumento da complexidade das tarefas que se podem mecanizar e a sua automatização depende apenas da evolução do conhecimento humano. Não podemos dizer que os computadores substituem as pessoas na realização de tarefas que eles são capazes de fazer, sem ao mesmo tempo termos presente que isso acontece com qualquer máquina ou equipamento. Essa instrumentalidade relativamente ao que é humano é o que carateriza todas as técnicas e equipamentos, incluindo os informáticos. O que distingue os computadores é a possibilidade de serem programados e entre o momento em que essa programação é efetuada e aquele em que são executadas as tarefas que resultam da sua operacionalidade, haver um lapso temporal distendido, mas isso em nada altera o carácter pessoal e a responsabilidade das pessoas sob cujo domínio essas

---

[224] *"It was observed that such a theory might lead to reconsidering the traditional notion of consent. It was also stated that there might be a need to state in the form of a rule that, unless otherwise agreed, when a contract was formed as a result of the operation of a computer program, a party that executed the contract should give express notice of the formation of the contract to the other party"*. "A/CN.9/360", par. 85.

[225] *"Another view was that, to the extent any doubts existed as to the legal effects of automated formation of contracts, it would be useful to eliminate those doubts by an express provision in the uniform rules"*. "A/CN.9/373", par. 131.

[226] Nesse sentido, e por todos, Rivero, D.C. (Mayo 2005). Análisis de los Antecedentes del Concepto de Firma Electrónica Como Equivalente de la Firma Manuscrita. *Revista de Contratación Electrónica*. N.º 60, pág. 99.

máquinas ou sistemas operam.[227] As relações contratuais são estabelecidas sempre mediante o consentimento das partes, e a expressão desse consentimento reflete a vontade real de cada uma das partes, de se vincular.[228]

Foi nesse sentido que a LMCE veio estabelecer que as mensagens expedidas de forma automática se consideram declarações negociais imputáveis à pessoa que em concreto é a responsável pela programação do sistema que procede a essa expedição.[229] Nos casos em que são sistemas informatizados que desencadeiam a sua geração e emissão, a pessoa responsável será sempre aquela que determinou a programação do respetivo sistema.[230] Quando o sistema informático funciona, executa essa programação, pelo que todas as operações que ele realiza, tendo sido estritamente determinadas pelo conteúdo dessa programação, são imputáveis imediatamente ao seu autor, quer tenha sido ele a executá-la, quer o tenha feito por intermédio de terceiros por sua conta.[231]

Trata-se apenas de um modo de exteriorização de uma vontade negocial, que perdura no tempo por vontade do seu autor, sendo que os sistemas informáticos e os computadores são apenas instrumentos dessa vontade.[232].

Os sistemas informáticos podem emitir automaticamente declarações negociais erradas, quando funcionam de forma inadequada relativamente à programação que os enforma.[233] Mas a existência de erros é intrínseca à ação humana e também ao

---

[227] Era dessa forma que se abordava a questão nos trabalhos da LMCE. *"Data messages that are generated automatically by computers without direct human intervention should be regarded as "originating" from the legal entity on behalf of which the computer is operated"*. "A/CN.9/426", par. 48.

[228] Nesse sentido,*"This situation may increase the possibility that, due to the lack of a direct control by the owners of the machines, a message will be sent, and a contract will be formed, that does not reflect the actual intent of one or more parties at the time when the contract is formed"*. "A/CN.9/333", par. 61. Do mesmo modo, *"Such automation might increase the possibility that, due to the lack of a direct control by the owners of the computer, a message would be sent, and a contract formed, that did not reflect the actual intent of one or more parties at the time when the contract was formed"*. "A/CN.9/360", par. 80.

[229] *"The Working Group was agreed that any rules on the expression of consent in an electronic environment should be based on the principle of party autonomy"*. "A/CN.9/360", par. 86.

[230] Essa sugestão foi apresentada no seio da Comissão e viria a ser consagrada na LMCE. *"A person having, or deemed to have, final control over the computer application should be deemed to have approved the sending of all messages dispatched by that application"*. "A/CN.9/360", par. 81.

[231] *"The main purpose of paragraph (l) was to set out the conditions under which a data record could be attributed to its originator, and not to deal with the approval of the content of the communication by the originator"*. "A/CN.9/406", par. 115.

[232] Foi maioritária a opinião de que as partes que intervêm na celebração dos contratos são livres de utilizar no processo negocial quaisquer sistemas informáticos ou outros, mesmo automatizados. *"Under existing rules of contract law parties were free to use such automated messages for the purpose of concluding contracts".* E mais *adiante "since computers programmed to automatically trigger contract offers and acceptances were carrying out conscious decisions of humans"*. "A/CN.9/373", par. 130.

[233] Nos trabalhos da LMAE o Reino Unido defendeu a adoção de uma definição de sistema informático, considerando-o como um equipamento ou programa informático que permita registar, comunicar, receber e arquivar a informação contida em mensagens de dados. *"The equipment, software and operational control which permit information to be generated, communicated, received or stored in a data message"*. "A/CN.9/409", pág. 9. Essa definição foi adotada na LMCE, com ligeiras alterações, na alínea f) do artigo

funcionamento dos sistemas informáticos, até porque estes são criados pelos homens. Nesses casos, a responsabilidade por esse erro deve ser imputada, por princípio ao responsável pelo sistema.[234]

2.º: *"Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages"*. "Guide to Enactment LMCE (1996)", United Nations publication Sales No. E.99.V.4, ISBN 92-1-133607-4, pág. 4.

[234] Assim se entendia também nos trabalhos preparatórios. *"It deals not only with the issue of contract formation but also with the form in which an offer and an acceptance may be expressed"*. "A/CN.9/WG.IV/WP.64", pág.s 157 a 171, par. 97.

Parte II – O procedimento de assinatura eletrónica

Capítulo I – Os tipos de assinatura eletrónica

A assinatura eletrónica nasceu como uma resposta das jurisdições dos Estados às necessidades da economia e do tráfego jurídico.[235]

Apesar da rapidez com que se propagou por todo o mundo a regulamentação jurídica da assinatura eletrónica, a realidade económica foi mais veloz e os agentes económicos foram adotando métodos expeditos de autenticação, pelo que foram surgindo ao longo do tempo diversos sistemas e métodos de autenticação, a uma velocidade superior à da produção legislativa.

A assinatura eletrónica não é uma realidade una e irrepetível, mas múltipla e diversa, como também o é a assinatura dos documentos em papel. Existem vários tipos

[235] Como afirma Garnacho: *"Já no princípio da década de 1970 as previsões de crescimento das trocas de informação (económica, financeira, comercial, etc.) evidenciaram a necessidade de dotar essas informações de um instrumento análogo à assinatura manuscrita, dotado, pelo menos, das mesmas funcionalidades desta. Ou seja, de um instrumento que fosse manifestação irrefutável da vontade do emissor da informação e, portanto, dotasse as transações efetuadas através da rede da necessária garantia do não repúdio"*. Garnacho, A.R. (2002); Op. Cit., pág. 1320. No mesmo sentido Gragera: *"A assinatura digital surge como resposta a esta deficiência que por sua vez se manifesta na necessidade de confidencialidade, integridade, identidade e não repúdio nas comunicações através deste tipo de redes"*. Gragera, M.L.D. (2002). Normativa Aplicable a la Firma Electrónica (Directiva 99/93/CE y Real Decreto-Ley 14/1999)". Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., *Régimen Jurídico de Internet*. La Ley. Madrid., pág. 1339.

de assinatura eletrónica e nem todas cumprem as mesmas funções, variando também o grau de segurança de cada um deles.[236]

A vinculação de uma pessoa a um documento eletrónico pode ser efetuada de uma forma mais ou menos segura, dependendo do método de assinatura que for utilizado. Esses níveis de segurança evoluíram à medida que foram aumentando as necessidades de segurança nas transações eletrónicas, e essa necessidade aumentou à medida que se expandiu a utilização das tecnologias eletrónicas na atividade económica. A necessidade de segurança jurídica depende sempre da dimensão e da natureza do risco e da sua perceção e avaliação pelas partes.

É essa realidade multiforme e diversificada que vamos analisar de seguida.

1. A Assinatura mediante digitação do nome

A digitação do nome escrito no final de um documento eletrónico é a mais básica e ancestral forma de autenticação eletrónica. Esse procedimento corresponde a um sinal de uma pessoa, de que é o autor do documento. Ainda hoje é relativamente frequente o envio de mensagem por correio eletrónico, assinando-se o respetivo texto apenas com a menção do nome do seu autor.[237]

A segurança desta forma de autenticação é escassa, dado que não existe certeza de que a pessoa que escreveu um determinado nome é efetivamente quem diz ser. Não existe qualquer prova dessa correspondência e é também praticamente impossível

[236] A abrangência do conceito de assinatura eletrónica é vasta e permite que sejam utilizados diversos meios para assinar, sejam eles símbolos, sons, sinais ou processos. A assinatura é uma manifestação que exterioriza a vontade de vinculação, e essa manifestação pode ter as mais variadas formas, desde a expressão das palavras "aceito" numa gravação, em resposta a uma proposta, até à ação de assinalar num ecrã de um computador a opção de aceitar e de se vincular a uma determinada proposta, até à utilização de outros meios específicos e mais seguros de assinatura. Do mesmo modo, Hatfield e Casamento, *"an electronic signature may consist of an electronic sound or symbol, such as an individual saying 'I agree,' or typing 'I agree' or the person's name or following some other process, such as clicking 'I agree,' which is attached to or logically associated with information inscribed (…)Another form of electronic signature is to say or select 'yes' over the telephone to accept terms and conditions contained in a writing acknowledged by the person so signing"*. Casamento, G. e Hatfield, P.; op. cit, pág. 86.

[237] Daniel Seng cita jurisprudência de Singapura onde se considera assinatura a menção do nome do titular de uma caixa de correio eletrónica, no cabeçalho de uma mensagem eletrónica, bem como nos casos em que o seu autor escreve o seu nome no final da mensagem. Em ambos os casos se considera que essas menções são evidências da vontade do seu autor em se vincular ao seu conteúdo Seng, D. (2008). The Singapore Electronic Transactions Act and the Hong Kong Eletctronic Transactions Ordinance. *Digital Evidence and Electronic Signature Law Review*. Vol 5: pág. 13. Os tribunais superiores entenderam, porém, que a primeira das menções antes referidas não constitui assinatura, porque identifica apenas o autor do envio, nada dizendo acerca da sua vontade de se vincular. Já, porém, a escrita do seu nome no final da mensagem foi considerada como um indício dessa vontade.

garantir-se com segurança ao destinatário de uma mensagem ou de um documento desse tipo que possa comprovar a identidade do seu autor.

A assinatura em forma de nome digitado também não garante que a informação onde foi colocada não foi alterada. Trata-se apenas de um indício cuja força probatória depende de uma avaliação ao caso concreto. Mas trata-se de uma assinatura eletrónica, dado que identifica uma pessoa e a liga aos dados de um conteúdo em forma eletrónica, embora essa ligação possua um poder vinculativo vulnerável, que pode ser facilmente colocado em causa, dadas as múltiplas possibilidades de adulteração a que é suscetível.

2. A Assinatura digitalizada

Trata-se da mera reprodução da aparência gráfica da assinatura manual, copiando-a e colocando-a em cima de um texto ou de um documento eletrónico, podendo depois ser reproduzido todo o documento em papel, com a aparência de ter sido assinado de forma original com a assinatura manuscrita do titular da assinatura.

Com os meios disponíveis é possível a qualquer utilizador reproduzir a assinatura digitalizada de outra pessoa e colocá-la num documento eletrónico, dando a aparência de que quem assinou aquele documento foi a pessoa a quem a assinatura pertence, pelo que se trata de um método inseguro de autenticação.

Este tipo de assinatura é uma espécie de réplica informática da chancela que é usada habitualmente nas empresas e nos serviços. A chancela é um carimbo que uma vez colocado no papel reproduz o aspeto e a aparência gráfica da assinatura de uma pessoa e é utilizada com alguma frequência para autenticar documentos quando a sua quantidade seja muito elevada ou se trate de cópias do mesmo documento. A Lei portuguesa admite o uso de chancela da assinatura de documentos no Código Civil, designando-a de reprodução mecânica.[238]

[238] O n.º 2 do artigo 375.º do Código Civil estabelece que *"Nos títulos emitidos em grande número ou nos demais casos em que o uso o admita, pode a assinatura ser substituída por simples reprodução mecânica"*. O Código de procedimento Administrativo não contém norma idêntica, referindo apenas que do conteúdo dos atos administrativos faz parte essencial a assinatura do seu autor ou do presidente do órgão que o emane (alínea g) do n.º 1 do artigo 151.º). A necessidade de assinatura não é um requisito legal do ato de notificação. O artigo 114.º do CPA não exige que a assinatura seja elemento essencial do conteúdo da notificação, tal como já não a exigia o artigo 68.º anterior CPA. Essa desnecessidade deve advir do facto de o ato administrativo que dá origem à sua notificação já estar assinado. No entanto a assinatura da notificação é um elemento essencial para a sua autenticação e para que o interessado que a recebe possa ter a segurança de que a notificação é proveniente da entidade competente para a fazer.

A utilização de chancela ocorre com frequência nos serviços onde se praticam muitos atos repetitivos e é usada sempre sob o domínio e o conhecimento do autor da assinatura. Não se trata de um método seguro de assinatura de documentos, porque não está garantido o seu carácter estritamente pessoal, que é próprio da assinatura de um documento.

A insegurança da assinatura por chancela é ainda aumentada pela possibilidade da sua fácil reprodução e utilização indevida por terceiros, sendo que essa reprodução pode ser efetuada a partir de qualquer documento assinado.

A automatização de procedimentos das empresas e dos serviços da administração pública, nomeadamente de envio de documentação – cartas de faturação, notificações e outras comunicações, começaram a ser impressas e envelopadas de forma automatizada pelos sistemas informáticos. A forma encontrada pela *praxis* dessas empresas e serviços, para personalizar essas comunicações, foi a de colocarem os sistemas informáticos a colar nesses documentos impressos uma espécie de imagem sobreposta com a fotografia do desenho da assinatura autografa do autor da notificação. O destinatário recebe a comunicação com a aparência de ter sido assinada pelo seu autor, mas não o foi, na verdade. Trata-se, portanto, de uma forma de chancela, só que não é colocada de forma manual pelo autor da assinatura ou por um colaborador seu, mas de forma mecanizada por um sistema informático.[239] É, portanto, na expressão que se nos afigura feliz do Código Civil, uma reprodução mecânica da assinatura, embora efetuada por um sistema informático ou por um computador.[240]

Este tipo de assinatura também não garante a integridade dos documentos onde foi colocada. Na verdade, depois de ser colocada no documento, podem facilmente nele ser introduzidas alterações, pelo próprio ou por terceiros, sem que se possa determinar depois qual é o original autêntico e a versão alterada.

---

[239] Quando se trate de documentos da administração pública, a assinatura digitalizada (ou mecânica na designação do Código Civil), retira-lhes a qualificação de documentos autênticos, porque essa natureza só a têm os documentos *"exarados, com as formalidades legais, pelas autoridades públicas nos limites da sua competência."* (n.º 2 do artigo 363.º do Código Civil). Ora, como uma das formalidades legais dos atos administrativos é a sua assinatura pela entidade competente para os praticar e essa assinatura é a assinatura autografa e pessoal, o documento assinado com a assinatura mecânica só poderá ter a força probatória de um documento particular. Aliás a norma do n.º 2 do artigo 373.º do Código Civil, que prevê a assinatura *"por simples reprodução mecânica"* está inserida na subsecção que regula os documentos particulares e não existe norma correspondente na parte relativa à regulação dos documentos autênticos no Código Civil.

[240] O legislador do Código Civil teve o cuidado de não designar esta *simples reprodução mecânica* por assinatura, estatuindo antes que a assinatura pode ser substituída por essa reprodução mecânica. Assim, na letra da lei, a chancela não é uma verdadeira assinatura, mas apenas uma forma de validação de documentos e de estabelecimento de uma vinculação de uma pessoa a um documento, mas não é uma forma de assinatura.

Como ressalva Linares Gil, a assinatura digitalizada é coisa diferente da assinatura digital.[241]

Trata-se também de uma assinatura eletrónica, mas a sua eficácia jurídica pode ser colocada em causa com relativa facilidade, dada a sua vulnerabilidade a adulterações e utilizações abusivas, sendo possível a sua utilização num contexto de risco baixo, nomeadamente quando as partes se conhecem e confiam mutuamente.

3. A autenticação por palavras-chave ou códigos secretos

A chamada palavra-chave, senha de acesso ou *password* é, provavelmente, nos nossos dias, o meio de identificação e de autenticação mais utilizado nos contactos eletrónicos.

O êxito deste sistema de identificação deve-se, fundamentalmente, à simplicidade do seu uso e ao facto de não ter custos para aos utilizadores.

Trata-se de um tipo de assinatura e de um meio de identificação assente em modelos criptográficos simétricos, que sofre das correspondentes limitações de segurança, em especial nas redes abertas.[242] Essas limitações tornaram-se mais sensíveis quando os sistemas fechados, nomeadamente bancários, que operavam com eles, passaram a operar nas redes abertas.[243]

---

[241] O Autor define a assinatura digitalizada como o processo de *"scanerizar (fazer uma cópia digital através de um scanner ou instrumento de digitalização) a assinatura manuscrita. Não tem nada que ver com a assinatura digital ou numérica…"*, Gil, M.I.L. (2004). Los Interesados en el Procedimiento: La Problemática de las Personas Jurídicas. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid, pág. 731.

[242] Como defende Barriuso Ruíz, *"A autenticação por contra-senhas não é a mais adequada, ainda que seja a mais usada. Para que estas contra-senhas sejam robustas é necessário que se mudem com frequência, que tenham uma longitude suficiente de caracteres (mais de oito), compostas por todos ao caracteres, maiúsculas, minúsculas, números e caracteres especiais, para evitar que sejam descobertas, havendo ainda necessidade de as conservar de forma secreta, mudá-las frequentemente e, em alguns casos, cifrá-las*". Ruíz, C.B. (2006), Op. Cit., pág. 618. Outro instrumento que passou a ser utilizado foi a limitação da validade das palavras-chave, nos casos em que o utilizador erra na sua indicação ao sistema. As organizações passaram a limitar a um máximo relativamente curto a quantidade de tentativas de acesso, normalmente três, findas as quais, se persistir o erro na menção da palavra-chave, o sistema a cancela.

[243] Como bem explicita Gamero Casado, *"este tipo de mecanismo de segurança é muito débil, em face da fácil violabilidade das chaves de acesso por intrusos do sistema, dando lugar ao que tecnicamente se conhece como disfarce ou apropriação da personalidade o que coloca graves reparos ao seu emprego como meio válido de notificação"*. Casado, Eduardo Gamero; Op. Cit., pág. 120, 121.

O método das senhas não cumpre todas as funções da assinatura eletrónica.[244] Embora se possa defender que toda a informação gerada pelo utilizador quando opera com um sistema, depois de se autenticar seja um documento eletrónico[245] que fica autenticado mediante invocação da senha de acesso, a verdade é que essa senha garante que foi uma determinada pessoa que efetuou a transação, mas não garante as restantes funções que são próprias da assinatura eletrónica, nomeadamente a integridade do documento, sua unidade como entidade autónoma e a sua confidencialidade, nem sequer o não repúdio.

Normalmente, no âmbito das convenções prévias de identificação e de autenticação que as partes estabelecem, um delas efetua a geração de um algoritmo que servirá para, de futuro, ser utilizado pela outra parte para se identificar e autenticar a informação que envia. Desse algoritmo faz parte uma chave que é entregue pela parte que a gerou à outra parte, e que é a palavra-chave.

Assim acontece, por exemplo, nas relações estabelecidas entre as entidades bancárias. Depois de identificarem o cliente e o número interno com que o distinguem dos restantes, que pode ser, por exemplo, o número da sua conta bancária, efetuam a geração de um algoritmo matemático que, com recurso a técnicas criptográficas, incorpora dados daquele número de identificação. Desse algoritmo faz parte um conjunto de algarismos que são a chave de acesso do cliente, também designada por palavra-chave.

---

[244] Alguns autores consideram mesmo que, por essa razão, o sistema das senhas ou *password* não é uma modalidade de assinatura digital. É o caso, por exemplo de Ortega Diaz que afirma que "*mais do que uma assinatura digital, este sistema é um meio de identificação"*. Díaz, J.J.O. Op. Cit., pág. 38. Mas a doutrina aceita, na sua larga maioria, que se trata de uma assinatura digital, até pela amplitude da definição desta, constante das legislações do diversos países. Ruíz, C.B. (2006). Op. Cit., pág. 618; Calviño, R.C., Op. Cit, pág.s 39 e 40; Gil, M.I.L. (2003). Modificaciones del Régimen Jurídico Administrativo del Empleo Masivo de Nuevas Tecnologías. En Particular el caso de la Agencia Estatal de Administración Tributaria. Em: Ros, R.M. e Gallego, M.L.M., *Derecho de Internet - La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*. Thomson, Aranzadi, Navarra, pág. 731, 732; Casado, Eduardo Gamero; Op. Cit., pág. 120¸ Más, F.J.G. (2004); Op. Cit., pág. 32. De forma mais concludente Velásquez e Sau afirmam que *"introduzir um código PIN numa caixa automática de uma entidade financeira, enviar por correio eletrónico uma firma manuscrita digitalizada, ou empregar a certificação digital para autenticar dados quando são enviados, podem ser acções suscetíveis de ser consideradas como assinatura digital"*. Velásquez, Raúl Rubio; Sau, Carlos Rodriguez; Muñoz, Ramiro Muñoz; Op. Cit, pág. 31.

[245] Esta consideração de que toda a informação gerada por um operador num sistema quando opera com a sua senha de acesso seja um documento eletrónico não é pacífica, porque não se trata de uma unidade documental, mas de um conjunto de trocas dispersas de informação, que o utilizador nem sequer tem conhecimento que se efetuam. Este apenas faz um conjunto de operações na máquina, sem digitar letras nem exprimir uma vontade em forma de discurso articulado, pelo que não se poderão considerar os registos dessas transações como documentos eletrónicos autenticados pelo operador. Trata-se, seguramente, de registos de atos praticados por uma pessoa identificada, mas não de documentos eletrónicos.

Quando o cliente pretende utilizar os serviços de levantamento automático ou de acesso ao *site* na Internet, invoca a sua identificação. Essa invocação é efetuada, normalmente pela inserção de um cartão ou de um código de identificação (também designado por *user id*). Mediante esta invocação, o cliente está a identificar-se perante o sistema informático, mas para poder aceder com segurança aos dados que pretende, o sistema necessita da prova de que a pessoa que está a operar com ele é mesmo quem diz ser. Para isso solicita a palavra-chave, que uma vez inserida, completa o algoritmo, comprovando assim que se trata mesmo da pessoa que diz ser.

A senha de acesso como método de identificação pessoal pressupõe sempre a existência de uma relação contratual prévia, e serve apenas para identificar as transações efetuadas entre as duas partes dessa relação. Não é possível existir uma senha de acesso para identificar sempre a mesma pessoa em todas as suas relações contratuais ou em todas as suas transações digitais. Na verdade, não se pode dizer que a senha de acesso seja um verdadeiro sistema de identificação digital de uma pessoa. É apenas um método de identificação em determinado tipo de relações específicas, perante uma determinada entidade.

Este sistema possui duas grandes debilidades:

i) Apesar de protegerem as partes contra a intromissão de terceiros, não as protegem de eventuais utilizações abusivas entre elas próprias, uma vez que a parte que é conhecedora do código secreto da outra parte, poderá, com esse código, fazer-se passar pela outra parte e eventualmente gerar documentos em nome dela, de forma maliciosa. Na verdade, a palavra-chave é gerada por uma das partes e entregue à outra para a utilizar nos contactos que com ela estabelece, mas a parte que a emite fica em condições de a conhecer e de a utilizar indevidamente;

ii) Não funcionam adequadamente em redes abertas, dado que a disponibilização do código a vários destinatários aumentaria as possibilidades de ele ser utilizado de forma fraudulenta e, no limite, torná-lo-ia público, acabando assim como segredo e eliminando-se o efeito da segurança da assinatura eletrónica. Este problema foi mitigado pelas empresas que começaram a utilizar de forma mais intensa as transações eletrónicas, estabelecendo uma convenção prévia de autenticação com cada um dos destinatários das suas transações (clientes ou fornecedores). Mas estas soluções têm o inconveniente de tornarem as transações complexas e demoradas, dado

que afastam aqueles clientes das empresas que pretendem efetuar aquisições de forma imediata, sem necessidade de estarem a fornecer os seus dados pessoais à outra parte.

As palavras-chave são meios de assinatura eletrónica, mas têm a debilidade de não garantirem a integridade dos dados que com elas se assinam, pelo que não são meios seguros de assinatura eletrónica nem de identificação.

4. Os métodos biométricos

Os métodos biométricos assentam na utilização de caraterísticas fisiológicas próprias de cada pessoa. Todos nós temos caraterísticas únicas e irrepetíveis que podem ser usadas para nos identificar e nos associar à prática de determinados factos, por exemplo o ADN recolhido de vestígios do corpo humano é usado como método de identificação na investigação criminal.

O método biométrico mais comum de identificação de uma pessoa são as suas impressões digitais, mas também é comum a identificação através da íris, do olhar, da voz e de outras caraterísticas fisiológicas.[246]

O primeiro documento que analisa a possibilidade de utilização de métodos biométricos de identificação e de autenticação, foi o estudo preliminar da UNCITRAL acerca da perfeição dos contratos através de comunicações eletrónicas.[247] Nesse estudo é referido que os métodos biométricos são os mais eficazes métodos de identificação e de autenticação, e são enunciadas as seguintes 6 técnicas biométricas então conhecidas:

i) Através das impressões digitais dos dedos da pessoa;

ii) Através da retina;

iii) Sistemas de quiro-geometria, que analisam o comprimento dos dedos, a largura da mão e a translucidez da pele;

iv) Através da voz, mediante dispositivos que gravam a voz e analisam o tom sonoro utilizado pela pessoa e as suas inflexões;

[246] Barriuso Ruiz faz um extenso elenco dos métodos biométricos de identificação, nomeadamente *"as impressões digitais, o reconhecimento do ADN, a geometria da orelha, da cara, da mão, as veias da mão, a iris e a retina oculares, o movimento do corpo, o timbre e as características da voz, a pulsação, a sintaxe, a grafologia da escrita manual ou nas teclas mecanográficas, a assinatura manual, gestos e movimentos corporais ou outros, como a análise do suor ou do odor, etc.."*. Ruíz, C.B. (2006). Op. Cit., pág. 608.

[247] "EDI, Electronic Data Interchange. Preliminary Study of Legal Issues Related to the Formation of Contracts by Electronic Means. Report of the Secretary-General." A/CN.9/333, 18 May 1990.

v) Através da análise da morfologia da assinatura manuscrita, utilizando técnicas de análise estática e dinâmica;

vi) Através da análise da forma como determinada pessoa utiliza o teclado do computador, nomeadamente analisando o ritmo de escrita e de utilização das teclas.

Para que funcione este sistema de autenticação, é necessário que os sistemas informáticos contenham um registo prévio da caraterística que foi selecionada. [248] Depois, quando o seu titular for efetuar cada uma das transações, o sistema compara a caraterística que tem registada com a apresentação que ele terá que fazer, dessa mesma caraterística. Caso exista identidade, será validada a autenticação e em caso negativo isso não ocorrerá.

Este método tem a vantagem de ser estritamente pessoal, não exige memorização e acompanha sempre o seu titular, porque é pessoal e inseparável, sendo essa uma importante caraterística que separa esta modalidade das duas que analisámos anteriormente.[249] Por essa razão, a utilização destes métodos é relativamente segura, porque é mais difícil a falsificação, dada a pessoalidade e a irrepetibilidade dos atributos que servem de instrumento da identificação e da autenticação. Nesse sentido se exprime Barriuso Ruiz de forma conclusiva: *"os traços biométricos não se podem perder, nem esquecer, dificilmente se falsificam nem se deixa constância deles em suportes digitais legíveis"*.[250]

Os métodos biométricos têm importantes vantagens e caraterísticas que lhe permitem garantir o carácter pessoal da assinatura eletrónica, bem como a simplicidade necessária para permitir a sua rápida expansão, mas trata-se ainda de uma tecnologia

[248] *"Six biometric technologies are currently available: retina scans which record the eye signature of an individual and store it in a microprocessor; thumbprint or fingerprint identification systems; hand geometry systems which measure, record and compare finger length, skin translucency, hand thickness or palm shape; voice verification devices which record voice patterns and inflections; signature verification devices which trace either the static or dynamic characteristics of a person's signature; keystroke dynamics which identify individuals by their typing patterns and rhythms"*. "A/CN.9/333", par. 55.

[249] Como afirma Diego Cruz Rivero, "*actualmente existem dois tipos de assinaturas digitais cujos meios para a sua criação se encontram em poder exclusivo do assinante: as assinaturas digitais biométricas e as assinaturas digitais de chave assimétrica. As primeiras são aquelas que utilizam informação de partes do corpo do próprio assinante e que são específicas deste: retina, impressões digitais, voz, etc."*. Rivero, D.C. (2006). *La Firma Electrónica Reconocida - Análisis de los Requisitos del Artículo 3,3 de la Ley 59/2003, de 19 de Diciembre, de Firma Electrónica*. Colegios Notariales de España. Madrid., pág. 50.

[250] Ruíz, C.B. (2006), Op. Cit., pág. 609.

não devidamente explorada, não tendo ainda atingido a maturidade suficiente para a sua generalização.[251]

Apesar disso os métodos biométricos são já utilizados como instrumento de identificação nos passaportes, em resultado da aprovação do correspondente regulamento europeu.[252]

Uma das razões que impediu o crescimento da utilização dos métodos biométricos foi o seu elevado custo, nomeadamente de leitura e armazenamento das caraterísticas fisiológicas das pessoas, bem como dos sistemas de reconhecimento.[253]

Nos últimos anos a biometria tem conhecido importantes avanços, e é possível que venha a generalizar-se a sua utilização, podendo inclusivamente essa generalização ocorrer mediante a conjugação com outros elementos caraterísticos de outros tipos de assinatura, como é o caso da assinatura digital.[254]

Os métodos biométricos são mais frequentemente utilizados como meio de identificação de pessoas do que como meio de autenticação de documentos, dada a dificuldade de garantirem a sua integridade.

5. A assinatura digital

A assinatura digital é reconhecidamente o método mais completo e evoluído de assinatura eletrónica, sendo à sua volta que se formou toda a legislação que a nível internacional regula a assinatura eletrónica. Essa completude resulta do facto de a assinatura digital ter sido construída como resposta às necessidades de segurança jurídica na utilização plena das tecnologias da informação e da comunicação, nomeadamente das redes abertas.

---

[251] *"As técnicas biométricas estão ainda num estado incipiente"*. González, N. R. (2007). La Utilización de las Nuevas Tecnologías en las Relaciones Entre las Administraciones Públicas y los Ciudadanos (En Particular, Registros Telemáticos y Notificaciones Telemáticas): Hacia un Cambio de Modelo. *Revista Española de Derecho Administrativo*, n.º 133, Enero - Marzo 2007. Editorial Thomson – Civitas. Navarra., pág. 116.

[252] Regulamento (CE) N.º 2252/2004 do Conselho, de 13/12/2004.

[253] Essa é uma das razões invocadas no texto a que antes nos referimos, da UNCITRAL: *"... except for biometric techniques, which are currently too expensive for general commercial use ..."*. "A/CN.9/333", pág. 17, par. 56.

[254] *"Caminhamos a passos largos para a introdução da biometria técnica de identificação de indivíduos a partir das suas características fisionómicas e/ou comportamentais. São características capazes de os identificar com precisão, seja através da informação fornecida pela leitura das suas impressões digitais, da informação fornecida pela sua íris ocular, ou ainda através da informação fornecida pela palma das suas mãos"*. Rodrigues, D. (2015, 9 de julho). *A identificação Biométrica: Ficção e Realidad*e. Público, pag 34.

Os modelos de identificação e de autenticação existentes antes da assinatura digital revelaram-se insuficientemente seguros no paradigma funcional das redes abertas e na plena utilização destas redes na atividade comercial.

A assinatura digital é também o resultado do conhecimento produzido pela evolução do funcionamento das redes eletrónicas, pelo conhecimento jurídico e pela evolução da matemática, e a sua conceção pretende dar resposta adequada às dificuldades de segurança dos restantes métodos de assinatura eletrónica.

A designação de assinatura digital advém da sua natureza de método que opera com os dígitos da linguagem binária de que se compões os documentos.

A assinatura digital é a única que, como veremos de seguida, cumpre todas as funções jurídicas inerentes a uma assinatura, sendo essa a razão por que foi adotada em todas as legislações que conhecemos, como o método mais seguro de assinatura.[255]

5.1. A utilização da criptografia

A assinatura digital utiliza a criptografia como instrumento de vinculação e autenticação, tal como a tecnologia das palavras-passe. Mas enquanto esta última utiliza a criptografia simétrica, a assinatura digital utiliza a tecnologia das chaves assimétricas.

A função da criptografia é a ocultação da informação e opera mediante a utilização da chave pública (suscetível de ser conhecida por qualquer pessoa) para encriptar e uma chave privada (do conhecimento exclusivo do seu titular) para desencriptar.

O titular da chave privada, secreta, é a única pessoa capaz de ler o conteúdo original dos documentos encriptados que lhe são enviados, porque só ele os pode desencriptar. Sendo ele o titular exclusivo dessa chave privada, mais ninguém pode aceder ao conteúdo das mensagens que lhe são enviadas sob a encriptação da sua chave pública.

[255] Como afirmam Blanco e Avelló, *"De entre todos os instrumentos que se experimentaram no passado para garantir a confiança nas transações digitais (chaves secretas, identificação biométrica mediante o reconhecimento da voz ou das impressões digitais a utilização de uma mesma chave para encriptar ou desencriptar uma mensagem ...) a assinatura digital baseada no uso de chaves assimétricas ou criptografia de chave pública é a que melhor satisfaz as exigências de segurança, e confiança que exigem as comunicações digitais".* Blanco, C. L. e López, L.A. (2004). El Uso de la Firma Electrónica por las Administraciones Públicas: Nuevos Modelos de Relación de Calidad en la Gestión Pública. Em: *Ministerio de Economia. Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid, pág. 25

Ora, a assinatura digital utiliza também a criptografia assimétrica, mas inverte a utilização das chaves. Na criptografia o titular da chave privada recebe documentos encriptados de terceiros, na função assinatura esse titular emite documentos encriptados para terceiros, pelo que:

i) A chave privada passa a ser utilizada, já não para desencriptar, mas para encriptar;

ii) A chave pública passa a ser utilizada, já não para encriptar, mas para desencriptar;

Tal como na função típica da criptografia, a chave privada é de acesso exclusivo pelo seu titular, podendo a chave pública ser partilhada, e ser inclusivamente de conhecimento universal.

Quando o titular da chave privada emite um documento encriptado por esta, qualquer terceiro que o receba o pode desencriptar com a chave pública correspondente. Como ambas as chaves desencriptam o que a outra encripta, ao fazer essa desencriptação, o destinatário adquire a certeza de que aquele documento só pode ter sido encriptado por uma chave, e que essa chave é a que está matematicamente relacionada com a chave pública que utilizou para desencriptar o documento. Essa certeza é dada por dois factos distintos:

i) Porque a chave pública está matematicamente relacionada com a chave privada;

ii) Porque a chave privada é de acesso exclusivo a uma só pessoa, o seu titular.

Na assinatura digital, a utilização da criptografia não serve para os seus fins típicos, de ocultação da informação constante dos documentos assinados, mas como forma de se obter segurança de que a pessoa que encriptou um determinado documento, é mesmo aquela que diz ser, e não outra que por ela se faz passar indevidamente. A assinatura passa a ser essa operação de encriptação e, mediante ela, o destinatário de um documento fica a saber com segurança quem é o seu autor.

Os tipos de assinatura que utilizam a criptografia como instrumento de garantia de segurança da vinculação de uma pessoa a um conjunto de dados, não o fazem para ocultar esses dados. O conhecimento que dela se utiliza para os fins da autenticação é apenas o próprio método criptográfico, ou seja, a detenção de uma chave criptográfica exclusiva, pessoal, confidencial e única, por uma pessoa. A utilização dessa chave encripta dados, mas essa encriptação não é um fim em si mesmo. É um meio. E é um

meio para se atingir um fim, que não é o de ocultar a informação, nem podia ser, porque assinar um documento não tem relação jurídica com a sua ocultação. Autenticar e guardar sigilo acerca da informação assinada são funções distintas.

A criptografia é utilizada como instrumento de assinatura eletrónica, apenas para dois fins – encriptar e desencriptar. Essas operações não servem a finalidade de ocultar informação, mas servem para revelar quem foi a pessoa que efetuou a operação de encriptação. Deste modo, a criptografia é utilizada para um fim que lhe é colateral, que é o de revelar a identidade de quem efetuou uma operação de ocultação de informação, encriptando um documento, e não para aquele que é o seu objeto principal, que é a ocultação da informação desse documento.

Utilizando a assinatura digital o conhecimento e os instrumentos da criptografia para assegurar a vinculação de documentos a pessoas e não especificamente para ocultar a informação, também essa função pode ser associada à assinatura digital nos casos em que ela se revele necessária. Nesses casos pode utilizar-se a criptografia para esse fim, mas essa utilização é externa e separada da função da assinatura.

5.1.1. Na vinculação de dados ao seu autor

Uma chave privada é uma fórmula matemática fixa, que uma vez aplicada a um conjunto de dados os altera, como ocorre com qualquer aplicação de uma fórmula matemática a quaisquer dados. Essa chave privada é gravada num suporte magnético, um cartão, um ficheiro num computador, contendo um pequeno aplicativo. Quando o seu titular dá ordem a um computador para aplicar essa chave sobre um documento eletrónico, o aplicativo desencadeia uma operação de aplicação da fórmula matemática que integra a chave privada, aos dados digitais que constituem o documento. Desse procedimento resulta a produção de um novo documento, que é o documento encriptado.

A chave privada é, então, um método de encriptação, e ela encripta sempre da mesma forma. Esse modo de encriptação carateriza-se pelo facto de ser suscetível de ser desencriptado pela chave pública que está com ela relacionada. Por essa razão, esse modo de encriptação constitui a evidência de que essa encriptação foi efetuada por aquela chave privada e não pode ter sido efetuado por qualquer outra. Trata-se de um sinal, uma marca.

Essa marca tem que estar ligada de forma segura a uma pessoa, para poder ser considerada uma assinatura. [256] E para isso é necessário ter-se a certeza de que só essa pessoa tem acesso à chave privada que produz aquele resultado.[257]

A segurança da conexão entre a chave privada e o seu autor é uma exigência crítica da assinatura eletrónica. E para que ela exista é necessário que se garanta exclusividade no acesso à chave privada, pelo seu titular.

Para que essa exclusividade se mantenha, a chave privada deve constar de um suporte magnético, que pode ser um cartão, um CD ou um suporte portátil, que possa ser conectado com o computador quando o seu titular pretenda efetuar a assinatura de um documento. O acesso a esse suporte deve, também ele ser protegido por uma outra chave, a que também só deverá aceder o respetivo titular. O titular da assinatura deve ter o cuidado de garantir que mais ninguém possa ter acesso ou utilizar a chave privada constante desse suporte.[258]

5.1.2. A possibilidade de partilha livre da chave pública

Também no paradigma do papel cada pessoa possui uma forma específica, única e irrepetível, de colocar a sua assinatura autógrafa e manuscrita num documento. E, salvo imitação ilícita, só essa pessoa possui a capacidade para colocar a sua assinatura num documento, porque só ela possui o conhecimento e as faculdades intelectuais e fisiológicas para colocar no papel a sua assinatura autógrafa com a configuração com que o faz. Com as assinaturas eletrónicas devem cumprir-se os mesmos princípios, pelo que só o autor ou subscritor deve possuir o conhecimento

[256] A ideia da utilização de um código secreto ou chave secreta vinha já de outros tipos de assinatura eletrónica, mas o conceito de "Chave Privada" foi utilizado pela primeira vez nos trabalhos na conceção do sistema das CMI Rules, como instrumento de segurança eletrónica dos documentos eletrónicos de transporte marítimo. A UNCITRAL passou a utilizá-lo a partir de 1996. *"Together with the receipt, the carrier transfers to the shipper a secret code ("private key") to be used for securing the authenticity and integrity of any future instruction to the carrier regarding the goods. The private key can be any technically appropriate code, such as a combination of numbers or letters that the parties might agree on"*. "A/CN.9/WG.IV/WP.69", par. 74. O conceito de chave privada viria a ser muito importante na construção da assinatura digital.

[257] "*Digital signatures are created and verified by using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and back into the original form"*. "A/CN.9/493", par. 36.

[258] *"Such a private key is likely to be kept on a smart card, or to be accessible through a personal identification number or through a biometric identification device, e.g., through thumbprint recognition"*. "A/CN.9/493", par. 38.

necessário para operar sobre o documento de uma determinada forma. E essa certeza é essencial.

No comércio tradicional praticamente não é necessária qualquer convenção prévia de identificação e de autenticação.

Essa simplicidade teria necessariamente que ser transportada para o comércio eletrónico, proporcionando as condições para que cada agente que efetua transações eletrónicas seja portador da sua identidade eletrónica e dos instrumentos necessários para a sua comprovação, sempre que seja solicitada para tal, sem ter necessidade de estabelecer convenção prévia de autenticação.

Essa autonomia de identificação e da sua demonstração não é compatível com os modelos tradicionais de assinatura eletrónica assentes na partilha de um segredo, dado que esse segredo teria que ser criado e partilhado antes da realização das transações eletrónicas correspondentes.

Para que exista segurança efetiva não é possível a partilha da chave de encriptação, sendo necessário que o instrumento criptográfico que foi colocado pelo autor no documento não tenha que ser revelado aos destinatários e eventualmente a terceiros. E isso só foi possível com a criptografia das chaves assimétricas. Uma vez que a chave de desencriptação está relacionada apenas com uma chave de encriptação e apenas com essa, o ato de desencriptação revela que aquele documento só pode ter sido encriptado pela chave com a qual está relacionada. [259]

A chave de desencriptação pode, portanto, passar a ser do conhecimento de qualquer pessoa, pelo que se designa de chave pública.

5.1.3. A autonomização da ação do emissor e do destinatário

A assinatura digital veio permitir que o autor dos documentos tenha autonomia para os produzir, autenticar e comunicar, pelo que passou a poder emitir documentos eletrónicos que o vinculam de forma exclusiva, sem necessidade de conhecer previamente os seus destinatários. Pode, nomeadamente, efetuar ofertas negociais eletrónicas, que podem ser aceites por qualquer interessado.

[259] *"One such key is used for creating a digital signature or transforming data into a seemingly unintelligible form, and the other one for verifying a digital signature or returning the message to its original form"*. "A/CN.9/493", par. 36.

Do mesmo modo qualquer pessoa pode verificar a autenticidade de um documento com uma assinatura digital, bastando para isso que conheça a chave pública do autor desse documento, sendo certo que o conhecimento da chave pública passou a ser facilitado pelo facto de ela não proporcionar em caso algum o acesso à chave privada que com ela está relacionada. O destinatário do documento efetua também a verificação da assinatura de forma autónoma, sem depender de qualquer comunicação do seu autor.

Fica, assim, aberta a possibilidade de serem realizados negócios jurídicos por meios eletrónicos, com segurança e validade e eficácia jurídicas, mesmo entre partes que não se conhecem, passando desta forma o comércio eletrónico a poder ser simples e a realização das operações a ser praticamente imediata.

5.1.4. A função *Hash*

Instrumento fundamental de segurança das assinaturas digitais é a inviabilidade de a partir da chave pública se poder descobrir, por derivação, a chave privada. Caso isso acontecesse poderiam terceiros passar a emitir documentos encriptados com essa chave, fazendo-se passar, de forma ilícita, pelo seu verdadeiro titular.

Essa possibilidade existirá sempre, pelo menos teoricamente, dado o poder de cálculo dos sistemas informáticos para, mediante tentativas sucessivas, que até poderiam ser automatizadas, efetuarem essa determinação da chave privada. A mesma tecnologia que permite construir criptogramas de elevada complexidade e segurança, pode também ser utilizada para, ao serviço de fins menos nobres, descobrir o segredo das chaves privadas, num movimento inverso. Designa-se de força bruta esta colocação em funcionamento de sistemas informáticos com programação própria para, operando sistematicamente, por tentativas sucessivas, derivem a chave privada dos documentos eletrónicos anteriormente assinados com a assinatura digital.

Para evitar essa determinação, os algoritmos de criação das chaves devem ser longos e matematicamente complexos, utilizando números aleatórios que exponenciem as necessidades de cálculos probabilísticos em série, que tornam praticamente inviável, em tempo útil, aquela derivação das chaves privadas. A dimensão dessa complexidade

deve ser tal, que a capacidade computacional existente não permita essa determinação em tempo útil.[260]

Mas essa complexidade tem como consequência que o algoritmo de encriptação tem que ser, também ele, de elevada complexidade, o que provoca uma ocupação intensa de recursos informáticos dos sistemas e tempo de demora na encriptação dos documentos eletrónicos, sempre que o seu autor os pretende assinar.[261] E isso acontece porque o sistema informático terá que efetuar uma vastidão de operações complexas, que são demoradas e ocupam recursos desse sistema. [262] Esta ocupação é problemática quando se opera na Internet em que a velocidade dos processamentos é muito importante. Quando os documentos eletrónicos a assinar são longos, essa complexidade é ainda maior.

Para evitar essa demora existem duas possibilidades:

i) Diminuir a complexidade e a longitude do algoritmo de encriptação que utiliza a chave privada, o que não é recomendável porque diminui a segurança;

ii) Diminuir o documento sobre o qual vai ser aplicada a chave privada, para que esta incida sobre uma pequena quantidade de dados, assim tornando as operações mais rápidas.

Foi esta segunda opção que foi adotada, pelo que, antes da aplicação do algoritmo com a chave privada pelo autor do documento para o assinar, existe uma operação que resume o documento que se pretende assinar, a uma pequena base, que

---

[260] Lucena López elucida o grau de segurança destas chaves do seguinte modo: *"Os algoritmos criptográficos usam chaves com um elevado número de bites, e usualmente mede-se a sua qualidade pela quantidade do esforço que se necessita para os descobrir. O tipo de ataque mais simples [que é usado para os descobrir] é a chamada 'força bruta', que simplesmente consiste em ir por tentativas sucessivas, tentando descobrir uma das chaves. Por exemplo o algoritmo DES tem 2^{56} possíveis chaves. Quanto tempo gastaríamos a tentar verificá-las todas se, por exemplo, dispuséssemos de um computador capaz de fazer um milhão de operações por segundo? Demoraríamos ... mais de 2200 anos! Mas se a chave do exemplo anterior tivesse 128 bits? O tempo requerido seria de 10^{24} anos"*. López, M.J.L. (2009). Op. cit.; pág. 27.

[261] Como nos diz Lucena Lopez, *"os algoritmos assimétricos empregam geralmente chaves de longitude muito mais longa que os simétricos (...) a complexidade de cálculo que comportam (...) torna-os consideravelmente mais lentos que os algoritmos de encriptação simétricos"*. López, M.J.L. (2009). Op. cit.; pág. 177.

[262] Como se descrevia nos trabalhos da UNCITRAL, *"Certain existing standards such as the ABA Digital Signature Guidelines refer to the notion of "computational unfeasibility" to describe the expected irreversibility of the process, i.e., the hope that it will be impossible to derive a user's secret private key from that user's public key. "'Computationally unfeasible' is a relative concept based on the value of the data protected, the computing overhead required to protect it, the length of time it needs to be protected, and the cost and time required to attack the data, with such factors assessed both currently and in the light of future technological advance" (ABA Digital Signature Guidelines, p. 9, note 23)"*. "A/CN.9/493", nota 10.

designaremos de "função resumo" (ou *hash* em Inglês).[263] Esse resumo obtém-se mediante a realização de uma operação prévia de sintetização, que é, também ela própria, uma encriptação.

A chave privada não será aplicada a todo o documento, mas apenas a um pequeno resumo dele.

Analisemos então como se efetua esta operação prévia de construção do resumo. Ele é obtido também, mediante um algoritmo matemático de criptografia, que é diferente da chave privada. Esse outro algoritmo opera sobre o documento eletrónico completo que se pretende assinar e gera uma sequência binária de símbolos, que é o resultado da encriptação efetuada. Trata-se de um novo documento, paralelo ao documento eletrónico original, mas muito mais pequeno do que este.[264] Este documento de resumo é obtido com relativa rapidez, porque a chave de encriptação que é utilizada para o obter é de natureza simétrica.

É sobre este documento eletrónico de resumo, designado de *hash*, que se vai aplicar a chave privada do respetivo autor ou subscritor. Ao contrário do que se possa pensar, essa chave privada não se aplica ao documento eletrónico completo, mas ao *hash*, que é um resumo dele.

Temos então que quando alguém aplica a sua chave privada para assinar um documento eletrónico, são efetuados dois procedimentos diferentes e separados em termos temporais:

i) O primeiro consiste na aplicação de uma chave simétrica de encriptação, que opera sobre o documento que se pretende assinar eletronicamente e gera o chamado *hash*;

ii) O segundo, que consiste na aplicação a esse *hash* da chave privada da assinatura eletrónica.[265] É este o momento em que se completa o procedimento de assinatura do documento pelo respetivo autor ou signatário.[266]

---

[263] A função *Hash* é também designada por "função de controlo", "função resumo", "função de controlo unidireccional", "impressão digital da mensagem". "A/CN.9/493", par. 40.

[264] Na definição de Baygual, o processo de criação do *hash "é uma função introduzida para reduzir o volume de memória utilizada no processo de dados, fazendo um 'resumo matemático' documento ou da mensagem a assinar"*. Baygual, Francesc A. Op. Cit., pág.s 1284.

[265] *"The signatory's software then transforms the hash result into a digital signature using the signatory's private key. The resulting digital signature is thus unique to both the information being signed and the private key used to create the digital signature"*. "A/CN.9/493", par. 41.

[266] A aplicação da chave privada do titular da assinatura eletrónica não opera sobre o texto completo (designado texto em claro) no seu todo, mas apenas sobre o *hash*. É por essa razão, que não se aplicando a chave privada diretamente sobre ele, não seja encriptado e possa circular completamente legível e aberto.

Na verdade o autor não assina o documento inicial, mas sim o resumo encriptado desse documento a que chamamos *hash*.[267]

Esta dupla encriptação garante a maior rapidez dos processamentos informáticos e que ocupem menos recursos, sem prejuízo da segurança.[268] Aplicada apenas a uma pequena sequência de dígitos resultantes de uma encriptação intermédia já efetuada por outra chave mais curta, ocupará menos recursos e será menos demorada.[269]

5.2. A função dos prestadores de serviços de confiança eletrónica

A separação das chaves privada e pública, a autonomização do seu funcionamento e das operações de quem assina e de quem verifica a assinatura, permitem que o sistema funcione sem necessidade de conhecimento nem contacto prévio entre as partes, mas levanta ainda dois problemas:

i) Quem vai criar e emitir os pares de chaves, privada e pública;[270]

Essa circulação não compromete em nada o segredo da chave privada, porque ela não se aplicou diretamente a esse documento. *"The text being electronically signed, although it also plays an important role in the signature-creation process (through a hash function or otherwise), should obviously not be subject to the same confidentiality as the information identifying the signatory*". "A/CN.9/WG.IV/WP.88", par. 96.

[267] É importante termos em conta que tanto a chave privada como a chave simétrica que resume o documento de base no *hash*, não operam sobre a representação gráfica dos documentos respetivos. Essas chaves operam sobre a estrutura digital binária de dados dos documentos, ou seja, sobre os dígitos de zero e um que constituem a sua estrutura na linguagem dos computadores.

[268] *"Na prática os métodos assimétricos empregam-se unicamente para codificar a 'chave de sessão' (simétrica) de cada mensagem ou transacção"*. López, M.J.L. (2009). Op. cit.; pág. 177. *"Hash functions therefore enable the software for creating digital signatures to operate on smaller and predictable amounts of data, while still providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it was digitally signed"*. "A/CN.9/493", par. 40.

[269] A assinatura digital utiliza assim, de forma conjugada, as vantagens da criptografia simétrica e assimétricas, aproveitando a simplicidade da primeira e a segurança da segunda. Como refere, Velásquez, Sal e Muñoz, *" Na prática a criptografia simétrica e assimétrica combina-me para aproveitar as características de cada uma. A criptografia assimétrica ou de chave pública tem a desvantagem de consumir mais recursos [informáticos] que a criptografia simétrica. Se queremos encriptar uma mensagem mais extensa, o mais lógico será fazê-lo mediante um algoritmo simétrico, que costumam sem muito eficientes; mas para enviar o documento que assinámos devemos fazê-lo mediante criptografia assimétrica …"*. Velásquez, R.R., Sau, C.R. e Muñoz, R.M. (2004). Op. cit., pág. 184.

[270] O conceito de utilização de uma chave privada por uma entidade terceira foi, pela primeira vez, concebido no âmbito dos trabalhos de conceção da LMCE para os documentos de transporte marítimo eletrónicos (*bill of lading*), em que uma entidade responsável por um registo da titularidade das mercadorias, emitia um código secreto para o respetivo titular, que seria cancelado se este transmitisse a sua propriedade, sendo nesse caso emitida nova chave privada ao adquirente e assim sucessivamente. *"Under the CMI Rules, it was the carrier who had the registry function in the sense that the carrier gave a unique secret code ("private key") to the shipper and that the shipper, by possessing that private key, was the only person holding the control of, and the title to, the goods, until, by using that private key, the shipper instructed the carrier to cancel the issued private key and issue a new and unique private key to a new holder of those rights"*. "A/CN.9/421", par. 41.

ii) Como se conexiona um par de chaves com uma pessoa em concreto que seja o seu titular. É que, do que expusemos até aqui, o destinatário da mensagem desencripta-a com a chave pública verificando assim que ela foi encriptada pela chave privada que lhe corresponde. Mas isso não lhe permite saber quem é a pessoa em concreto que detém aquela chave privada, e esse conhecimento é essencial para a vinculação jurídica dessa pessoa ao documento eletrónico.

Tanto a emissão do par de chaves como a sua vinculação a uma pessoa determinada são funções exercidas por uma entidade terceira, especializada em prestar serviços de confiança jurídica no domínio das comunicações eletrónicas. Essas funções são da mais elevada importância para a fiabilidade das assinaturas eletrónicas, pelo que essas entidades devem possuir credibilidade e idoneidade suficiente para garantir dois atributos essenciais:

i) A segurança do procedimento de emissão do par de chaves;

ii) A confidencialidade da chave privada, a exclusividade do acesso a ela pelo respetivo titular, e a identificação deste.

Os prestadores de serviços de confiança possuem a credibilidade necessária para que todos os agentes neles confiem, devendo a sua atividade ser auditada e certificada por outras entidades, assim se garantindo uma cadeia segura de confiança e de credibilidade.

Quando emitem um par de chaves e o entregam ao respetivo utilizador, essas entidades emitem um certificado, que é um documento eletrónico. Esse certificado é uma declaração formal dessa entidade, que garante a todos os interessados que aquele par de chaves pertence à pessoa que identifica como tal.

Normalmente o certificado acompanha o documento eletrónico assinado com a chave privada do respetivo autor ou subscritor. Através dele qualquer pessoa que assim o pretenda, pode, na presença do documento eletrónico assinado, verificar a identidade da pessoa que invoca ter assinado o documento e, mediante a aplicação da chave pública, confirmar que a encriptação foi efetuada pela chave privada correspondente. Assim se confirma que o autor ou subscritor daquele documento é o titular daquela chave privada, com a identificação que consta do certificado.

5.3. O resultado da assinatura de um documento eletrónico

Quando geramos um documento eletrónico e o assinamos com uma assinatura digital, estamos a produzir em simultâneo três documentos separados, mas ligados entre si, que em caso de envio por comunicação eletrónica seguem também para o destinatário:

i) O documento original, tal como o elaborámos perfeitamente legível e, portanto, não encriptado. Este documento é designado de *"documento em claro"*, tal qual como foi produzido inicialmente pelo seu autor. Esse documento não apresenta nenhuma transformação, e por isso, não está assinado, quando analisado autonomamente. O "*documento em claro*" pode ser de vários tipos, por exemplo, um texto escrito perfeitamente legível, uma folha de cálculo, uma imagem desenhada num computador ou resultante da transposição de outro suporte, por exemplo, uma fotografia; um filme que tenha sido efetuado num sistema informático ou através de uma gravação digitalizada, uma reprodução sonora, etc.[271]

ii) Um documento à parte e que, esse sim, é o documento assinado com a assinatura digital, que resultou das seguintes operações de transformação desse documento em claro:

   a. Uma primeira encriptação com uma chave simétrica que produziu o *hash*;

   b. Na segunda operação, aplica-se ao *hash* que acabamos de referir, a chave privada do autor do documento. Podemos dizer que o autor do documento não assina eletronicamente todo o documento inicial, a que chamamos documento em claro. Ele assina apenas o *hash* desse documento.

iii) - O certificado de assinatura eletrónica, emitido pelo prestador de serviços de certificação que o emitiu. Esse certificado identifica quem é o titular da assinatura digital e contém a chave pública respetiva.

[271] Todos estes documentos podem ser documentos eletrónicos porque, como vimos, podem ser convertidos em suporte digital, e a partir daí suscetíveis de serem objeto de processamento informático. A sua digitalização envolve a composição, na linguagem binária dos computadores, em sequências de dígitos de um e zero. Sobre essas sequências podem ser efetuados vários processamentos informáticos. Um desses processamentos pode ser a aplicação de um algoritmo matemático que os encripte.

Estes três documentos formam um conjunto único e inseparável, a partir do momento em que o autor do documento aplica a chave privada sobre o resumo resultante da aplicação da função *hash*. É nesse exato momento que o documento se considera eletronicamente assinado.

5.4. O procedimento de verificação da assinatura eletrónica do destinatário

Analisemos agora as operações de verificação da assinatura efetuadas pelos destinatários dos documentos.

5.4.1. A verificação da autenticidade e da identidade

O destinatário de um documento eletrónico assinado com assinatura digital recebe os três documentos anteriormente referidos.

Caso pretenda analisar desde logo o documento em claro pode fazê-lo, por exemplo procedendo à sua leitura, se se tratar de um texto, porque ele se apresenta com a mesma configuração com que o seu autor o elaborou.[272]

Caso pretenda verificar quem é a pessoa que está vinculada àquele documento, deve ser conhecedor da chave pública de quem diz ser o seu autor ou subscritor. Esse conhecimento obtém-se nos locais onde a chave pública está disponibilizada, sendo que inicialmente constava de diretórios de acesso público, mas mais tarde passou a ser prática corrente faze-la constar do próprio certificado que acompanha o documento com a assinatura eletrónica que foi enviado.[273]

Conhecedor dessa chave pública, o destinatário aplica-a ao *hash* que está encriptado com a chave privada e verifica que o seu computador desencripta esse documento com sucesso.

---

[272] A confidencialidade não é uma função da assinatura, tal como na correspondência normal em papel, a confidencialidade não resulta da sua assinatura, mas da colocação do documento num envelope fechado. Porém, a tecnologia da assinatura digital permite que se garanta confidencialidade nas comunicações eletrónicas, como veremos no capítulo referente às funções da assinatura eletrónica.

[273] *"If many people need to verify the signatory's digital signatures, the public key must be available or distributed to all of them, for example by publication in an on-line repository or any other form of public directory where it is easily accessible"*. "A/CN.9/493", par. 38.

Esse resultado permite constatar que aquele *hash* só podia ter sido encriptado pela chave privada que corresponde à chave pública que o desencriptou.

Dado que o destinatário sabe, através do certificado, que aquela chave pública pertence a uma pessoa determinada e nele identificada, fica também a saber quem foi o autor ou subscritor do documento.

Conclui-se aqui o percurso metodológico de determinação da vinculação jurídica de um autor ou de um subscritor a um documento eletrónico.

5.4.2. A verificação da integridade dos documentos eletrónicos.

Acabamos de constatar que o autor do documento não aplicou a sua chave privada sobre toda a extensão desse documento (o *documento em claro*), mas apenas sobre uma síntese desse documento, mas que é, ele mesmo, um documento à parte.

Mas se assim é, só existe a certeza de que o *hash* não foi alterado desde aquele momento em que nele foi aplicada a chave privada do autor do documento. E sendo assim, como pode o destinatário do documento ter a certeza de que o documento, tal como foi elaborado, que designamos documento em claro, não foi alterado ele próprio?

Essa é uma outra função da assinatura digital, que é diferente da função de identificação e da função de autenticação. Averiguar se o documento em claro foi alterado desde que foi enviado pelo remetente, é averiguar se se cumpre a função integridade. Esta é também uma função típica da assinatura eletrónica.

Quando o destinatário recebe o documento assinado eletronicamente, aplica sobre o *hash* encriptado que recebeu, a chave pública do autor. Em resultado dessa operação obtém esse *hash* desencriptado. Com essa desencriptação, fica também acessível ao destinatário a mesma chave simétrica que havia sido anteriormente utilizada pelo autor para gerar o *hash* (recordemos que o autor ou subscritor formou o *hash* aplicando sobre o documento em claro, esta mesma chave simétrica).

De seguida, conhecedor da chave simétrica, com que o autor havia encriptado o respetivo texto original e havia gerado a função *hash*, o destinatário da mensagem pode aplicar de novo essa chave simétrica ao documento em claro. Dessa aplicação resultará de novo um *hash*, que há de ser igual ao que o autor havia formado inicialmente para obter esse resumo do documento em claro, que é o *hash* inicial.

Fica então o destinatário com dois resumos resultantes da função *hash*:

1. – Aquele que lhe foi gerado pelo autor do documento, e que lhe havia sido enviado por ele;

2. – O que foi obtido por ele próprio ao aplicar a chave simétrica sobre o documento em claro que recebeu.

Na posse desses dois resumos, o destinatário compara-os. Se ambos forem exatamente iguais, obtém a certeza de que o texto original do documento não foi alterado.[274]

O procedimento que acabamos de descrever conduz à conclusão de que o documento que foi assinado pelo respetivo autor ou subscritor não foi alterado desde que nele foi colocada a sua assinatura digital. É este procedimento que assegura a verificação da integridade do documento.[275]

[274] *"Verification of a digital signature is accomplished by computing a new hash resultof the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks whether the digital signature was created using the corresponding private key, and whether the newly computed hash result matches the original hash result that was transformed into the digital signature during the signing process"*. "A/CN.9/493", par. 43.

[275] Aparentemente esta operação poderia fazer-se de modo mais simples se o destinatário, ao abrir a função *hash*, obtivesse a partir dela o texto inicial, mas isso não é possível porque o algoritmo de encriptação da função *hash* é simétrico e é unidireccional, pelo que não se pode obter a partir dele, por reversão, o texto inicial. É assim por razões de segurança. Mas não sendo possível essa reversão, o procedimento que se segue é o contrário, ou seja, aplica-se de novo o algoritmo sobre o texto original e obtém-se um resumo igual ao que foi recebido, constatando-se assim a validade da assinatura. Nesse sentido Ortega Diaz: "*A função hash é unidireccional e, portanto, irreversível, não permitindo que um arquivo comprimido possa ser descomprimido*". Díaz, J.J.O. Op. Cit., pág. 51.

Capítulo II – O conceito jurídico de assinatura eletrónica

Os primeiros instrumentos normativos não definiam, nem utilizavam o conceito de assinatura eletrónica. Tanto a LMCE como a generalidade das convenções privadas adotadas pelas organizações internacionais, estabeleciam apenas mecanismos de equiparação da validade e dos efeitos das mensagens e dos documentos em suporte eletrónico aos documentos em papel.

Essa equiparação dependia da verificação de um conjunto de critérios de vinculação entre o conteúdo informacional dos suportes eletrónicos utilizados nas operações económicas e os respetivos agentes. Essas evidências de vinculação não eram designadas inicialmente de assinaturas, mas antes de métodos ou atributos das mensagens cuja existência, uma vez verificada, produzia o efeito de transpor para esses conteúdos informacionais os mesmos efeitos que a lei confere aos documentos em papel, quando assinados.

O direito da assinatura eletrónica nasceu, assim, como o direito da equivalência jurídica entre as mensagens transmitidas ou guardadas em suporte eletrónico e os documentos em papel. Compreende-se que assim fosse, em face das dificuldades em

encontrar técnicas eletrónicas que produzissem o mesmo efeito de gravação indissociável e estável que as assinaturas manuais têm nos documentos em papel.

Só mais tarde, em especial após o desenvolvimento da tecnologia das assinaturas digitais, a legislação passou a adotar um conceito próprio de assinatura eletrónica.

O direito da assinatura eletrónica nasceu sem um corpo de conceitos próprio, que lhe conferisse sistematicidade, essencialmente em razão da inexistência de conhecimento tecnológico que assegurasse a sua efetividade. Esse corpo concetual só mais tarde se viria a sedimentar.

1. O ponto de partida no paradigma do papel

O paradigma da assinatura nos documentos em papel é a assinatura escrita pela mão do seu autor no próprio documento, que designamos por assinatura manual e autógrafa.[276] É assim tanto nos países de tradição anglo-saxónica, como nos países de tradição romanista.[277] Uma assinatura num documento revela a sua origem pessoal, determinando a pessoa que é o seu autor ou que o subscreve. Foi neste contexto do papel como suporte documental único que se formou o conceito de assinatura.[278]

Sendo a assinatura o mais importante instrumento de vinculação de um sujeito a um documento, não é, porém, o único,[279] dado que se utilizam para esse fim outros instrumentos, como é o caso da colocação de carimbos, os selos, nomeadamente o chamado selo branco das entidades públicas,[280] a chancela, a utilização de papel timbrado, etc.[281]

---

[276] Como se diz num dos textos de trabalho da UNCITRAL, de 2007, *"The paradigm case of signature is the signatory's name, written in the signatory's own hand, on a paper document (a "handwritten" or "manuscript" signature)"*. A/CN.9/630; 25 April 2007, annex, par. 3.

[277] No mesmo sentido o Grupo de Trabalho da LMCE: *"As is the case under the common law, the paradigm of a signature in civil law countries is the handwritten one"*. "A/CN.9/630", annex, par. 6.

[278] Existe uma definição de assinatura manuscrita no diploma que em Portugal criou o cartão do cidadão (a Lei n.º 7/2007, de 5/2): *"Por assinatura entende-se, para efeitos da presente lei, a reprodução digitalizada do nome civil, escrito pelo respectivo titular, completa ou abreviadamente, de modo habitual e característico e com liberdade de ortografia."* (n.º 1 do artigo 12.º).

[279] Assim também se reconhecia nos trabalhos preparatórios da LMCE: *"Signatures are not the only method of identification recognized by law to attribute documents and records to a given person"*. A/CN.9/WG.IV/WP.104/Add.3, 15 September 2003, par. 14.

[280] O selo branco é um instrumento de autenticação dos documentos das administrações públicas, que tem origem no antigo selo real, que era o instrumento de certificação e autenticação dos documentos reais. Em Portugal foi criado o Imposto do Selo em 1667, que ainda hoje existe e é o mais antigo imposto do sistema fiscal português, Este imposto incidia originariamente sobre os atos documentados e autenticados com o selo real, tendo-se mantido como um imposto sobre a autenticação dos documentos, que ainda hoje

A eficácia vinculante das assinaturas não é sempre uniforme e varia em função da eficácia com que o instrumento que materializa a assinatura exterioriza a vinculação do autor ao documento. Existem formas de vinculação pessoal com eficácia probatória relativamente reduzida, como são a colocação de iniciais do nome da pessoa ou o nome completo por extenso no documento.[282]

Todos esses sinais são indicadores da origem dos documentos, entendida sempre essa origem como sendo referida a uma pessoa determinada, que fica por eles vinculada juridicamente. A eficácia jurídica do seu efeito de vinculação dependerá sempre de uma avaliação *a posteriori* das entidades competentes, nomeadamente os tribunais.

A lei portuguesa e a generalidade das legislações estrangeiras, não tipificam as formas de assinatura em termos gerais, só o fazendo em situações especiais de negócios formais que pelo seu valor ou pela sua importância, exigem requisitos formais. As garantias de origem dos documentos e o sistema de segurança na vinculação dos seus autores aos respetivos conteúdos são deixados em geral à liberdade das partes, prevalecendo, assim o primado da autonomia da vontade.[283] Só em casos excecionais de documentos formais são acrescentadas exigências adicionais mediante a associação de outros elementos probatórios de autenticidade, nomeadamente o reconhecimento da assinatura por entidades terceiras de confiança, como são os notários, bem como a participação presencial dessas entidades no ato da assinatura.

é parcialmente. Pires, J.M.F. (2016). *Lições de Impostos Sobre o Património e do Selo. 3.ª Edição*, Livraria Almedina. Coimbra, pág. 453.

[281] *"Some countries generally require that contracts for the sale of goods above a certain amount should be "signed" in order to be enforceable. However, the concept of signature adopted in that context is such that a stamp, perforation or even a typewritten signature or a printed letterhead might be regarded as sufficient to fulfil the signature requirement"*. A/CN.9/608/Add.2, par. 24.

[282] A liberdade de forma, que é comum às tradições romanista e anglo-saxónica, tanto no que respeita à necessidade, em termos gerais, de constância dos contratos em suporte escrito, como à sua assinatura, como ainda à forma que esta deve assumir, não significa, porém, indiferenciação em matéria probatória. A sua força probatória dependerá sempre do efeito vinculante da assinatura. E nessa matéria, se a jurisprudência é mais pragmática nos países anglo-saxónicos, a interpretação generalizada nos países de tradição romanista é sempre mais formalista e rigorosa nos casos em que a lei exija forma escrita ou assinatura. *"It could therefore be said that against a general background of freedom of form for the conclusion of business contracts, civil law countries tend to apply strict standards to assess the evidentiary value of private documents and may be dismissive of documents whose authenticity is not immediately recognizable on the basis of a signature"*. "A/CN.9/630", annex, par. 6.

[283] Este era o ponto de partida no que respeita à determinação do modo de as partes de se vincularem e dos instrumentos que para isso utilizavam. "*With paper-based transactions, a number of indicators can be used by a relying party to determine whether the document is authentic and the signature genuine. These include the use of paper (sometimes with water marks, coloured backgrounds, or other indicators of reliability) to which the message is affixed, the use of letterhead, handwritten signatures, or delivery in sealed envelopes via a trusted third party (such as postal services)"*. A/CN.9/WG.IV/WP.73, par. 29.

Nesses casos a eficácia vinculante da assinatura é mais elevada, sendo que a segurança das partes quanto a essa eficácia é também necessariamente mais elevada. O poder que as entidades notariais possuem, de conferir fé pública aos atos em que participam, oferece a esse tipo de assinaturas uma maior eficácia, capaz de se impor em caso de litígio. Essa eficácia garante às partes maior segurança jurídica.

Nos países de tradição jurídica anglo-saxónica, a exigência de assinatura nos negócios jurídicos dos comerciantes é muito antiga e radica no *Statute of Frauds*, uma lei publicada em Inglaterra em 1677, que tinha como objetivo diminuir o incumprimento das obrigações das partes nos contratos de comércio.[284] Essa lei seria replicada nos EUA, onde o Código Comercial Uniforme estabelecia no art.º 2-201, parágrafo 1, que a assinatura dos contratos pela parte demandada era elemento indispensável à eficácia executiva dos contratos comerciais quando o seu valor fosse superior a 500 dólares.[285]

A prática jurídica e a jurisprudência haveriam, mais tarde, de interpretar de forma aberta o conceito de assinatura contido nestas leis, admitindo que ela se expresse não apenas mediante a assinatura autógrafa manuscrita, mas também mediante iniciais do nome, pseudónimos, a simples impressão do nome, mediante cruzes e ainda carimbos.[286] [287] Resulta assim a consolidação na jurisprudência americana, de um

---

[284] Assim se reconhecia nos trabalhos preparatórios a importância deste documento. *"The Statute of Frauds was originally passed in Great Britain in 1677 "[f]or the prevention of many fraudulent practices which are commonly endeavoured to be upheld by perjury and subordination of perjury"*. "A/CN.9/630", annex, nota de rodapé 12.

[285] O artigo 2-201, subsecção 1 do Uniform Commercial Code of the United States, tem a seguinte redação: "*Except as otherwise provided in this section, a contract for the sale of goods for a price of $500 or more is not enforceable by way of action or defence unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by a party against whom enforcement is sought or by his authorized agent or broker*". "A/CN.9/630", annex, nota de rodapé 13.

[286] Nos trabalhos preparatórios da LMCE era analisada da seguinte forma essa jurisprudência: *"Variations on this theme have been considered by the English courts from time to time, ranging from simple modifications such as crosses or initials, through pseudonyms and identifying phrases, to printed names, signatures by third parties and rubber stamps. In all these cases the courts have been able to resolve the question as to whether a valid signature was made by drawing an analogy with a manuscript signature".* "A/CN.9/630", annex, par. 4. Nas notas de rodapé deste texto são citadas um conjunto de decisões dos tribunais no mesmo sentido (em especial notas de rodapé 16 a 23).

[287] Nos EUA a jurisprudência considera que tem eficácia de vinculação do seu autor, uma assinatura colocada numa mensagem eletrónica mediante a escrita do nome do seu autor. *"Thus, where the parties had regularly used e-mail in their negotiations, the courts have found that the originator's typed name in an e-mail satisfied statutory signature requirements. Aperson's "deliberate choice to type his name at the conclusion of all e-mails" has been considered to be valid authentication"*. A/CN.9/630/Add.2; 26 April 2007, par. 30. São citados neste documento vários acórdãos proferidos nos tribunais americanos, merecendo realce a decisão proferida no processo Jonathan P. Shattuck v. David K. Klotzbach, pelo Superior Court do estado do Massachusetts, 11 December, no sentido de que é válido e cumpre todos os requisitos de assinatura, o ato de uma pessoa colocar apenas o seu nome por extenso no final do texto que envia *"deliberate choice to type his name at the conclusion of all e-mails" has been considered to be valid authentication"*. "A/CN.9/630/Add.2", par. 30.

conceito abrangente de assinatura, que envolve qualquer sinal ou inscrição que seja colocado num documento, com intenção de vinculação mediante autoria ou subscrição. Trata-se de uma conceção funcional e finalista, que se centra no resultado que a assinatura revela e admite que essa revelação possa ser efetuada independentemente da forma como o instrumento que a revela assumir.[288]

Nos países de tradição romanista prevalece a regra geral da liberdade de forma no que respeita ao modo de vinculação das partes, tanto no que respeita ao suporte, escrito ou não, dos contratos, como à sua assinatura.[289] O legislador só determina em casos excecionais a forma escrita dos contratos e a necessidade da assinatura dos documentos respetivos, nomeadamente em razão do seu elevado valor[290] ou no caso de negócios pessoais, ou em negócios em que a assinatura seja essencial à sua própria configuração, como é o caso das letras de câmbio e dos endossos.

A admissibilidade em geral dos contratos sem necessidade de cumprimento de requisitos específicos de assinatura não prejudica os efeitos em termos de prova, que depende, naturalmente, da força vinculativa que cada documento possua relativamente ao seu autor, sendo que nessa matéria será muito importante a determinação da existência de assinatura e, havendo-a, o tipo de assinatura de que se trate. Em matéria de prova, os países de tradição romanista são mais formalistas do que os países anglo-saxónicos.[291]

---

[288] Admite-se assim qualquer sinal, desde que revele essa intenção de vinculação. Como se refere na decisão proferida pelo United States District Court for the Central District of Illinois, em 30/1/ 2002, no processo Central Illinois Light Company v. Consolidation Coal Company, qualquer símbolo colocado ou reconhecido por uma parte com a intenção direta de autenticar um documento cumpre os requisitos de assinatura: *"any symbol executed or adopted by a party with present intention to authenticate a writing"*. Esse sinal pode inclusivamente consistir apenas no nome datilografado por uma pessoa no final de um documento, *"a typed name or letterhead on a document is sufficient to satisfy the signature requirement"*. "A/CN.9/630/Add.2", par. 30.

[289] *"Most civil law jurisdictions follow the rule of freedom of form for contractual engagements in private law matters, either expressly24 or impliedly25 subject, however, to a more or less extensive catalogue of exceptions depending on the jurisdiction concerned. This means that, as a general rule, contracts need not be in "writing" or "signed" in order to be valid and enforceable"*. "A/CN.9/630", annex, par. 5.

[290] É o caso, por exemplo, do artigo 1341.º do Code Civil Francês, que exige a assinatura apenas nos contratos de valor mais elevado, sendo que nos de valor mais elevado se exige a intervenção de notário. A redação desse artigo é a seguinte: *"Il doit être passé acte devant notaires ou sous signatures privées de toutes choses excédant une somme ou une valeur fixée par décret, même pour dépôts volontaires, et il n'est reçu aucune preuve par témoins contre et outre le contenu aux actes, ni sur ce qui serait allégué avoir été dit avant, lors ou depuis les actes, encore qu'il s'agisse d'une somme ou valeur moindre. Le tout sans préjudice de ce qui est prescrit dans les lois relatives au commerce"*.

[291] *"In contrast to common law jurisdictions, civil law countries tend to interpret evidentiary rules rather strictly"*. "A/CN.9/630", annex, par. 5.

Também é assim no direito alemão, onde a assinatura não é indispensável à existência de um documento com relevância jurídica, em decorrência do princípio da liberdade de forma.[292]

Porém, para efeitos probatórios, o art.º 416.º do Código Civil Alemão, estabelece que os documentos privados só fazem prova em juízo quando assinados pelo autor, ou com assinatura reconhecida por notário.[293]

Em Portugal, os art.ºs 410.º e 413.º do Código Civil, exigem a assinatura das partes nos contratos-promessa quando se refiram a contratos para os quais a lei exija documento escrito, devendo a assinatura ser reconhecida presencialmente nos casos de contratos-promessa de compra e venda de bens imóveis. A exigência de reconhecimento da assinatura prevê-se também para os casos em que as partes pretendam atribuir eficácia real às promessas, como prevê o art.º 413.º.

Do mesmo modo, o art.º 875.º do Código Civil estabelece que o contrato de compra e venda deve ser titulado por escritura pública ou documento particular autenticado. Também o art.º 1143.º do Código Civil obriga a assinatura dos contratos de mútuo de valor superior a 25.000 euros. Do mesmo modo a assinatura é elemento essencial do testamento, nos termos do art.º 2206.º do Código Civil.

Em termos gerais, a assinatura é um requisito de vinculação das partes a documentos, que a lei só exige em casos especificamente previstos. Em casos pontuais a lei exige a assinatura de documentos com requisitos de forma específicos, com é o caso do reconhecimento. Estes graus de vinculação são diferenciados em função dos efeitos da assinatura, que por sua vez são determinantes do grau de eficácia vinculativa de cada um dos tipos de assinatura.

Existem também vários tipos de assinaturas e também vários graus de eficácia jurídica vinculativa de cada uma delas, desde aquelas que são efetuadas perante entidade com poderes que conferem fé pública,[294] às assinaturas em que as partes se limitam a colocar as iniciais do seu nome ou a escrevê-lo por extenso.

---

[292] Assim se reconhecia nos trabalhos preparatórios da LMCE. *"Under German law a signature is not an essential element of the notion of "document""*. "A/CN.9/630", annex, nota de rodapé 27.

[293] *"Indeed, section 416, on the evidentiary value of private documents (Privaturkunden), provides that private documents constitute "full proof" for the information they contain as long as they are signed by the author or by a notarized signature)".* "A/CN.9/630", annex, nota de rodapé 27.

[294] Em Portugal, o Código do Notariado prevê dois tipos de reconhecimento das assinaturas por notário: presencial e por semelhança. No primeiro a assinatura é efetuada na presença do notário e no segundo o reconhecimento é efetuado por mera comparação com a assinatura constante do documento de identificação (artigo 153.º do Código do Notariado).

Nas versões iniciais do projeto de LMAE, constava um conceito geral de assinatura, que era comum à assinatura manuscrita e eletrónica, e servia de base para só depois se estabelecer o conceito definidor desta última. Pretendia-se que essa definição servisse de base para o conceito de assinatura eletrónica, a partir das funções da assinatura manual.[295] Porém, ela não consta do seu texto final por se ter entendido como desnecessário num texto legislativo que tinha como objeto a assinatura eletrónica.

2. Antecedentes do conceito de assinatura eletrónica

A assinatura eletrónica não era considerada um instrumento essencial para a validade e a eficácia jurídica dos suportes eletrónicos. Só a emergência das redes abertas criaria o contexto para o nascimento do conceito.

Quando os suportes eletrónicos começaram a ser utilizados pela economia, a primeira preocupação era a de garantir a sua operacionalidade, nomeadamente a sua legibilidade, compreensão e conservação. A primeira referência à utilização dos documentos eletrónicos foi efetuada na Convenção para Facilitação do Tráfego Marítimo Internacional, de 1977, e exigia apenas a sua legibilidade e inteligibilidade.[296]

As Hamburg Rules, de 1978, são o primeiro instrumento convencional que prevê a assinatura por meios eletrónicos, mas sem estabelecer requisitos de validade.[297]

Mas a instituição de um conceito jurídico de assinatura eletrónica não era considerada necessária neste contexto, onde se pretendia apenas uma equiparação jurídica dos suportes eletrónicos ao papel. É ainda nessa linha que se integra a LMCE.

---

[295] Na primeira versão do projeto, de 1997, a norma que definia o conceito de assinatura era logo a alínea a) do artigo 1.º, que tinha a seguinte redação: *“"Signature" means any symbol used, or any security procedure adopted by [or on behalf ot] a person with the intent to identify that person and to indicate that person's approval of the information to which the signature is appended”*. A/CN.9/WG.IV/WP.73, par. 15. A justificação para a inclusão dessa definição no projeto era reconhecida nas notas explicativas pela necessidade de ela servir de base para as definições de assinatura eletrónica que se lhe seguiam: *“That definition is intended mostly to serve as a basis for the subsequent defInitions of "electronic signature" and "secure electronic signature"”*. *Idem*, par. 17.

[296] A Convenção para a Unificação de Certas Regras Relativas ao Transporte Aéreo Internacional, introduzida pelo Protocolo de Montreal, de 25/9/1975 exigia apenas a conservação: *“Any other means which preserves a record of the carriage to be performed may be substituted for the delivery of an air waybill”*, disponível em http://nasamer.ku.edu.tr/sites/nasamer.ku.edu.tr/files/mevzuat/conventions/montreal-convention.pdf (consulta efetuada em 26/5/2015).

[297] “*The signature on the bill of lading may be handwriting, printed in facsimile, perforated, stamped, in symbols, or made by any other mechanical or electronic means*…”. A/CN.9/221, pág. 20.

2.1. A emergência do EDI e o conceito de assinatura na LMCE

A LMCE não contém uma definição do conceito de assinatura eletrónica, e não podemos dizer que seja um instrumento normativo sobre assinatura eletrónica. Trata-se, antes, de um conjunto de normas sobre documentos eletrónicos.

A LMCE estabelece, pela primeira vez, uma definição de mensagem eletrónica, efetua uma inventariação das funções que desempenham as assinaturas em papel e, de seguida, tipifica quais são os requisitos que considera essenciais para que os documentos eletrónicos cumpram essas funções, de forma equivalente aos documentos em papel. São os pressupostos essenciais da equivalência funcional entre os documentos eletrónicos e os documentos em papel, que a LMCE estabelece, mais do que a definição de um conceito de assinatura eletrónica.

Na construção do regime jurídico dos documentos eletrónicos (mensagens eletrónicas na sua terminologia, dada a sua natureza de instrumento normativo que responde às necessidades do EDI), são criados três grandes regimes:

i) O princípio geral da não discriminação dos suportes eletrónicos. Mediante uma norma geral de equivalência, a LMCE consagra o princípio geral de que não pode ser negada validade nem eficácia legal a uma mensagem só pelo facto de ela se apresentar em suporte eletrónico.[298] Acrescenta o art.º 6.º que para que se considerem cumpridos os requisitos de documento escrito, basta que a informação seja apresentada de forma que possa ser acedida para utilizações futuras.[299] A equivalência funcional entre as mensagens eletrónicas e os documentos em papel constitui-se sem necessidade da sua assinatura;

ii) Para os casos em que a lei exija expressamente assinatura dos documentos, a LMCE constrói um outro método jurídico de equivalência funcional. Podia ter-se construído um conceito de assinatura aplicável aos documentos eletrónicos, mas não foi isso que aconteceu. Enunciou-se, antes, um conjunto de pressupostos de

[298] O artigo 5.º da LMCE, sob o título *"Legal recognition of data messages"*, tem a seguinte redação: *"Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message"*. "Guide to Enactment LMCE (1996)", par. 5.

[299] O artigo 6.º da LMCE, tem a epígrafe "*Writing*" e o seu n.º 1 tem a seguinte redação: *"Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference"*. "Guide to Enactment LMCE (1996)", par. 5.

equivalência a documento assinado. O art.º 7.º da LMCE estabelece que o requisito essencial de equivalência das mensagens eletrónicas aos documentos assinados exigidos por lei é a existência de um método, sendo que esse método deve cumprir três requisitos fundamentais: [300]

1. Identificar uma pessoa;
2. Revelar a aprovação, por essa pessoa, do conteúdo de um documento.[301]
3. Tratar-se de um método fiável, sendo que a fiabilidade deve ser sempre avaliada em face das circunstâncias da sua utilização e à luz da finalidade da mensagem.[302]

iii) A prevalência da autonomia da vontade, considerando-se que nos casos em que exista convenção prévia de identificação e de autenticação entre as partes que trocam mensagens em suporte eletrónico, prevalece o regime de autenticação que as partes convencionaram livremente, considerando-se cumprido o requisito da fiabilidade do método de autenticação.

Estes três instrumentos de equivalência das mensagens eletrónicas aos documentos em papel constituem os prolegómenos fundamentais do direito da segurança jurídica dos suportes eletrónicos.

2.2. As limitações do regime da LMCE

Do que se tratava na LMCE e nas convenções que a antecederam, não era ainda da construção de um regime de segurança jurídica dos suportes eletrónicos nem

[300] A previsão de assinatura dos documentos eletrónicos consta dos n.ºs 1 e 2 do artigo 7.º da LMCE, que têm a seguinte redação: *"Article 7. Signature (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement"*. "Guide to Enactment LMCE (1996)", pág. 6.

[301] *"Article 7 ... should be considered as setting out a manner in which a reliable method could be used "to identify a person" and "to indicate that person's approval" of the information contained in a data message"*. A/CN.9/WG.IV/WP.73, par. 6.

[302] *"The following functions of a signature were considered: to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document."*. "Guide to Enactment LMCE (1996)", par. 53.

de segurança eletrónica, mas antes da eliminação dos entraves legais que pudessem existir à utilização daqueles suportes. Esta eliminação assenta no conceito de fiabilidade do método que conduzirá à identificação do autor da mensagem e da aprovação do seu conteúdo.

No contexto da sua elaboração esse interesse prevalecia sobre a necessidade de segurança jurídica, que ainda não era sensível em toda a sua extensão atual. Por essa razão a LMCE revela um conjunto de limitações, de que destacamos as seguintes:

i) Não tipifica qualquer mecanismo de avaliação do requisito da fiabilidade, e a sua definição centra-se apenas no resultado pretendido, pelo que é aceite qualquer instrumento que a proporcione;[303]

ii) Este carácter vago e finalista transporta para a atividade probatória das partes, em caso de litígio, a determinação da eficácia desse método em relação à finalidade assinalada, ficando as partes dependentes da decisão do tribunal, sem outra segurança;

iii) Não são enunciados quaisquer métodos que garantam essa fiabilidade, e aparentemente também não eram conhecidos do legislador da LMCE;[304]

iv) Do conjunto dos requisitos funcionais de equivalência, não integra a LMCE o requisito da certeza da participação pessoal do autor no ato de assinar. Explica esse facto a ausência de mecanismos tecnológicos disponíveis de garantia.

Apesar das limitações antes enunciadas, a formulação dos pressupostos de autenticação da LMCE tem o mérito de, sendo abrangente e vaga, servir de instrumento para que viessem a ser acolhidas na sua previsão as inovações tecnológicas que já então se pressentiam.[305]

---

[303] Nos trabalhos da LMCE enunciam-se as circunstâncias relevantes para se avaliar essa fiabilidade. O problema é que esses fatores são também eles genéricos, podendo conduzir a que normalmente se considerem cumpridos. São enunciados 14 fatores, dos quais selecionamos os primeiros sete:*" (1) the sophistication of the equipment used by each of the parties; (2) the nature of their trade activity; (3) the frequency at which commercial transactions take place between the parties; (4) the kind and size of the transaction; (5) the function of signature requirements in a given statutory and regulatory environment; (6) the capability of communication systems; (7) compliance with authentication procedures set forth by intermediaries*. "Guide to Enactment LMCE (1996)", par. 58.

[304] Ressalva-se, o caso de existir um convénio prévio de autenticação entre as partes. Nesse caso, como vimos, é à luz dele que deve ser avaliada a sua fiabilidade, devendo assim considerar-se como cumprida a autenticação e, como tal assinado o documento, se o método utilizado for o que resulta do convénio.

[305] O carácter genérico da formulação da LMCE é assumido, quando se refere que se trata de estabelecer apenas um critério básico de autenticação. *"Thus, article 7 may be regarded as establishing a basic standard of authentication for data messages"*. "Guide to Enactment LMCE (1996)", par. 59.

Estabeleceu-se, porém, um conjunto de pressupostos que, na prática, são uma aproximação às necessidades fundamentais que devem ser satisfeitas para que um documento eletrónico se tenha como assinado. Essas funções da revelação da identidade e da aprovação do conteúdo do documento, bem como da fiabilidade, serão muito importantes para que, mais tarde, se viesse a formar um conceito próprio de assinatura eletrónica, como veremos já de seguida.

3. O conceito de assinatura no contexto das redes abertas

O conceito de assinatura só nasce verdadeiramente depois da emergência das redes abertas. As transações eletrónicas eram, até aí, estabelecidas em contextos eletrónicos fechados, como era o caso do EDI, criados especificamente entre partes que já anteriormente se conheciam e onde o risco era reduzido e a necessidade de segurança jurídica era também limitada em conformidade. Nesse ambiente controlado não era necessário o instrumento de assinatura, porque as partes convencionava entre si a forma de autenticação das suas mensagens.

As redes abertas alteraram este paradigma e tornaram insuficiente o regime da LMCE, nomeadamente pelos seguintes motivos:

i) As redes abertas mudaram o conceito de mercado, que deixou de corresponder a um espaço físico, localizado geograficamente e aberto em períodos temporais limitados e onde os agentes económicos se conhecem.

ii) Os mercados eletrónicos abertos perderam o conceito de espaço, de tempo e de conhecimento dos agentes;

iii) Mais do que os documentos, é necessário nas redes abertas identificar as pessoas com segurança;

iv) As transações eletrónicas ocorrem de forma instantânea, pelo que os instrumentos de autenticação devem ser também eles instantâneos e não dependentes de convenções prévias de autenticação;

v) As redes abertas exigiam que a ordem jurídica fosse dotada de instrumentos novos e mais eficazes, de segurança jurídica.

vi) A segurança jurídica na rede exige um nível de segurança nos instrumentos de vinculação que seja apreciada imediatamente, não

sendo suficiente a previsão de normal gerais a serem integradas em caso de litígio, em conformidade com as circunstâncias do caso;

vii) E esse nível de segurança e certeza jurídica dependia da definição clara de um conceito de assinatura eletrónica e da delimitação das circunstâncias em que se consideram reunidos os pressupostos para que esses documentos se considerem assinados por meios eletrónicos.

A expansão da utilização das redes abertas na atividade económica e nos procedimentos administrativos provocou uma rotação do centro de gravidade do direito dos suportes eletrónicos, da necessidade de remoção de entraves jurídicos mediante a equivalência funcional, para um nível mais exigente de segurança jurídica na sua utilização, no que respeita à identificação e à vinculação.

O novo contexto tecnológico exigia o máximo nível de segurança, mas ao mesmo tempo rapidez e simplicidade.[306] É a essas necessidades que o regime jurídico da assinatura eletrónica tenta dar resposta.

3.1. A formação do conceito de assinatura eletrónica na LMAE e na Diretiva da UE

Funda-se na LMAE o conceito jurídico de assinatura eletrónica, que estabelece também a definição das suas funções fundamentais, os seus sujeitos de direito, e o seu regime.[307]

O conceito de assinatura eletrónica que consta da alínea a) do art.º 2.º da LMAE é o seguinte: *""Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message"*.[308]

---

[306] *"The interest for promoting security in the exchange of electronic communications needs therefore to be balanced against the risk of providing an easy way for traders in bad faith to repudiate their freely assumed legal obligations. Achieving this balance through rules and standards that are internationally recognized and operable across national borders is a major task of policymaking in the area of electronic commerce"*. "A/CN.9/630/Add.1", par. 14.

[307] Os trabalhos de conceção da LMAE iniciaram-se em 1996 e logo em dezembro de 1997 foi apresentada a primeira versão, sendo que a versão final, após discussão prolongada é de janeiro de 2001 A/CN.9/WG.IV/WP.73.

[308] "A/CN.9/493". Fazendo uma tradução livre da nossa responsabilidade, e definição seria a seguinte em português: *""Assinatura eletrónica" significa dados em forma eletrónica contidos numa mensagem de dados, anexos ou logicamente associados a ela, que podem ser usados para identificar o autor da*

A definição assume a assinatura eletrónica com a natureza de um conjunto de dados, ou seja, uma assinatura já não é um símbolo nem um elemento escrito, mas dados, apenas dados, em suporte eletrónico, compostos por *bites*, que para serem classificados como assinatura têm que cumprir os seguintes requisitos:

1. – Requisitos relacionados com o documento eletrónico:
    a. Estão consignados no próprio documento ou;
    b. Estão anexados ao documento ou;
    c. Estão logicamente associados ao documento;
2. – Requisitos relacionados com o titular da assinatura – Identificam o titular que assinou o documento;
3. – Requisitos de conexão entre o titular da assinatura e o documento eletrónico:
    a. Revelam que o assinante assinou pessoalmente o documento;
    b. Vinculam o titular ao documento e;
    c. Indicam que o titular aprova o conteúdo do documento.

A função da assinatura eletrónica é a de proporcionar os seguintes resultados no domínio da confiança jurídica:[309]

1. – Identificar o assinante;
2. – Conferir certeza acerca da sua participação no ato da assinatura;
3. - Vincular o assinante com o conteúdo do documento.

O regime da LMAE assenta na criação de um corpo de conceitos jurídicos que conferem autonomia à assinatura eletrónica e permitem estabelecer o seu regime para além da mera equivalência funcional com o papel. Trata-se de uma mudança de paradigma relativamente à LMCE e ao direito convencional anterior.

A assinatura é um instrumento de vinculação de sujeitos de direito a dados. E esses dados são de três tipos, os dados da própria assinatura, os dados do documento e os dados da identificação do titular. A assinatura consiste numa estrutura jurídica que se funda numa estrutura logica que conexiona todos esses conjuntos de dados entre si e garante a sua estabilidade e vinculação. Esta mudança só se tornou possível pela

---

assinatura relativamente à mensagem de dados e indicar que o assinante aprova a informação contida na mensagem de dados".

[309] Estas três funções foram estabilizadas ao longo dos trabalhos da UNCITRAL e enunciados nos seguintes termos no Guia para a Transposição: *"The Working Group discussed the following functions traditionally performed by hand-written signatures: to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document"*. "A/CN.9/WG.IV/WP.88", par. 29.

emergência do conhecimento contido na assinatura digital e em especial pela sua sistematização jurídica nas Guidelines da ABA. A apresentação, logo em 1997, do projeto da LMAE, teria um elevado impacto na produção legislativa que se lhe seguiu.[310]

A definição da LMAE releva, pela primeira vez, que, a par da importância da vinculação dos sujeitos de direito aos documentos por eles assinados, uma outra função da assinatura consiste na estabilidade e na segurança da conexão da própria assinatura ao documento assinado. A LMAE, em linha com as Guidelines da ABA, operam uma verdadeira rotação no conceito da assinatura eletrónica, passando a centrá-la na conexão dos dados do documento de base assinado com os dados da assinatura, assegurando-se a vinculação subjetiva do signatário como uma consequência dessa associação de dados.

Este conceito de assinatura eletrónica, estruturado, nos dados da assinatura, do signatário e do documento, bem como a função da conexão entre eles, haveria de ser estruturante na sua sedimentação jurídica futura.

A Diretiva de 1999 da UE é já tributária desta mudança, fazendo assentar em nos três tipos de dados envolvidos e na sua conexão, bem como na qualificação jurídica que da sua operacionalidade resulta, que é a autenticação, a definição do conceito da assinatura. A Diretiva define a assinatura eletrónica como *"os dados sob forma eletrónica, ligados ou logicamente associados a outros dados eletrónicos, e que sejam utilizados como método de autenticação"*.[311]

Uma das diferenças mais importantes entre ambas as definições é que a diretiva europeia exclui da definição as funções de aprovação do conteúdo das mensagens, provavelmente pelas razões que mais adiante analisaremos.

Do mesmo modo se excluem do conceito os requisitos de vinculação e de participação do autor ou subscritor no ato de assinatura. A definição da diretiva utiliza apenas o conceito de autenticação, mas ele integra na sua essência o de identificação, dado que a autenticação é uma função de identificação da origem da informação, e essa

[310] Os dados e a sua conexão fixa são a base objetiva e factual da assinatura, a partir dos quais se formam os efeitos jurídicos que também integram o conceito da assinatura eletrónica. E esses efeitos eram assim enunciados nos trabalhos da UNCITRAL: *"Depending on the nature of the document that was signed. For example, a signature might attest to: the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text (thus displaying awareness of the fact that legal consequences might possibly flow from the act of signing); the intent of a person to associate itself with the content of a document written by someone else; the fact that, and the time when, a person had been at a given place"*. "A/CN.9/WG.IV/WP.88", par. 29.

[311] Transcrevemos o n.º 1 do artigo 2.º da Diretiva 1999/93/CE, de 13/12/1999.

é uma origem pessoal, de uma pessoa determinada, que tem que ser identificada. Não existe autenticação sem identificação do sujeito dessa autenticação.

No que respeita à função de demonstração da participação do autor no ato de assinatura ela é exterior ao ato de assinar e constitui uma consequência jurídicas do ato de assinatura, que está para além desse ato, sendo antes um efeito dele.

3.2. O conceito de assinatura eletrónica no Regulamento EIDAS

A definição do Regulamento (UE) N.º 910/2014 continua a assentar na conexão de dados, estabilizando, nesta parte, o conceito da Diretiva, e assumindo essa base objetiva como o elemento central do conceito.[312]

O Regulamento EIDAS altera, porém, substancialmente, o efeito desta conexão de dados, contido na definição do conceito de assinatura. O Regulamento elimina do conceito a autenticação, substituindo-o pelo conceito de assinatura. A função da assinatura não é já a da "*autenticação*", mas apenas a de "*assinar*".

Esta mudança deve-se a duas alterações fundamentais no conhecimento jurídico acerca do direito da confiança eletrónica:

i) Por um lado a limitação do conceito de documento eletrónico, pelo abandono da ideia de que todas as trocas de dados eletrónicos consubstanciariam documentos eletrónicos, passando estes a ser considerados apenas os conteúdos armazenados em suportes eletrónicos;

ii) Por outro lado a autonomização do conceito de identificação eletrónica, separando-o do de assinatura eletrónica.

Em consequência desta dupla separação, a necessidade de se utilizar o conceito de autenticação para a verificação e a confirmação dos dados, tanto de assinatura eletrónica como de identificação eletrónica, conduziu à necessidade de se retirar do conceito de assinatura o conceito de autenticação, porque ele não é específico dela, mas comum a este conceito e ao de identificação.

Por outro lado, sendo a assinatura eletrónica apenas um conceito jurídico aplicável aos documentos eletrónicos, tal como acontece nos documentos não

[312] A definição do conceito de assinatura eletrónica do Regulamento EIDAS é a seguinte: "*Os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar*". (n.º 10 do artigo 3.º)

eletrónicos, o ato de assinar é, em si mesmo, um ato destinado ao conferir segurança jurídica acerca da vinculação de um sujeito de direitos e obrigações a um determinado documento eletrónico. A assinatura é, assim, o resultado da conexão entre os três tipos de dados que anteriormente enunciámos.

A autenticação da identidade do signatário, dos elementos da assinatura e dos dados dos documentos é também uma das funções da assinatura, mas sendo a autenticação uma função essencial da assinatura, não é específico dela.

Analisamos, de seguida, a estrutura do conceito de assinatura eletrónica.

3.3. A assinatura eletrónica como um conjunto de dados

Os sistemas informáticos operam com dígitos e a sua combinação. São eles o elemento radical de todos os sistemas informáticos. A informação, o conhecimento e os documentos eletrónicos são dados. E se assim é, a certeza acerca da estabilidade dos documentos não se pode limitar à forma como as plataformas informáticas os apresentam para leitura ou visualização humana. A segurança tem que se fundar nos próprios dados, nas sequências específicas e irrepetíveis em que se estrutura cada documento e na forma como estão combinados.

Por essa razão a definição de assinatura assenta nos dados de suporte do documento. E a assinatura sendo uma evidência, uma representação que confirma o acontecimento da autoria e da participação de uma pessoa num documento, ela própria consiste em dados. Por essa razão a assinatura eletrónica é estruturalmente diferente da assinatura manual, dado que esta é uma manifestação pessoal, inata, física e intrinsecamente pessoal, enquanto aquela é um procedimento mecânico.

É por essa razão que a Lei alemã de 1997, que regulou a assinatura digital, a define como "*um carimbo aposto em dados digitais*",[313] um carimbo eletrónico, que, como vimos, resulta da aplicação de uma chave privada sobre uma sequência de carateres. Do mesmo modo, a primeira lei de assinatura digital, publicada em 1995 no Estado do Utah, nos EUA, define assinatura digital como "*uma sequência de bites que uma pessoa que pretende assinar cria em relação a uma mensagem claramente*

[313] Lei da Assinatura Digital de aprovada pela Lei Federal de 1/8/1997 (Signaturgesetz Sigg), que define a assinatura digital no n.º 1 do § 2.º do artigo 3.º

determinada".[314] Também a lei portuguesa tem uma definição técnica de assinatura digital, considerando-a como "*o resultado de um processamento eletrónico de dados*".[315] E as legislações atualmente vigentes se referem à assinatura como "dados", como analisámos no capítulo referente ao conceito de assinatura.

Designar este conjunto de procedimentos técnicos em que consiste materialmente a assinatura eletrónica, associando-o ao conceito de assinatura, só se compreende pela necessidade de lhe conferir o mesmo valor jurídico que a lei atribui à assinatura manuscrita e a mesma confiança que a cultura e o tráfego jurídicos reconhecem à assinatura manuscrita. Trata-se, portanto, de uma convenção de carácter jurídico, que se traduz numa manifestação da utilização do princípio da equivalência funcional.

3.3.1. A natureza dos dados da assinatura eletrónica

Como os suportes eletrónicos são sempre, na sua essência dados, a assinatura eletrónica também é composta de dados. Mas os dados da assinatura são diferentes dos dados do documento que autentica. Temos, então, uma dualidade de dados, e uma conexão entre esses dois universos. E esta conexão opera sobre aquela dualidade, como uma entidade essencial. A assinatura eletrónica assenta em dois elementos fundamentais:

iii) Um dualismo de dados, que são:
    1. Os dados que autenticam;
    2. Os dados que são autenticados.

iv) Uma ligação ou uma associação lógica entre ambos os universos de dados antes referidos.

Tal como as assinaturas manuscritas, que utilizam os mesmos materiais elementares dos documentos em papel, que são o próprio papel e a tinta, também as assinaturas eletrónicas utilizam os dados dos documentos que se destinam a autenticar.

[314] Utah Digital Signature Act, 46-3-103, (10). Em 2006 o Estado do Utah publicou uma nova lei das assinaturas eletrónicas, integrada no Title 46 do Utah Code, sob o título "Notarization and Authentication of Documents and Electronic Signatures". Disponível no endereço http://le.utah.gov/xcode/Title46/Chapter4/46-4-S201.html, (última consulta efetuada em 30/10/2015).
[315] Alínea b) do artigo 2.º do DL n.º 290-D/99, de 3/8.

Uma assinatura eletrónica não é só essa representação de dados, tal como uma assinatura em papel não é apenas o desenho estilizado do nome do seu autor. Associados a esses referenciais, existe todo um conjunto de outros elementos que lhe conferem sentido.

O núcleo essencial da assinatura eletrónica não representa nada por si só, se não estiver associado a uma pessoa em concreto, e é por isso que se poderia entender que a assinatura não é, na verdade, apenas esse conjunto de dados. Vista isoladamente, uma agregação de dados não tem significado em si mesma. Eles só são uma assinatura se estiverem associados a um documento, como a própria norma estabelece, bem como a uma pessoa devidamente identificada. Aqueles dados são o elemento comum ao documento e à pessoa que o assinou, são eles que estabelecem um vínculo entre ambos. Para serem uma assinatura, esses dados necessitam de um sistema de identificação da pessoa que é o titular de assinatura, e esse sistema é externo a esses dados e à assinatura. Necessitam também de um documento a que se reportem, que é o objeto de base da assinatura. Necessitam, finalmente, de uma conexão que os ligue ao documento. Analisamos, de seguida, como se organiza essa dualidade de dados.

3.3.2. A natureza da associação dos dados

Todas as definições de assinatura eletrónica contidas nas normas que vimos analisando abrangem dois tipos diferentes de associação dos dados de assinatura aos dados do documento assinado, que são:

i) Uma ligação entre esses dados ou;

ii) Uma associação lógica entre esses dados.

Esta diferenciação é essencial para a abrangência do conceito e do regime jurídico, nomeadamente no que respeita aos níveis diversos dessa conexão.

3.3.2.1. A mera ligação de dados

Na formulação do primeiro tipo, a menção a uma mera ligação (a formulação da LMAE refere-se a dados anexos), é pouco exigente, e basta-se com qualquer tipo de ligação.

São dados as letras com que uma pessoa escreve o seu nome no final de um texto que envia por correio eletrónico. A constância desses dados na mensagem representa uma associação entre o nome e o documento, e o facto de se tratar do nome da pessoa que é o seu autor, representa uma assinatura. É certo que se trata de uma vinculação fraca entre o nome da pessoa e o texto, cuja associação pode ser desfeita de forma simples, mediante as teclas de um computador. Trata-se, também de uma associação pouco segura entre os dados que compõem o nome e a pessoa que os digita no computador, que pode ser também facilmente desfeita, uma vez que qualquer pessoa pode escrever o nome de outra. Apesar disso trata-se de um conjunto de dados que associam uma pessoa a um documento e isso integra-os no conceito de assinatura eletrónica antes referido.

Do mesmo modo a designada assinatura digitalizada é composta por uma sequências de dados que, uma vez colocados sobre um documento em suporte eletrónico, ficam a ele anexados, apesar da sua escassa segurança que resulta do facto de essa anexação poder ser eliminada ou substituída por outra.

Apesar da sua escassa segurança, a assinatura mediante a colocação do nome no final de um texto em suporte eletrónico ou a chamada assinatura digitalizada, são assinaturas eletrónicas, que pelo mero facto de se apresentarem nesse suporte, não podem ser discriminadas nos seus efeitos jurídicos.

As definições do conceito de assinatura eletrónica, em especial a do Regulamento EIDAS, são suficientemente abrangentes para incluir também estes tipos de assinatura. E embora o seu poder de vinculação seja fraco, isso não afasta estes tipos de assinatura do conceito. Na verdade, uma coisa é a definição do conceito e a natureza do referencial a que se aplica, e coisa diferente são os diversos graus de eficácia que as várias espécies que se integram nesse conceito são suscetíveis de proporcionar. Uma coisa é a substância e outra o modo, ou seja, neste caso o grau de segurança jurídica que cada tipo de assinatura eletrónica oferece às partes.

Esta formulação abrangente é também a que melhor se harmoniza com o princípio da neutralidade tecnológica, deixando às partes a opção por tipos de assinatura mais ou menos seguros, em função da avaliação do risco e da necessidade de segurança jurídica, em face das circunstâncias.

3.3.2.2. A assinatura por associação lógica entre dados

Diferente da ligação entre dados é a associação lógica entre esses dados. O carácter lógico dessa associação só é possível mediante um procedimento sistemático, de natureza matemática.

É esse carácter lógico que garante a sua segurança e a unicidade e irrepetibilidade dessa conexão. A conexão lógica é fixa e determinada, podendo ser cristalizada, objetivada e constatável, por terceiros. Sendo uma conexão matemática é demonstrável e insuscetível de disputa, porque positivada e avaliável mediante demonstração científica. Pelo contrário, a conexão por associação não depende de qualquer método e normalmente é meramente visual ou circunstancial, sem uma estrutura interna que lhe confira autonomia e objetividade. Esta conexão é, portanto, mais segura e estável, e é nela que se integra o modo como operam as chaves assimétricas sobre os dados dos documentos autenticados.

Esta associação é tanto o produto da aplicação de uma chave simétrica sobre um documento, que gera uma sequência mais curta (*hash*), como a aplicação da chave privada sobre aquele *hash*, que forma a assinatura.[316]

Nos casos em que são utilizados método biométricos de autenticação e de vinculação de uma pessoa, os sistemas informáticos que são utilizados para assinar documentos e para verificar a assinatura operam da mesma forma, com os dados resultantes da digitalização dos elementos biométricos de cada pessoa. No caso da assinatura digital, a assinatura tem como núcleo essencial a aplicação da chave privada sobre o *hash*, porque é nessa operação que se concentra o ato de subjetivização do documento com os elementos pessoais do seu autor.

A opção por esta terminologia limitativa de chamar assinatura apenas aos dados do *hash* encriptado, foi debatida nos trabalhos preparatórios da LMAE, sendo que nas versões iniciais se utilizava o conceito alternativo de "assinatura", com a formulação de a "assinatura eletrónica" ser definida como a *"assinatura em forma eletrónica contida numa mensagem de dados, anexa ou logicamente associada a ela, e utilizada por uma pessoa com a intenção de a identificar e de indicar a sua aprovação do conteúdo dessa mensagem de dados do conteúdo dessa mensagem de dados, e*

[316] A aplicação da chave privada, que corresponde ao ato pessoal de vinculação ao documento, e que constitui verdadeiramente o ato da assinatura eletrónica, não se aplica a todo o documento que é enviado, mas apenas ao *hash*, sendo que este é uma sequência binária de síntese da sequência binária do documento que se pretende autenticar. Como se especifica nos documentos preparatórios da LMAE, *"It was explained that it was not the message as a whole, but only its numerical representation that changed as a result of processing the message through the use of an algorithm."* "A/CN.9/446", par. 67.

utilizada para satisfazer as condições do art.º 7.º da Lei Modelo da UNCITRAL Sobre Comércio Eletrónico".[317] Na redação final, a definição de assinatura passou a ser a de *"dados em forma eletrónica contidos numa mensagem de dados, anexos ou logicamente associados a ela, que podem ser usados para identificar o autor da assinatura relativamente à mensagem de dados e indicar que o assinante aprova a informação contida na mensagem de dados"* (tradução nossa).

A alteração da formulação do preceito deveu-se à necessidade de evitar que a definição do conceito ficasse associada a uma tecnologia em concreto de assinatura, neste caso da assinatura digital.[318] Por essa razão, o conceito de assinatura eletrónica passou a ser reportado não a uma assinatura, mas aos "dados". A adoção deste conceito tem origem na definição que havia sido aprovada pela *International Standards Organization (ISO)* em 1998.[319]

Esses dados que são o referencial da assinatura, são apenas os dados a que foi aplicada a chave privada, pelo que a definição se centra no núcleo essencial do ato de assinar, que consiste apenas no comportamento do autor da assinatura que ordena ao sistema informático que aplique os dados da sua chave privada, que só ele possui, e que só ele pode ordenar, ao conjunto de dados que constitui o *hash*.[320]

---

317 *""Electronic signature" means [a signature] [data] in electronic form in, or attached to, or logically associated with a data message [and used by [or on behalf of] a person with the intent to identify that person and to indicate that person's approval of the contents of the data message]"*. A/CN.9/WG.IV/WP.73, pág. 6.

318 Como refere o documento respetivo,*"As a matter of drafting, it was generally agreed that the word "data" should be used instead of the words "a signature""*. "A/CN.9/446", par. 30. Essa alteração pretende garantir a neutralidade tecnológica, mesmo relativamente a tecnologias de assinatura que venham e emergir no futuro. Prendem-se também com a necessidade de evitar confusão entre a assinatura manual e a assinatura eletrónica, dado que esta é apenas uma técnica de autenticação e não uma assinatura com o conceito da assinatura manual. *"The concepts of both electronic signature and enhanced electronic signature should not be used in the Uniform Rules since they were not in fact "signatures", but rather techniques that enabled the identification of the sender of a data message and identification of the message that was sent. Accordingly, there was no rationale for using the term "signature" to describe such techniques, and in fact to do so could create confusion as the term "signature" carried with it meanings closely associated with its use in the paper environment and with the legal effects of its use in that environment"*. A/CN.9/457, par. 48.

319 Essa origem é reconhecida do seguinte modo:*"During the discussion, the suggestion was made that the Working Group should consider, merely for purposes of comparison, the text adopted in 1988 by the International Standards Organization (ISO), which read as follows: "Digital signature: data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient" (ISO 7498-2)"*. "A/CN.9/446", par. 69.

320 O grupo de trabalho da UNCITRAL chegou a ponderar definir a assinatura eletrónica como um "método" de autenticação, mas a ideia foi abandonada, porque o que se pretendia era uma definição centrada no resultado final da vinculação e não no procedimento de formação da assinatura. O conceito de método reporta para o modo como opera o mecanismo de autenticação, quando o que se pretende definir é a própria autenticação em si mesma, como um produto e não como um procedimento. *"Having reviewed that wording, the Working Group was of the view that defining the electronic signature as a*

São esses os dados que uma vez submetidos ao elemento de pessoalização que é a chave privada, garantem um produto específico, único e irrepetível, que resulta de uma operação matemática. O ato de assinar cumpre-se exclusivamente com a ordem dada ao sistema informático para aplicar a chave privada ao *hash*.[321] Os dados da chave privada são secretos, e por isso pessoais do titular da assinatura, e é o conhecimento desse segredo aplicado, que revela a autoria ou a subscrição de um documento. É esse conhecimento exclusivo e pessoal que confere a segurança de que só o seu titular os podia ter utilizado.[322]

Quando se trate da autenticação por meios biométricos, falaremos também de dados, mas não de chave privada. Neste método de autenticação, os dados utilizados os traços fisionómicos que são pessoais e também irrepetíveis, mas trata-se, também aqui de dados, dado que esses traços físicos ou fisionómicos são guardados nos computadores em forma de dados para serem confrontados com os traços fisionómicos quando o seu titular se pretende identificar.[323] E a sua aplicação a um documento forma também uma conexão lógica entre os dados de identificação pessoal e os dados do documento assinado.

As formas de assinatura eletrónica que asseguram a associação lógica de dados resultam de uma operação material, matemática e informática, que produz dados novos a partir de outros dados, e que constitui, em si mesma, uma demonstração de que só uma determinada pessoa, que possui um dos fatores dessa composição (a chave privada) o poderia ter gerado. Por ser essa pessoa o detentor único desse elemento constituinte do produto gerado pela encriptação, que é a chave pública, este procedimento revela a pessoa que está na sua origem, o seu autor ou criador.[324]

"method" was inappropriate, since it created confusion between the process of creating an electronic signature and the result of that process". A/CN.9/483, par. 61.

[321] Trata-se de uma definição nuclear, que pressupõe os restantes elementos contextuais. *"It was widely felt that, in any event, the definition should cover only those core elements that should be kept confidential to ensure the quality of the signature process, to the exclusion of any other element which, although it might contribute to the signature process, could be disclosed without jeopardizing the reliability of the resulting electronic signature"*. "A/CN.9/483", par. 71.

[322] Como se refere de forma exemplar no Guia de Incorporação, *"Only the private key needs to be covered by the definition, since only the private key should be kept confidential and it is of the essence of the public key to be made available to the public"*. "A/CN.9/WG.IV/WP.88", par. 96.

[323] *"The signature creation data was precisely the factor used to establish the link between the electronic signature and the person of the signatory"*. "A/CN.9/483", par. 71.

[324] Relevamos que a chave privada não é diretamente aplicado sobre o documento original a assinar, mas sobre um resumo deste.

3.3.2.3. A associação aos elementos da identificação

A assinatura eletrónica também pressupõe a referência a um sistema externo que associe de forma segura e credível a pessoa às suas chaves privada e pública. E essa conexão pressupõe a referência a um sistema de identificação pessoal que contenha todos os elementos de identificação civil da pessoa e que sirva de base para que se estabeleça a associação dessa pessoa à sua chave privada.

Esta associação é idêntica à que ocorre na assinatura manual, em que a vinculação do autor pressupõe a sua identificação e esta se efetua por referência ao sistema de identificação legal. Só que esse procedimento só se efetua de forma completa quando se estabelecem relações pela primeira vez, passando a partir daí essa referenciação a ser intuitiva e simples, porque as pessoas se conhecem. Nas relações eletrónicas, em especial nas redes abertas, essa proximidade existencial não existe e a segurança jurídica exige que o procedimento se efetue de forma sistemática. Essa conexão é assegurada pelos prestadores de serviços de confiança.

3.3.2.4. A abrangência da definição

Foi neste conceito de associação ou ligação entre dados que constituem documentos e outros dados que se relacionam com uma pessoa, que se centraram as definições de assinatura eletrónica da Diretiva 1999/93/CE[325] e do Regulamento (UE) N.º 910/2014.[326]

As definições de assinatura eletrónica que analisamos possuem a abrangência necessária para incluírem todos os tipos de assinatura eletrónica. Todos eles, na verdade, consistem em dados em suporte eletrónico que, de uma forma ou de outra estão ligados aos dados dos documentos, podendo essa ligação ser simples ou então consistir numa associação lógica.

Essa associação poderá ter níveis diferenciados de segurança e de evidência, e a forma como os dados de assinatura estão associados à pessoa que os utiliza pode ter

[325] Diretiva 1999/93/CE, de 13/12/1999. Transcrevemos a definição do n.º 1 do artigo 2.º: *"«Assinatura eletrónica»: os dados sob forma eletrónica, ligados ou logicamente associados a outros dados eletrónicos, e que sejam utilizados como método de autenticação"*

[326] Transcrevemos a definição do n.º 10 do artigo 3.º do Regulamento EIDAS: *"«Assinatura eletrónica»: os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar".*

também níveis diferenciados, sendo nessa diferenciação que se fundam os diversos tipos de autenticação das assinaturas eletrónicas.

Esses diversos graus de segurança e de certeza fundamentam os diversos efeitos jurídicos das assinaturas eletrónicas e dos documentos que sejam por elas autenticados.

3.4. As limitações de um conceito geral de assinatura eletrónica

O conceito de assinatura eletrónica que acabámos de analisar é genérico e pretende englobar todo o universo de tipos de assinatura eletrónica existentes, com níveis de segurança e de fiabilidade distintos. Por essa razão ele se centra nos requisitos essenciais de identificação, de vinculação e dos dados individuais utilizados para esse fim. Como referem os próprios documentos de trabalho da UNCITRAL, do que se trata é da definição de um conceito básico de assinatura, que cumpra os requisitos mínimos para ser considerada como tal.[327]

Trata-se de um conceito indispensável para que sobre ele opere o princípio da equivalência funcional entre as assinaturas eletrónicas e as manuais e para assegurar o princípio da não discriminação das assinaturas eletrónicas só pelo facto de se apresentarem nesse formato. Na expressão da própria UNCITRAL, trata-se de um conceito minimalista, assente no princípio da neutralidade tecnológica e no propósito de conferir uma relevância jurídica a todas as tecnologias de assinatura eletrónica.[328]

Ora, nas assinaturas manuais existem também níveis de garantia de fiabilidade que as partes podem utilizar à medida das suas necessidades de segurança e em conformidade com os níveis de risco. A necessidade de níveis mais elevados de garantia assume um relevo maior nas redes abertas para que seja possível realizar operações com eficácia jurídica com qualquer pessoa, independentemente do local onde esta se

[327] Como se refere nos trabalhos preparatórios, *"In an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the originator of an electronic communication, namely to identify the author of a document, and indicates the originator's intention in respect of the information contained in the electronic communication"*. "A/CN.9/608/Add.2", par. 26.

[328] *"This approach is also called minimalist, since it gives a minimum legal status to all forms of electronic signature. Under the minimalist approach, electronic signatures are considered to be the functional equivalent of handwritten signatures, provided that the technology employed is intended to serve certain specified functions and in addition meets certain technology-neutral reliability requirements"*. "A/CN.9/630/Add.2", par. 6.

encontre e independentemente do conhecimento que anteriormente se tenha dela ou não, bem como independentemente do valor dessa operação.

Nas assinaturas manuais, existem meios de autenticação da assinatura que conferem uma segurança jurídica adicional às partes intervenientes nos negócios, como é o caso da assinatura feita perante testemunhas, da assinatura reconhecida por notário, ou ainda da assinatura feita perante notário.[329] Existem também situações em que a lei assume a existência de assinaturas com menores garantias de segurança, como é o caso das assinaturas por chancela ou mediante reprodução mecânica.[330]

As garantias de segurança nas redes abertas são mais difíceis de alcançar, dada a possibilidade de através delas se estabelecerem relações com pessoas desconhecidas, muitas vezes localizadas em jurisdições nacionais também distintas. Por essas razões devem ser garantias eficazes e rigorosas, e possuir uma abrangência multinacional.

Subsistia, porém, a necessidade de regular a possibilidade da existência de um regime de segurança acrescida na assinatura eletrónica que, tal como ocorre nas assinaturas manuais, conferisse um grau de confiança mais elevado aos agentes económicos e que não excluísse a relevância jurídica dos restantes tipos de assinatura eletrónica.

Foi com esse propósito que surgiu a necessidade de se prever a existência de assinaturas dotadas de um nível de segurança jurídica e de confiança reforçada, que foram designadas de assinatura eletrónica avançada,[331] segura,[332] certificada,[333] ou qualificada.[334] É esse conceito que analisaremos de seguida.

3.5. A assinatura eletrónica qualificada

[329] Em Portugal, o artigo 375.º do Código Civil estabelece que a assinatura reconhecida por notário, num documento particular, se tem como verdadeira. Se o reconhecimento for efetuado por semelhança, vale como juízo pericial.

[330] O n.º 2 do artigo 373.º do Código Civil prevê a possibilidade de os documentos serem assinados por meios mecânicos, quando se trate de *"títulos emitidos em grande número"* ou nos *"casos em que o uso o admita"*.

[331] *"Enhanced electronic signature"*. "A/CN.9/457", par. 33.

[332] *"The word "secure" is not intended to indicate that any given technique may, in fact or in law, provide absolute security"*. A/CN.9/WG.IV/WP.73, par. 19.

[333] *"Certified electronic signature"*. "A/CN.9/457", par. 33.

[334] *"Sometimes referred to as "enhanced", "secure" or "qualified" electronic signatures"*. "A/CN.9/WG.IV/WP.88", par. 76.

3.5.1. Conceito de assinatura eletrónica qualificada

A assinatura eletrónica qualificada corresponde ao nível mais elevado de segurança jurídica na autenticação de documentos eletrónicos. Não se trata de um tipo novo de assinatura, diferente dos restantes,[335] mas de uma qualificação jurídica que é atribuída a qualquer tipo de assinatura eletrónica que cumpra um conjunto de requisitos funcionais da mais elevada exigência em matéria de confiança e de segurança.

O que distingue as assinaturas que cumprem estes requisitos são os seus efeitos jurídicos no que respeita à garantia das partes, de eficácia dos meios de vinculação jurídica das pessoas aos documentos eletrónico, bem como o cumprimento de um conjunto de requisitos formais e substanciais.

A necessidade de se regular a assinatura eletrónica qualificada foi sentida como forma de conferir às assinaturas eletrónicas um regime jurídico de confiança idêntico ao das assinaturas manuais, quando a lei exige alguma qualificação de segurança mais elevada.

Se no paradigma do papel, a lei confere a essas assinaturas um nível mais elevado de segurança jurídica quando estão reunidos pressupostos mais elevados de fiabilidade, deve também a legislação da assinatura eletrónica conferir a estas efeitos idênticos nos casos em que níveis acrescidos de fiabilidade estejam reunidos. A assinatura eletrónica qualificada pretende, assim, corresponder ao mais elevado nível de exigência legal em termos de segurança jurídica das assinaturas.

A assinatura eletrónica qualificada assegura um nível acrescido de fiabilidade e de segurança aos agentes económicos.[336] Esse facto não desqualifica as restantes

[335] Apesar de a adoção na legislação de uma assinatura com efeitos reforçados para a segurança das partes não desqualificar automaticamente as restantes formas de assinatura eletrónica, esse efeito pode ter relevância ao nível da eficácia das assinaturas eletrónicas em jurisdições estrangeiras, como veremos quando analisarmos mais adiante o regime do reconhecimento internacional. É que a existência de especificidades nacionais de qualificação pode ser um entrave à utilização da assinatura no comércio internacional, em especial quando não se trata de assinaturas qualificadas. E quando se utilizam estas, o seu efeito de gerarem eficácia adicional, pode ser eliminado pela inexistência de reconhecimento ou certificação nas jurisdições estrangeiras onde eventualmente possam necessitar de ser utilizadas. *"The downside to this approach is that once reliability a priori is predicated upon the use (among other conditions) of a particular technology, all other technologies – or even the same technology used under slightly different conditions – become a priori unreliable, or at least fall under suspicion a priori of unreliability"*. A/CN.9/630/Add.3, par. 6.

[336] *"It is merely intended to qualify a higher level of trustworthiness of an electronic signature by reference to a set of criteria which, once met, would entail certain legal effects"*. A/CN.9/WG.IV/WP.73, par. 19.

assinaturas eletrónicas como inseguras, nem lhes retira efeitos jurídicos.[337] Trata-se antes de um conjunto de requisitos que uma vez verificados, relativamente a qualquer tipo de assinatura, reforçam a sua capacidade para conferir segurança aos agentes económicos, do ponto de vista da sua eficácia para produzirem efeitos jurídicos.[338]

Parte-se de um sistema de duplo nível de assinaturas eletrónicas que tem na sua base a regra da não discriminação dos meios eletrónicos de autenticação e simultaneamente se consagra um regime que proporciona efeitos jurídicos reforçados àquelas assinaturas que cumprem pressupostos de maior segurança.[339] Assim acontece também com a LMAE, bem como com a legislação da UE e dos respetivos Estados Membros.

Os documentos legislativos da UE sobre assinatura eletrónica assentam neste sistema de duplo nível. A Diretiva 1999/93/CE, de 13/12/99, previa que os Estados Membros atribuíssem efeitos jurídicos às assinaturas eletrónicas avançadas baseadas num certificado reconhecido e criadas por um dispositivo seguro de criação de assinatura, não utilizando ainda o conceito de assinatura eletrónica qualificada.[340] Estas

---

[337] Durante os trabalhos preparatórios da LMAE foi debatido o efeito que teria a introdução de uma previsão normativa que estabelecesse os requisitos de uma assinatura eletrónica segura, nomeadamente na possibilidade de daí resultar uma desqualificação das restantes assinaturas como eventualmente inseguras. Prevaleceu o entendimento de manter um regime dual, por ser mais maleável e aberto a eventuais alterações de tecnologia. Assim, a possibilidade de qualquer assinatura eletrónica possuir relevo jurídico proporciona as condições para a expansão da sua utilização, sem prejuízo de as partes poderem recorrer a sistemas mais seguros quando assim o entenderem. Por outro lado deixa à liberdade das partes a possibilidade de escolherem um modelo de autenticação que entenderem como o mais adequado. Por exemplo, quando duas partes se conhecem e confiam mutuamente, não haverá tanta necessidade de utilizarem, nas transações que efetuam, assinaturas eletrónicas qualificadas. Nesses casos podem utilizar sistemas mais simples de autenticação, incluindo, por exemplo, a possibilidade de gerarem entre elas pares de chaves sem qualquer certificação de entidades terceiras. *"As a matter of freedom of contract, parties should be free to agree that, as between themselves, they would rely on an authentication technique that was less secure than the type of electronic signature described in subparagraph"*. "A/CN.9/446", par. 37.

[338] *"Widespread concern was expressed that an enhanced electronic signature would be considered as if it were a distinct legal concept, rather than just a description of a collection of technical criteria, the use of which made a method of signing particularly reliable"*. A/CN.9/465, par. 66.

[339] *"At the basic level, legislation adopting a two-tiered system generally grants electronic signatures functional-equivalence status with handwritten signatures, based on technologically neutral criteria. Higher-level signatures, to which certain rebuttable presumptions apply, are required to comply with specific requirements that may relate to a particular technology"*. "A/CN.9/630/Add.2", par. 16. Neste documento citam-se como exemplo de legislações que adotaram o sistema do duplo nível Singapura e a Diretiva das Assinaturas Eletrónicas da UE, mas a generalidade das legislações nacionais dos países da UE o adotam, aliás no seguimento da diretiva.

[340] O artigo 5.º da Diretiva, que estabelecia a equivalência das assinaturas eletrónicas às assinaturas legalmente reconhecidas em papel sob o título *"Efeitos legais das assinaturas eletrónicas"*, estabelecia que *"Os Estados-Membros assegurarão que as assinaturas eletrónicas avançadas baseadas num certificado qualificado e criadas através de dispositivos seguros de criação de assinaturas: a) Obedecem aos requisitos legais de uma assinatura no que se refere aos dados sob forma digital, do mesmo modo que uma assinatura manuscrita obedece àqueles requisitos em relação aos dados escritos; e b) São admissíveis como meio de prova para efeitos processuais"*.

assinaturas conferiam aos respetivos documentos o efeito jurídico que a lei interna estabelecia para os documentos em papel.

A diretiva estabelece um conjunto de requisitos substanciais necessários para que os certificados sejam reconhecidos, no anexo I. Estabelece também, relativamente aos prestadores de serviços de certificação, um conjunto de requisitos que devem cumprir para que possam emitir certificados reconhecidos (Anexo II), bem como os requisitos que devem cumprir os dispositivos seguros de criação de assinaturas eletrónicas (Anexo III). As assinaturas eletrónicas qualificadas são aquelas que cumprem esses três tipos de requisitos substanciais. Esta técnica seguiu o exemplo da LMAE, que anexa uma lista de requisitos substanciais para que as assinaturas eletrónicas possam ser consideradas como qualificadas.

Trata-se de requisitos destinados a garantir a máxima segurança dos meios de autenticação eletrónica, em três níveis, tanto no que respeita ao rigor dos procedimentos das entidades de certificação, como aos certificados, como ainda no que respeita aos meios de assinatura.

A consagração legislativa das assinaturas eletrónicas qualificadas é um importante avanço na criação de condições de segurança para os agentes económicos utilizarem os meios eletrónicos nas suas operações. Este efeito acrescido de confiança e de segurança jurídica é o adequado para responder às necessidades emergentes das situações de maior risco, em face dos valores envolvidos nas transações ou de outros fatores de álea jurídica.

3.5.2. Efeitos jurídicos da assinatura eletrónica qualificada

Os efeitos da assinatura eletrónica qualificada traduzem-se numa maior eficácia probatória no que respeita à identificação do seu titular e à sua vinculação jurídica aos documentos a que é aplicada, dados os níveis mais elevados de autenticação que ela proporciona.

Essa maior força probatória é conferida pela lei mediante o estabelecimento de uma presunção legal de prova ou então uma estatuição imperativa que atribua a este tipo de assinatura efeitos probatórios determinados.

Em termos comparativos poderíamos dizer que o nível de confiança que a assinatura eletrónica qualificada confere às partes é idêntico àquele que as assinaturas

manuais reconhecidas por notário conferem, embora não cumpram esse formalismo.[341] O objetivo da consagração legal das assinaturas eletrónicas qualificadas é exatamente o de estabelecer uma equivalência funcional a esse tipo de assinaturas, assim se alcançando um regime de equivalência pleno entre as assinaturas manuais e as eletrónicas.[342]

Nas assinaturas em papel, a função do notário, quando efetua a autenticação da assinatura é assegurar, perante todos os interessados que:

i) Identificou, ele próprio o assinante;

ii) Verificou que a assinatura foi colocada no documento pessoalmente pelo assinante;

iii) Seguiu todos os procedimentos formais legalmente estabelecidos, no que respeita à identificação do autor da assinatura e de observação da sua efetiva participação no ato de assinar;

iv) Assegura, como entidade dotada de fé pública, e portanto como entidade de confiança, que aquela pessoa ficou vinculada àquele contrato.[343]

---

[341] A necessidade de se estabelecer um regime de equivalência das assinaturas eletrónicas às assinaturas manuais de valor reforçado, nomeadamente quando certificadas por notário, havia sido sentida em face do carácter manifestamente insuficiente do artigo 7.º da LMCE, em face da emergência e do acelerado crescimento da utilização das redes abertas. *"However, the determination of what constituted a reliable method of signature in the light of the circumstances could only be made under article 7 of the Model Law by a court or other trier of fact intervening ex post, possibly long after the electronic signature had been used"*. E mais adiante, *"In contrast, the benefit expected from the Uniform Rules in favour of certain techniques, which were recognized as particularly reliable, irrespective of the circumstance in which they were used, was to create certainty (through either a presumption or a substantive rule), at or before the time any such technique of electronic signature was used (ex ante), that it would result in legal effects equivalent to those of a handwritten signature"*. "A/CN.9/465", par. 64.

[342] Certeza e previsibilidade são os dois conceitos de referência que servem como objetivos de um regime jurídico das assinaturas eletrónicas qualificadas, e que estiveram sempre presentes nos trabalhos da UNCITRAL. *"It nevertheless gave a clear message that certainty and predictability could be achieved by determining which signature techniques satisfied the reliability criteria of draft articles 6 and 7"*. "A/CN.9/465", par. 91.

[343] A circunstância de a fé pública só poder ser conferida por notários, não dispensa a participação destes quando a lei a exige expressamente, no reconhecimento dos atos respetivos. Embora a assinatura eletrónica qualificada confira o mais elevado grau de fiabilidade na vinculação, sempre se levantará o problema da fé pública. A legislação italiana prevê a existência de notários que certificam as assinaturas eletrónicas, assinando, eles próprios os documentos assinados pelas partes (artigo 25.º, n.º 1 do "Codice D'ella Administrazioni Digitale". Ruggieri, F. (2008). Comments on the Italian 'Code For Digital Administration. *Digital Evidence and Electronic Signature Law Review*, Vol 5: pág. 29. Porém, essa exigência não é comum. E embora a segurança das assinaturas qualificadas seja a mais elevada, não nos parece que possa ser dispensada a intervenção do notário no caso em que a lei expressamente o exige. A intervenção do notário acrescenta certeza jurídica acerca da confirmação de que a pessoa que assina é o titular do certificado, mas essa garantia já é conferida pelo certificado, nos casos em que é qualificado. Ruggieri acrescenta que o notário pode certificar também que o autor assinou livremente o documento *("the public officer is required to ascertain if (...) the person has signed the document freely"*. *Ibidem*, pag. 33.), mas essa é já uma função externa à função da assinatura. O papel dos notários na autenticação

Os efeitos jurídicos de uma assinatura que preencha os requisitos necessários para ser considerada qualificada consistem também numa presunção de vinculação de uma pessoa determinada e identificada a um documento, pelo que nessa matéria se trata de efeitos equivalentes. A diferença está apenas no funcionamento do regime de prova nos casos em que a assinatura ou o documento sejam impugnados. No caso da assinatura eletrónica qualificada, a metodologia de apreciação do tribunal será diferente, em função da distribuição do ónus probatório pelas partes.[344] No caso das assinaturas não qualificadas terá que ser efetuada uma avaliação da fiabilidade da assinatura, no caso das assinaturas qualificadas essa fiabilidade deriva diretamente da lei, cabendo à parte impugnante o ónus probatório da destruição desse pressuposto.[345] O estabelecimento deste regime probatório é muito importante, dada a reconhecida dificuldade de se fazer prova em tribunal nesta matéria.[346]

Em termos substanciais, levantam-se questões acerca do efeito da utilização da assinatura eletrónica qualificada. Segundo uma teoria, esse efeito deveria limitar-se à segurança do instrumento técnico que aplica a assinatura, como dispositivo eletrónico. Entendia-se que a qualificação da assinatura não deveria ir além desse instrumento,

---

dos documentos e das assinaturas eletrónicas tem levantado dúvidas. Por exemplo a lei espanhola da assinatura eletrónica de 1999 ressalvava que as suas normas em nada prejudicavam a função das entidades dotadas de fé pública. Na lei de 2003 (Ley 59/2003, de 19 de diciembre), a alínea a) do n.º 6 do artigo 3.º prevê que os documentos eletrónicos possam ser autenticados por notários. Nadal refere que a função notarial é diferente da função de assinatura eletrónica: *"en ningún caso los notários puden ser substituídos por un prestador de servícios de certificación (...) cuya función es distinta y (...) no está revestida de los atributos própios de aquellos"*. Nadal, A.G. (2009). Op. cit., pag. 42. Em nosso entendimento a função distingue-se apenas pela fé pública que as entidades certificadoras não conferem, sendo que a segurança jurídica da sua função notarial se pode aproximar, no que respeita à identificação do autor da assinatura e da fiabilidade desta, daquela que é conferida pelos notários, quando se trate de assinaturas qualificadas. Apesar disso, a verificação da assinatura pode ser um serviço prestado por um prestador certificado, caso em que essa verificação pode ser atestada e classificada como segura, por ter sido feita por um operador especializado.

[344] Como se refere num dos documentos de trabalho da UNCITRAL, *"The consequence of this approach, however, is that such conditions are typically only confirmed a posteriori, and there is no assurance that a court will recognize the use of any particular method".* A/CN.9/630/Add.3, par. 5.

[345] A determinação do efeito vinculante de uma assinatura ao seu autor, quando impugnada, terá que ser sempre efetuada pela entidade competente para a avaliação, em função da conformidade dos procedimentos conexos com a sua aplicação, bem como os seus atributos, com o quadro legal existente. No caso de litígios judiciais essa atividade de probatória terá que ser desenvolvida pelo tribunal, confrontando as circunstâncias de facto com os requisitos legais de fiabilidade. *"When legislation adopts the minimalist approach, the issue of whether electronic signature equivalence has been proven normally falls to a judge, arbitrator or public authority to determine, generally by means of the so-called "appropriate reliability test". Under this test, all types of electronic signature that satisfy the test are considered valid; hence, the test embodies the principle of technological neutrality"*. "A/CN.9/630/Add.2", par. 11.

[346] *""Proof to the contrary" might require detailed and costly investigations of the various technical devices and procedures involved in the creation of the electronic signature".* A/CN.9/WG.IV/WP.84, par. 47.

nomeadamente não poderia abranger a intenção do seu autor, de se vincular, e menos ainda de aprovar o conteúdo do documento assinado.

Outros entendimentos alargavam o âmbito de abrangência da qualificação à identificação do autor da assinatura, e outros ainda à segurança acerca da sua participação pessoal no ato da assinatura.[347]

O nível mais elevado de segurança alcança-se quando todos esses elementos conexos com a criação da assinatura estão assegurados, bem como quando a identificação do seu autor se revela a mais eficaz e segura.

A generalidade dos instrumentos normativos utiliza o princípio da equivalência funcional para estabelecer a regra de que se consideram cumpridos os requisitos legais de assinatura manuscrita reconhecida previstos na lei para as assinaturas manuais, nos casos em que se utiliza a assinatura eletrónica qualificada.[348] Centra-se, assim, nos efeitos da assinatura, a definição dos requisitos da assinatura eletrónica qualificada.

Embora nas primeiras versões do projeto da LMAE se contemplasse a existência de um tipo de assinatura eletrónica de mais elevada fiabilidade, designada de assinatura eletrónica referendada, ou reforçada, na tradução literal do inglês *"enhanced electronic signature"*, esse conceito não foi transposto para a versão final, pelas razões que já antes expusemos.[349] Apesar disso, era necessário criar um regime de equivalência entre a assinatura eletrónica e as assinaturas manuscritas reconhecidas, para os casos em que a lei as exigisse. É em resposta a essa preocupação que se deve analisar o conteúdo do art.º 6.º da LMAE, que estabelece o seu âmbito de aplicação para os casos em que se trate de assinaturas expressamente exigidas por lei. Ora essas assinaturas são aquelas em que a lei exige uma determinada forma, e isso ocorre, normalmente, nos casos em que a lei exige requisitos de confiança acrescidos, como é o caso das assinaturas reconhecidas por entidade que lhe confira fé púbica. É para estabelecer um regime de equivalência funcional a esse tipo de assinaturas que se dirige o art.º 6.º. A referência à lei, constante da parte inicial do n.º 1 ("*Where the law requires a signature of a person")*, deve ser entendida como uma substituição do conceito de assinatura qualificada, mas com a necessidade de restringir o conjunto de requisitos de segurança adicionais que constam

[347] Uma exposição dos diversos entendimentos expressos e debatidos nos trabalhos de conceção da LMAE consta desenvolvida nos par.s 67 a 70 do "A/CN.9/465".

[348] Essa foi também a conclusão do Grupo de Trabalho da UNCITRAL. *"The Working Group generally agreed that the focus of draft article 6 should be on replicating in an electronic environment the legal consequences of the use of a handwritten signature"*. "A/CN.9/465", par. 70.

[349] *"Noting its earlier decision to delete the definition of "enhanced electronic signature" (see above, par. 64), the Working Group decided to delete the word "enhanced" in subparagraph (e)"*. "A/CN.9/483", par. 78.

desse artigo, apenas aos casos de assinaturas formais que a lei exige.[350] Uma assinatura eletrónica que não cumpra aqueles requisitos, não equivale a uma assinatura formal, mas continua a ser uma assinatura eletrónica.[351] E essas outras assinaturas eletrónicas possuem também relevância jurídica e são suscetíveis de produzir efeitos jurídicos de vinculação das partes, beneficiando essas assinaturas do reconhecimento legal resultante da aplicação do princípio da não discriminação e da equivalência funcional.[352]

A Diretiva 1999/93/CE prevê no n.º 1 do art.º 5.º, que os Estados Membros devem estabelecer uma equivalência plena entre as assinaturas eletrónicas que cumprem os requisitos correspondentes e as assinaturas manuscritas.

O Regulamento EIDAS introduz importantes alterações ao conceito de assinatura eletrónica qualificada. Em primeiro lugar, estabelece, de forma expressa e imperativa, que as assinaturas eletrónicas qualificadas possuem um efeito legal equivalente ao das assinaturas manuscritas, consagrando assim uma equivalência plena das assinaturas eletrónicas qualificadas à assinatura manual, independentemente do grau de garantia de segurança desta (no n.º 2 do art.º 25.º). Esta equivalência traduz-se, em termos práticos, no estabelecimento de uma presunção legal de que estas assinaturas

---

[350] O Guia de Transposição da LMAE refere o objetivo era o da criação de um tipo de assinatura reforçada. *"The new Model Law is expected to create a benefit in favour of certain techniques, which are recognized as particularly reliable, irrespective of the circumstances in which they are used. That is the purpose of paragraph 3, which is expected to create certainty (through either a presumption or a substantive rule), at or before the time any such technique of electronic signature is used (ex ante), that using a recognized technique will result in legal effects equivalent to those of a handwritten signature".* "UNCITRAL Model Law ... 2001", par. 118. Apesar desse propósito, a verdade é que da LMAE constam os requisitos substanciais e a previsão da sua adoção pelas legislações nacionais, mas a verdade é que não definiu os requisitos formais e os procedimentos de criação desse tipo de assinaturas.

[351] Pretendia-se que a introdução dos requisitos de fiabilidade e de segurança adicionais que constam dos artigos 6.º e 7.º da LMAE, não afastasse do regime das assinaturas eletrónicas aquelas que não cumprissem esses requisitos, mas que fossem, na mesma, instrumentos de autenticação. Pretendeu-se criar um tipo de assinaturas de valor de segurança reforçado, sem prejuízo de continuarem a existir formas de assinatura de mais baixo nível de segurança. *"Those duties and obligations, it was said, might be appropriate in connection with high-value certificates or electronic signatures of the type previously referred to as "enhanced electronic signatures". However, those duties and obligations might be excessive with respect to low-value certificates or electronic signatures offering a lesser degree of security"*. Inicialmente ponderou-se, nos trabalhos preparatórios da LMAE, que se estabelecesse para esse tipo de assinaturas, uma definição do conceito de "assinante", limitando-o aos casos em que ao assinante de documentos em que a lei exige determinada forma de assinatura. *"One suggestion to counter that problem was to restrict the definition of "signatory" by limiting it to persons by whom or on whose behalf "legally required signatures" could be created"*. A versão final da LMAE seguiu a opção de limitar a esses casos e âmbito do 6.º. "A/CN.9/483", par. 78.

[352] Este cuidado de salvaguardar os efeitos jurídicos das assinaturas eletrónicas que não cumpram os requisitos de serem consideradas como qualificadas, foi salvaguardado na LMAE, e é uma das razões para que o conceito de assinatura eletrónica qualificada tenha sido eliminado da LMAE. Como bem se refere nos comentários de Singapura ao projeto de UNCUECIC, as assinaturas eletrónicas são válidas por si, sem necessidade de corresponderem a nenhum requisito especial de fiabilidade. *"In our view, electronic signatures are merely another form of signature, and should in principle be legally valid as signatures without any special requirements of reliability"*. "A/CN.9/578/Add.10", par. 18.

asseguram identificação do signatário, a autenticidade da assinatura e do documento, e a sua integridade. O estabelecimento desta equivalência aplica-se também aos selos eletrónicos qualificados (n.º 2 do artigo 35.º) que, na prática, correspondem a assinaturas eletrónicas de pessoas coletivas.

Em segundo lugar, o Regulamento EIDAS estabelece um regime de criação e de gestão das assinaturas eletrónicas qualificadas, criando a categoria dos prestadores qualificados de serviços de segurança, fazendo depender essa atribuição de um conjunto de requisitos minuciosamente regulados como veremos mais adiante. O regime dos prestadores qualificados adquire natureza pública e imperativa, aplicando-se a todos os Estados Membros, fazendo depender a classificação de prestador qualificado, de uma avaliação prévia do conjunto dos requisitos de segurança, por entidades de avaliação de conformidade, bem como de uma decisão das entidades de supervisão.

Além da eficácia jurídica das assinaturas eletrónicas qualificadas e dos selos qualificados, o Regulamento EIDAS faz também assentar neste tipo de assinaturas, a criação de um sistema europeu de interoperabilidade das assinaturas eletrónicas qualificadas e de reconhecimento mútuo da sua validade e dos seus efeitos em todos os Estados Membros.

3.5.3. Requisitos substanciais da assinatura eletrónica qualificada

Os requisitos constitutivos da classificação de uma assinatura eletrónica como qualificada foram definidos pela primeira vez no art.º 6.º da LMAE, que deve ser interpretado em sequência com o art.º 7.º da LMCE.[353] [354] Mais tarde, em 2007, a UNCUECIC haveria de também conter normas idênticas acerca das assinaturas eletrónicas com valor reforçado.[355]

[353] A formulação legislativa não utiliza o conceito de assinatura eletrónica qualificada, embora estabeleça os respetivos pressupostos e efeitos de equivalência funcional das assinaturas eletrónicas às assinaturas manuscritas autenticadas no seu artigo 6.º da LMAE. A generalidade das legislações nacionais, haveria de, nessa sequência, vir a consagrar aquela designação. *"It was also agreed that, while the revised version of draft article 7 to be prepared by the Secretariat would no longer mention the notion of "enhanced electronic signature", it should not be interpreted as preempting the final decision of the Working Group, to be made at a later stage, as to whether the draft Uniform Rules would refer to that notion or not"*. "A/CN.9/465", par. 89.

[354] Os requisitos da assinatura eletrónica qualificada constam do n.º 3 do artigo 6.º da LMAE, (com o título "*Compliance with a requirement for a signature"*). A/CN.9/493"01, pág.s 6 e 7.

[355] Essa previsão consta do n.º 3 do artigo 9.º da "UNCUECIC".

Aquele art.º 7.º estabelecia que a assinatura consistia num método de identificação de uma pessoa e de determinação da sua aprovação de um documento que, para que fosse equivalente a uma assinatura formal, teria que ser fiável, sendo que essa fiabilidade teria sempre que ser avaliada, e que essa avaliação teria que ser efetuada à luz das circunstâncias do caso ou da existência de eventuais acordos de autenticação prévios. A LMCE não estabelecia os pressupostos de determinação da fiabilidade, sendo que essa falta de densificação se atribui ao facto de, à data da sua elaboração, não serem conhecidos meios tecnológicos que o permitissem. Essa lacuna era um fator de insegurança para os agentes económicos, dado que não poderiam obter certeza acerca do efeito vinculativo reforçado das assinaturas.

A LMAE representa um avanço na densificação dos pressupostos substanciais na assinatura qualificada, porque passam a ser definidos de forma objetiva, oferecendo assim uma maior segurança às partes.

Os requisitos substanciais que são constitutivos da assinatura eletrónica qualificada foram identificados nos trabalhos preparatórios como sendo os de identificação, exclusividade, fiabilidade em sentido estrito, vinculação e integridade.[356] Analisamos, de seguida, cada um deles.

1. - A identificação é a primeira função da assinatura eletrónica, indispensável para que exista segurança na assinatura que a torne merecedora da classificação como qualificada. Essa segurança é, antes de mais, a segurança acerca da identidade do signatário e é essencial à vinculação de uma pessoa a um documento. Ela depende da segurança dos procedimentos utilizados pela entidade certificadora que gerou o instrumento de criação da assinatura, para identificar o respetivo titular e se certificar da sua efetiva identidade.[357] É este requisito que garante que um terceiro de má-fé não se poderá fazer passar pelo real titular da assinatura.
2. O requisito da exclusividade garante que o instrumento de criação da assinatura, que no caso da assinatura digital é a chave privada, só possa ser

[356] Essa identificação é resumida da seguinte forma:*"With a view to providing a basic standard against which the quality of such electronic signatures might be assessed, subparagraph (c)(ii) lists four criteria: uniqueness, identification, reliability, and linkage with the information being signed"*. A/CN.9/WG.IV/WP.73, par. 22.

[357] Este requisito está estabelecido na alínea a) do n.º 3 do artigo 6.º da LMAE, que tem a seguinte redação: *(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;"*. "A/CN.9/493", pág. 6.

utilizado pelo seu titular.[358] Essa exclusividade é assegurada pelo cumprimento dos procedimentos de segurança na entrega do certificado e da chave privada ao seu titular. Este princípio deve garantir que não existe probabilidade razoável de que outra pessoa possa utilizar aquela chave privada.[359]

3. O requisito da fiabilidade em sentido estrito assegura que o dispositivo de criação da assinatura, ou seja, o dispositivo onde está a chave privada, só pode ser utilizado pelo seu titular.[360] Este requisito destina-se a garantir que sempre que é utilizada a chave privada de uma pessoa, ela só pode ter sido utilizada por essa pessoa.[361] Essa segurança depende da adoção de um conjunto de procedimentos que assegurem que em caso de perda ou extravio do dispositivo, bem como sempre que terceiros tenham, ou possam ter, a ela acesso, se procederá ao cancelamento do certificado ou à eliminação da possibilidade de um terceiro se apoderar dele e assinar documentos de forma ilegítima em nome do titular. O procedimento de gestão das chaves privadas, tanto no que respeita ao comportamento do seu titular como ao prestador de serviços de certificação, deve assegurar com o mais elevado grau de certeza possível, que o dispositivo de assinatura eletrónica não possa ser indevidamente utilizado por terceiro.
4. Ao contrário dos anteriores, que relacionam a assinatura com o seu titular, o requisito da vinculação relaciona a assinatura com o documento a que foi

[358] Este requisito está ínsito também na alínea a) do n.º 3 do artigo 6.º da LMAE.

[359] *"The requirement that a secure electronic signature be "uniquely linked" to the person applying it is intended to ensure that there is no reasonable likelihood that more than one person would produce the same signature absent fraud or other improper conduct*". A/CN.9/WG.IV/WP.73, par. 23.

[360] Este requisito está estabelecido na alínea b) do n.º 3 do artigo 6.º da LMAE, que tem a seguinte redação: *"(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person"*. "A/CN.9/493", pág. 6.

[361] Nas notas das reuniões preparatórias da LMAE é dado o exemplo da utilização de uma senha de acesso numa caixa automática para levantar dinheiro. Essa senha de acesso garante ao banco que foi utilizada a senha de determinada pessoa que o banco conhece previamente e com ela tem uma relação contratual. Mas não garante que efetivamente essa pessoa que efetuou a operação e não outra, porque o banco não tem forma de o saber. O titular da senha de acesso terá uma enorme dificuldade em provar que não foi ele que efetuou a operação. É essa garantia, e a possibilidade de a assegurar, que o princípio da fiabilidade, se destina a prosseguir. *"The use of a personal identification number (PIN) in an automatic teller machine provides the bank with an automatic, objective, and prompt identification of a specific person that is tied to a specific address and a specific account number when the funds are withdrawn. Such a person is not in a position to deny that the request for funds contains his or her signature (although that person may deny having signed the request; that is the subject of the reliability requirement)"*. A/CN.9/WG.IV/WP.73, par. 23.

aplicada.[362] Este requisito assegura que uma determinada assinatura que foi colocada num determinado documento não possa ser extraída dele e depois ser indevidamente utilizada para assinar outro documento. Garante, portanto, a integridade da assinatura e a exclusividade da sua conexão lógica e única com o documento. Para garantir a integridade da assinatura é necessário que existam sistemas de deteção da sua eventual utilização perversa. A assinatura eletrónica de uma pessoa não é uma entidade rígida, com uma ontologia própria. Embora o par de chaves seja único e imutável e o resultado da sua aplicação a um mesmo documento seja sempre o mesmo, esse resultado é diferente para cada documento. Caso o símbolo de uma assinatura de um documento seja ilicitamente copiado e colocado noutro, deve o sistema de assinatura estar dotado de funcionalidades que inutilizem a assinatura, nomeadamente assinalando que ela está invalidada.[363]

5. O requisito da integridade é idêntico ao da vinculação, porque se reporta também à segurança da conexão da assinatura com o documento assinado. Mas, ao contrário dele, não tem por objeto a integridade da assinatura, mas a integridade do próprio documento.[364] A assinatura, para ser segura, deve ser capaz de detetar todas as alterações que eventualmente sejam efetuadas no documento depois de ter sido assinado, evidenciar que essas alterações foram efetuadas e estar dotada de mecanismos que tornem a assinatura inválida e evidenciem essa invalidação. Este requisito não é exclusivo da assinatura eletrónica em geral, dado que a garantia da integridade dos documentos é externa à assinatura, uma vez que se reporta a acontecimentos eventuais que são sempre posteriores ao ato de assinar. Porém, em muitas circunstâncias a lei exige que um determinado documento eletrónico seja assinado, tendo

[362] Este requisito consta da alínea c) do n.º 2 do artigo 6.º da LMAE, que tem a seguinte redação: *"(c) any alteration to the electronic signature, made after the time of signing, is detectable"*. "A/CN.9/493", pág. 6.

[363] *"A secure signature must be linked to the data message being signed, in such a manner that if the message is changed the signature is invalidated"*. A/CN.9/WG.IV/WP.73, par. 26.

[364] Nas assinaturas eletrónicas, a integridade da assinatura fica corrompida com a quebra da integridade do documento, dado que a assinatura opera com os dados que compõem o próprio documento, pelo que, alterando-se os dados quebra-se a assinatura. Esta é uma diferença importante relativamente à assinatura manuscrita, onde a assinatura se pode manter íntegra, apesar de o documento de base ter sido alterado. No mesmo sentido, Ormazábal Sanchez, *"la autenticidade de la firma digital no es disociable de la valoración de los datos cifrados"* e mais adiante, *"fijada la autenticidad de la firma queda excluída cualquier duda sobre la autenticidade de la información documentada"*. Sánchez, O.G. (2010). La Incidencia de la Ley de la Firma Electrónica en el Valor Probatorio de los Soportes Informáticos. Mucho Ruido y Pocas Nueces. Em: *Presente y Futuro de la e-Justicia en Espanha y la Unión Europea*. Thomson Reuters, Aranzadi, Pamplona, pag. 237.

como objetivo garantir a sua integridade. Nesses casos, este requisito é essencial à assinatura.[365]

A verificação destes requisitos nem sempre é assegurada por todos os tipos de assinatura eletrónica, seja porque a tecnologia que se utiliza não o permite, seja porque, permitindo-o, não estão reunidas condições de segurança para se poder concluir que está garantida a sua efetividade. São exemplo disso os casos de digitação do nome de uma pessoa no final de uma mensagem, as assinaturas digitalizadas, mas também a utilização das palavras-chave, em que ambas as partes que efetuam negócios entre si mediante a utilização de meios eletrónicos, conhecem, ou podem conhecer, o código de autenticação.

Do mesmo modo, mesmo quando se utiliza a tecnologia das assinaturas digitais, podem não ser observados os requisitos substanciais que acabamos de enunciar. Isso ocorre, por exemplo, quando duas partes que se conhecem entre si, utilizam chaves criptográficas geradas por elas próprias, sem qualquer intervenção de um terceiro prestador de serviços. Na verdade, é possível emitir pares de chaves criptográficas assimétricas sem necessidade de intervenção de entidades terceiras. Essa emissão pode ser efetuada por uma das partes, que entrega à outra uma chave privada, para ser utilizada, voluntariamente por ambas.

É também possível que duas partes utilizem como sistema de autenticação, nas comunicações que fazem entre si, uma palavra-passe, mas, para garantir sigilo nas comunicações, a parte que envia aplica sobre o documento a chave pública do destinatário.[366]

A utilização destes mecanismos de assinatura pode ser também segura, mas é-o apenas nas relações entre as partes, e a avaliação da sua fiabilidade tem a dificuldade de ser efetuada sempre *a posteriori*, o que não proporciona às partes uma segurança completa, dado que sempre ficarão dependentes de uma avaliação que é futura e com algum grau de incerteza.[367]

---

[365] É por essa razão que a norma que consagra este requisito, constante da alínea d) do n.º 3 do artigo 6.º da LMAE, se inicia por estabelecer o seu âmbito de aplicação aos casos em que o objetivo da exigência de assinatura seja a garantia de integridade do documento. "A/CN.9/493", pág. 6.

[366] Dessa aplicação resulta a encriptação do documento, que só poderá ser desencriptado pelo destinatário, utilizando a sua chave privada.

[367] A avaliação da fiabilidade da assinatura dependeria sempre do contexto concreto em que ela foi utilizada, e ainda da finalidade concreta que se perseguia com a sua aplicação. A fiabilidade depende, assim, do contexto e da finalidade em concreto, o que se compreende pelo carácter instrumental da assinatura, relativamente aos negócios ou atos em que é aplicada. *"In the light of all the circumstances, including any agreement between the originator and the addressee of the data message, the signature or*

A utilização de assinaturas qualificadas tem a vantagem de conferir uma maior segurança jurídica às partes, nomeadamente quando efetuadas em redes abertas, mas é sempre mais onerosa, e poderá não ser necessária em transações efetuadas por agentes económicos que se conhecem entre si, em especial quando esse conhecimento é complementado com a existência de convenções de autenticação que as partes estabeleceram livremente entre si, aceitando o seu efeito vinculativo.

Para estes casos poderão as partes entender não ser necessária a existência de uma categoria de assinaturas eletrónicas de segurança reforçada, que normalmente exigem a intervenção de terceiros independentes e especializados.[368] Por essa razão a própria previsão da existência de assinaturas com grau de fiabilidade mais elevado não era pacífica, porque poderia conduzir a que as restantes fossem consideradas como menos eficazes no seu efeito vinculativo.[369] Considerava-se até que essa previsão poderia causar ainda dificuldades de interoperabilidade, em especial nos casos de reconhecimento internacional das assinaturas.[370] Na verdade, ao estabelecerem-se requisitos diferenciados entre países diferentes, esse facto poderia causar dificuldades no reconhecimento internacional.[371] Mas prevaleceu sempre a opção pela manutenção

---

authentication method must be shown to be as reliable as is appropriate for the purpose for which the data message is generated or communicated". "A/CN.9/630/Add.3", paragrafo 4.

[368] O nível de fiabilidade de uma assinatura é questão que interessa em primeiro lugar aos intervenientes nas comunicações eletrónicas, que a saberão adequar ao contexto e às finalidades em que a utilizam, bem como ao tipo de equipamentos e de sistemas que utilizam. *"The level of reliability depended on the information system and that it was for the parties to choose the level of reliability adequate for their transactions"*. "A/CN.9/797", par. 86. Nas citações seguintes deste documento, referenciá-lo-emos de forma sintética por "A/CN.9/797".

[369] Tal como se refere nos comentários de Singapura ao projeto de UNCUECIC, mais importante que a forma da assinatura eletrónica é a prova do vínculo entre ela e o assinante, tendo em conta o contexto, que é determinante da sua eficácia. *"It is not the form of the signature, but the proven link between the signature and the purported signor based on the context, that gives the signature its legal effect"*. "A/CN.9/578/Add.10", par. 18.

[370] Essas dificuldades eram ainda recentemente manifestadas em matéria de utilização de documentos eletrónicos transferíveis no transporte internacional de mercadorias. *"The presence of a general reliability standard could hamper use of electronic transferable records as legal consequences of failure to meet those standards were not clear"*. A/CN.9/WG.IV/WP.130, par. 69. Apesar disso, manteve-se o entendimento de adoção, nesta material, de uma norma geral de fiabilidade, com o cuidado de respeitar o princípio da neutralidade tecnológica. *"It was further mentioned that if a general reliability standard were to be included, it should be drafted in a manner mindful of technological neutrality"*. A/CN.9/WG.IV/WP.132, par. 67.

[371] *"Setting mandatory minimum requirements could have a negative impact on existing business practices, which differed significantly in the way they ensured reliability"*. "A/CN.9/797", par. 86. Esta mesma reserva é ainda colocada atualmente, nos trabalhos que decorrem em matéria de harmonização das normas relativas aos documentos de transporte de mercadorias no mercado internacional. *"The presence of a general reliability standard could hamper the use of electronic transferable records as legal consequences of failure to meet those standards were not clear"*. A/CN.9/804, par. 42.

do requisito da fiabilidade das assinaturas, por efeito da sua importância para a sua utilização segura nas redes abertas.[372]

Do mesmo modo que a assinatura manuscrita, a assinatura eletrónica deve possuir níveis de fiabilidade que correspondam a essas necessidades.[373] Por essa razão prevaleceu o sentido de que a assinatura eletrónica deve também refletir essa diferenciação.

É nesse sentido que, para além do postulado genérico de equiparação da assinatura eletrónica às assinaturas manuscritas reconhecidas, a LMAE consagra a possibilidade de existência de assinaturas que possuam caraterísticas intrínsecas, que lhes confiram desde logo essa equivalência.

3.5.3.1. Requisitos substanciais da legislação da UE

A Diretiva 1999/93/CE[374] estabeleceu uma tripla exigência para que as assinaturas eletrónicas possuam o efeito jurídico das assinaturas eletrónicas qualificadas.

Essa tripla exigência compõe-se dos seguintes três conjuntos de requisitos:[375]

i) Que se trate de assinaturas eletrónicas avançadas;

ii) Que sejam baseadas num certificado qualificado e que;

iii) Sejam criadas por um dispositivo seguro de criação de assinatura.

Trata-se de três requisitos cumulativos, que só os tipos de assinaturas tecnologicamente mais avançadas podem cumprir, o que se compreende pelos efeitos que delas resultam em termos de vinculação jurídica.

O Regulamento EIDAS, mantendo a mesma estrutura de requisitos substanciais, especifica que o último requisito deve garantir que o dispositivo de criação da assinatura deve ser também ele qualificado, criando para o efeito essa figura jurídica.

---

[372] Como se refere num documento recente da UNCITRAL, "*While party autonomy could suffice to establish reliability standards in closed systems, there was a need for the draft provisions to set out reliability standards applicable to open systems".* "A/CN.9/804", par. 43.

[373] *"The degree of trustworthiness offered by a certificate should normally be commensurate with the purposes for which the certificate was used"*. "A/CN.9/483", par. 79.

[374] Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13/12/1999.

[375] N.º 1 do artigo 5.º da Diretiva: *"1. Os Estados-Membros assegurarão que as assinaturas eletrónicas avançadas baseadas num certificado qualificado e criadas através de dispositivos seguros de criação de assinaturas: a) Obedecem aos requisitos legais de uma assinatura no que se refere aos dados sob forma digital, do mesmo modo que uma assinatura manuscrita obedece àqueles requisitos em relação aos dados escritos; e b) São admissíveis como meio de prova para efeitos processuais"*.

Do mesmo modo, no que respeita aos certificados qualificados, a sua emissão fica também expressamente reservada aos prestadores de serviços qualificados, que o Regulamento passa a regular.[376]

Outra das mais importantes inovações do Regulamento é a criação do estatuto de prestador qualificado de serviços de confiança, e um dos requisitos dos certificados qualificados de assinatura eletrónica é de que tenha sido emitido por um prestador com esse estatuto.

Analisamos, de seguida esses requisitos:

3.5.3.1.1. Que se trate de assinatura eletrónica avançada

A assinatura eletrónica avançada corresponde, em termos gerais, à assinatura digital, assente na criptografia assimétrica, por ser a única que garante os requisitos legais estabelecidos e a efetividade da ligação entre dados. Esses requisitos foram genericamente estabilizados na LMAE, tendo sido acolhidos também na Diretiva Europeia e no Regulamento EIDAS e são os seguintes:[377]

i) A assinatura estar associada de modo único ao signatário. Na versão da diretiva utilizava-se o requisito de que deveria estar associada inequivocamente ao signatário. O Regulamento EIDAS é mais exigente, dado que o requisito da unicidade na conexão entre o signatário e cada assinatura que ele cria é essencial à segurança jurídica. Vinca-se a natureza única e irrepetível de cada assinatura;

ii) Permitir a identificação do signatário, uma das funções nucleares da assinatura eletrónica, e a identificação deve emergir diretamente do produto que evidencia a assinatura. A identificação não emerge diretamente da criptografia assimétrica, mas depende da existência de uma declaração em conformidade, emitida por uma entidade terceira de confiança;

[376] O n.º 12 do artigo 3.º do Regulamento define assinatura eletrónica qualificada como "*uma assinatura eletrónica avançada criada por um dispositivo qualificado de criação de assinaturas eletrónicas e que se baseie num certificado qualificado de assinatura eletrónica*". Do mesmo modo, na alínea a) do anexo I, estabelece-se que a emissão do certificado qualificado tem que ser feita por um prestador qualificado de serviços, requisito que não existia na alínea b) do anexo I da Diretiva.
[377] Utilizamos como referência a redação do artigo 26.º do Regulamento EIDAS.

iii) A assinatura deve ser criada com meios que o signatário, com um elevado nível de segurança, possa utilizar sob o seu controlo exclusivo. Trata-se do requisito da fiabilidade estrita, destinado a garantir que o meio de criação da assinatura eletrónica não possa ser utilizado por um terceiro que dele se apoderou indevidamente. Este meio de criação de assinatura, que é aquele do qual consta a chave privada, deve estar protegido para evitar acessos indevidos e ser suscetível de ser guardado pelo seu titular para que assim possa, com elevado nível de segurança, ser apenas utilizado pelo signatário;[378]

iv) Estar ligada aos dados que assina, de tal modo que seja detetável qualquer alteração posterior desses dados. Trata-se do requisito da integridade, que a metodologia das assinaturas digitais, mediante a utilização conjugada da criptografia assimétrica e simétrica permite.[379]

A assinatura eletrónica avançada assegura a efetividade da dupla vinculação dos dados em que ela se materializa. Por um lado ao documento que é assinado e, por outro, ao seu titular ou signatário. Essas duas vinculações permitem uma terceira, que é a vinculação do signatário ao documento assinado. Temos então, em termos sistemáticos, três conjuntos de dados, dois de base e pré-existentes, correspondendo o primeiro aos dados do documento que é autenticado pela assinatura, ou seja, os dígitos de zero e um que constituem o suporte informático desse documento. O segundo conjunto corresponde aos dados de criação da assinatura, que é o algoritmo que contém a chave privada do titular da assinatura, e que só o respetivo titular possui em seu poder. A intersecção de ambos estes conjuntos faz operar uma operação matemática realizada pelo sistema informático, utilizando ambos os conjuntos de dados. Dessa operação resulta a produção de um terceiro conjunto de dados, a que chamamos assinatura eletrónica.

A assinatura avançada é a base fundamental da assinatura qualificada e, em termos técnicos, elas em pouco se distinguem, uma vez que a assinatura qualificada tem

---

[378] Enquanto o Regulamento tem esta formulação, a Diretiva exigia que o meio de criação da assinatura se devia "*manter sob seu controlo exclusivo*", referindo-se ao signatário. A importância que este meio, ou dispositivo de criação da assinatura desempenha, levou o legislador do Regulamento a criar a figura dos dispositivos qualificados.

[379] A definição do conceito consta do n.º 2 do artigo 2.º da Diretiva: *"«Uma assinatura eletrónica que obedeça aos seguintes requisitos: a) Estar associada inequivocamente ao signatário; b) Permitir identificar o signatário; c) Ser criada com meios que o signatário pode manter sob seu controlo exclusivo; e d) Estar ligada aos dados a que diz respeito, de tal modo que qualquer alteração subsequente dos dados seja detectável*".

que ser sempre uma assinatura avançada, que cumpre requisitos adicionais de confiança. Esses requisitos necessários à qualificação consistem no controlo do seu cumprimento e da sua verificação, pelas entidades intervenientes no processo de criação das assinaturas eletrónicas, sendo que esse controlo é de caráter público e assegurado pelas entidades de supervisão, como veremos mais adiante, no ponto 1.2.3 do Capítulo II da Parte III.

Esses requisitos adicionais para que a assinatura eletrónica avançada possa ser classificada como qualificada são dois – o de que o certificado seja qualificado e o de que o dispositivo de criação da assinatura eletrónica seja também qualificado. Analisamos, de seguida, cada um desses requisitos, que o Regulamento EIDAS estabelece, na sequência da Diretiva.

3.5.3.1.2. Que o certificado seja qualificado

Um certificado é um atestado eletrónico, que conexiona um par de chaves a uma pessoa em concreto. Trata-se de uma declaração, passada por uma entidade de confiança, que confirma determinado par de chaves foi criado para uma pessoa em concreto. O certificado conexiona os dados da criação da assinatura eletrónica aos dados do signatário. E esse certificado deve ser sempre emitido, naturalmente, pelo prestador de serviços a quem foi solicitado, pelo signatário, que criasse o par de chaves que utiliza para assinar. Como do processo dessa fez parte a identificação do signatário requerente, só o prestador de serviços pode emitir esse certificado.

A Diretiva estabelecia que cumpriam os requisitos de um certificado qualificado, aqueles em que se verificasse um conjunto de pressupostos, enunciados no seu Anexo I. O Regulamento EIDAS mantém formulação idêntica, mas acrescenta que só podem emitir certificados qualificados os prestadores qualificados de serviços de confiança. Tudo porque este Regulamento faz depender a classificação de um prestador como qualificado, de um ato de reconhecimento prévio, emanado por uma entidade supervisora.

Assim, para que um certificado seja qualificado é necessário que se cumpram os seguintes pressupostos:

i) Pressupostos relativos à credibilidade do prestador de serviços de confiança eletrónica que emite o certificado. Estes certificados só podem ser emitidos por um prestador qualificado, nos termos do anexo I do

regulamento EIDAS. Esta categoria de prestadores de serviços foi criada pela primeira vez no Regulamento, sendo reconhecida, mediante controlo prévio, pelas entidades de supervisão, criadas pelos Estados Membros da UE. O regime de certificação prévia destina-se a conferir a máxima garantia de segurança, mediante um sistema de controlo público dessas garantias, que são minuciosamente elencadas no Anexo II do Regulamento, como analisamos mais adiante (Parte III, Capítulo II, ponto 1.6). Já no regime da Diretiva os certificados qualificados só podiam ser gerados por entidades que oferecessem maiores garantias de segurança, mas essas garantias dependiam do cumprimento de um conjunto de requisitos objetivos, constantes do Anexo II, sem necessidade de qualquer reconhecimento.[380] Trata-se de um conjunto de requisitos que foi crescendo à medida que as necessidades de segurança jurídica o exigiram, e que podemos agregar em três categorias:[381][382]

ii) Pressupostos relativos aos próprios certificados. Os certificados qualificados devem possuir os elementos que o Regulamento EIDAS elenca no Anexo I, que seguem de perto aqueles que eram enunciados no Anexo I da Diretiva, e que agrupamos em três categorias:

   a. Relativos ao signatário, nomeadamente a sua identificação, o pseudónimo, sendo o caso disso, a chave pública, os atributos do estatuto com que assina, designadamente se o faz em nome ou representação de outrem. A identificação do signatário é a função mais importante do certificado, porque através dele se liga um par de chaves a uma pessoa, mediante uma declaração de uma entidade terceira, que é merecedora de confiança pública, reforçada pelo seu estatuto de entidade qualificada;
   b. Relativos ao prestador de serviços de certificação que o emitiu, incluindo o nome e, sendo pessoa coletiva, o número de registo, a

[380] O número 10 do artigo 2.º da Diretiva inclui no próprio conceito de certificado qualificado a exigência de que seja emitido por um prestador de serviços que cumpre os requisitos do anexo II: *"«Certificado qualificado», um certificado que obedece aos requisitos constantes do anexo I e é fornecido por um prestador de serviços de certificação que cumpre os requisitos constantes do anexo II"*.

[381] Uma enunciação de todos os possíveis critérios de fiabilidade técnica a efetuar na avaliação da prova, ou então, no caso das assinaturas classificadas *a priori* como qualificadas, foi enunciado nos trabalhos preparatórios da LMAE, em "A/CN.9/630/Add.2", par. 12.

[382] Seguimos e sistematizamos o elenco se fatores de segurança das entidades certificadoras contidos no Guia para a Transposição da LMAE. "UNCITRAL Model Law ... 2001", par. 61.

assinatura eletrónica ou o selo eletrónico avançados deste e a indicação do país em que está estabelecido;[383]

c. Relativos ao certificado, em especial o código que o identifica, o período de validade, a menção de que é um certificado qualificado, bem como as restrições a que está sujeito quanto ao valor e tipo de documentos.

No regime da diretiva, a classificação dos certificados como qualificados não dependia do estatuto de quem os emitia. Eles seriam qualificados apenas quando cumprissem um conjunto de requisitos, mas a lei já distinguia entre os certificados qualificados e os restantes, que seriam aqueles que não cumpriam os requisitos que antes referimos ou que, cumprindo-os, não cumprissem os prestadores de serviços que os emitiam os requisitos que a Diretiva para eles estabelecia. À separação entre certificados qualificados e os restantes, veio o Regulamento EIDAS acrescentar a separação entre prestadores qualificados e não qualificados de serviços de confiança, reservando apenas para os primeiros o direito de emitirem certificados qualificados.[384]

Um certificado qualificado proporciona às partes uma garantia mais eficaz de que o par de chaves corresponde efetivamente à pessoa que identifica, não só pelas caraterísticas intrínsecas do certificado, como também pelas caraterísticas da entidade que o emitiu.

3.5.3.1.3. Que o dispositivo de criação de assinatura seja qualificado

Este requisito respeita ao instrumento tecnológico que o signatário utiliza para assinar documentos. Quando pretende assinar um documento, o signatário recorre a um

[383] O Regulamento EIDAS veio ainda acrescentar a necessidade de identificação do local onde está disponível, para verificação, o certificado que sustenta a assinatura eletrónica avançada do prestador qualificado, bem como o local onde os terceiros de confiança podem inquirir da validade do certificado qualificado. Estas exigências facilitam uma verificação automatizada, da validade do certificado e da identidade do prestador de serviços. Nos casos em que o prestador qualificado que emitiu o certificado é uma pessoa coletiva, o certificado deve conter o seu selo eletrónico avançado e já não, ao contrário do regime da Diretiva a sua assinatura eletrónica avançada. Esta alteração justifica-se pelo facto de o Regulamento EIDAS reservar as assinaturas eletrónicas para as pessoas singulares, criando de novo a figura dos selos eletrónicos para as pessoas coletivas, como instrumento de autenticação dos documentos por elas emitidos.

[384] A lei configura, assim, dois tipos de certificados, os qualificados e os não qualificados, sendo que a distinção fundamental reside nos efeitos jurídicos e na segurança que proporcionam às partes. Como refere Nadal, *"se estabelecem, el la ley de firma electrónica, dos categorías de certificados, un certificado ordinário ey un certificado reconocido"*. Nadal, A.G. (2009). Op. cit, pag. 209.

suporte do qual consta, nomeadamente a sua chave privada e dá ordem ao sistema informático para que aceda a esse suporte e utilize os dados com a chave privada para efetuar a operação de assinatura. Esse suporte contém o dispositivo eletrónico mediante o qual se consuma a assinatura e deve estar protegido contra o acesso de terceiros, podendo estar gravado num computador ou num suporte magnético, por exemplo, um cartão.

Para que a assinatura seja considerada como qualificada, esse dispositivo tem que ser sempre, também ele qualificado.[385] O Regulamento EIDAS estabelece os seguintes requisitos para que esses dispositivos possam ser qualificados (Anexo II):

i) A segurança acerca da confidencialidade dos dados necessários à criação de assinaturas. Trata-se de um requisito essencial para se garantir que mais ninguém, que não o signatário, possa ter acesso a esses dados. Para isso, o acesso a eles deve estar protegido por um mecanismo que impeça que terceiros possam aceder a esses dados;

ii) Os dados de assinatura, que são o par de chaves, só podem ter sido gerados uma vez, ou seja, não podem ter sido cancelados e depois gerados de novo. Esta irrepetibilidade é essencial para garantir que em caso algum a chave privada possa ser duplicada, pelo que, mesmo nos casos em que as chaves foram canceladas não podem voltar a ser reutilizadas;

iii) A chave privada não pode ser obtida a partir da chave pública, nem de outros elementos constantes dos documentos assinados, assim se garantindo a integridade da assinatura e dos dados da assinatura, contra falsificações;

iv) O signatário tem condições para guardar o segredo da chave privada e impedir que terceiros possam a ela aceder. Os prestadores de serviços de certificação não podem garantir que o signatário guardará com segurança o suporte magnético onde a chave privada está gravada, mas é indispensável que ela lhe seja fornecida num suporte que tenha condições para ser guardado, nomeadamente um cartão, um *chip* ou um disco

[385] O conceito de dispositivo qualificado é mais uma das inovações do Regulamento EIDAS, que estabelece os respetivos requisitos. Esses requisitos incluem todos os que constam da Diretiva, embora não se limitem a ele.

magnético que, por sua vez, esteja protegido, por exemplo com uma palavra-chave;

v) Os dispositivos não devem em caso algum modificar os dados do documento a assinar, respeitando a sua integridade;

vi) Os dispositivos devem proporcionar as condições para que o signatário possa visualizar o documento a assinar antes de aplicar a sua assinatura;

vii) Tanto a geração dos dados necessários para a criação da assinatura eletrónica, como a sua gestão, podem ser feitas por um prestador de serviços de confiança, desde que tenha o estatuto de qualificado. Este requisito foi acrescentado pelo Regulamento EIDAS e destina-se a permitir que estas entidades, e apenas elas, prestem o serviço de assinar documentos em nome de terceiros e por sua conta. Esta possibilidade aplica-se, nomeadamente nos casos em que seja necessário assinar, de forma automatizada, uma quantidade elevada de documentos, devendo, nesse caso, o procedimento automatizado ser efetuado por um prestador qualificado. Neste caso essas entidades podem duplicar os dados de criação da assinatura eletrónica, desde que a sua segurança esteja ao mesmo nível dos dados originais e se limite à necessidade de garantir a continuidade do serviço (n.º 4 do Anexo II do regulamento EIDAS).

3.5.4. Requisitos formais da assinatura eletrónica qualificada

Do que estudámos até aqui, acerca das assinaturas eletrónicas qualificadas, podemos concluir que essa classificação depende, fundamentalmente, dos prestadores de serviços de confiança que produzem os dispositivos de assinatura (pares de chaves, e aplicativo que produz o *hash* e o assina) e os certificados para que os signatários possam assinar documentos eletrónicos.

Uma assinatura eletrónica qualificada distingue-se das restantes, nomeadamente das avançadas, pelo facto de o dispositivo de assinatura e o certificado serem qualificados. E em ambos os casos, para que o sejam, é necessário que o prestador de serviços que os produziu seja qualificado. Por essa razão, o que melhor distingue as assinaturas eletrónicas qualificadas é a qualificação do prestador de serviços que produziu o dispositivo de assinatura e emitiu o certificado, para além do

cumprimento dos requisitos legais. É esse o requisito formal atualmente vigente na UE, depois da entrada em vigor do Regulamento EIDAS.

Para que os prestadores de serviços sejam classificados como qualificados é necessário que eles próprios cumpram um conjunto de requisitos que analisaremos mais adiante (Parte III, Capítulo II, ponto 1.6). Esses requisitos destinam-se a assegurar, por sua vez, a todos os agentes, um elevado nível de confiança nessas entidades e nos serviços que prestam. É essa confiança geral, que beneficia tanto os signatários como os terceiros com quem estabelecem relações jurídicas, como todos os interessados, que se pretende que seja fomentada e sedimentada pelo atribuição da classificação de qualificados aos prestadores de serviços de confiança que mereçam essa classificação, porque cumprem um conjunto de requisitos estabelecidos na lei.

Por essa razão, estas entidades desempenham um papel essencial para a confiança jurídica na utilização dos meios eletrónicos no tráfego jurídico.[386] E a garantia de cumprimento dos requisitos substanciais que acabámos de analisar cabe, fundamentalmente, aos prestadores de serviços confiança.

O Regulamento estabelece requisitos diferenciados em três domínios separados: i) para os certificados; ii) para os prestadores de serviços de certificação e iii) para os dispositivos de criação das assinaturas eletrónicas. A verificação de que esses requisitos estão cumpridos depende do procedimento formal, que consiste no reconhecimento, pelas entidades de supervisão, de que os prestadores de serviços de confiança são qualificados. Essa classificação é um ato formal e depende de reconhecimento prévio por aquelas entidades, que assenta em auditorias efetuadas pelos organismos de verificação de conformidade ou pelas próprias entidades de supervisão.

Fica assim garantida uma resposta definitiva e simples à questão mais importante, que tanto na Diretiva como na LMAE não estava resolvida, porque não existiam prestadores de serviços qualificados nem dispositivos qualificados, limitando-se em ambos os casos, a lei, a estabelecer os pressupostos substanciais para a equivalência. E não existindo um regime de reconhecimento formal, a verificação desses pressupostos tinha que ser apreciada pelas partes e em caso de litígio, a sua comprovação dependeria sempre de decisão do tribunal.

---

[386] Essa constatação é antiga e prosseguida desde muito cedo, nos trabalhos da UNCITRAL. "*The primary factors that determine whether a digital signature is secure include: (1) whether the certification authority has properly identified the holder; (2) whether the certification authority has properly authenticated the holder's public key; (3) whether the holder's private key has been compromised; and (4) whether the process is trustworthy (e.g., whether the public key algorithm and the key length used are appropriate)"*. A/CN.9/WG.IV/WP.73, par. 39.

Para que seja plena a equivalência das assinaturas eletrónicas às assinaturas manuscritas, e seja capaz de produzir os efeitos para que está orientado o seu regime jurídico, é necessário que seja avaliada a verificação dos pressupostos substanciais que que anteriormente analisámos, que já constavam genericamente da LMAE e da Diretiva, com exceção da exigência da qualificação dos prestadores de serviços e dos dispositivos de criação de assinatura. E para que essa avaliação produzisse efeitos plenos, idênticos aos da assinatura manuscrita era necessário que se cumprissem um conjunto de requisitos formais, nomeadamente:

i) Que a avaliação do cumprimento dos requisitos fosse efetuada por uma entidade competente e especializada;

ii) Que, de seguida, essa entidade declarasse verificados esses pressupostos e a segurança da assinatura;

iii) Que essa declaração fosse efetuada *a priori*, de modo que todos os interessados em possuir um instrumento de geração de assinatura eletrónica soubessem se ele cumpria, ou não, os requisitos da sua classificação como assinatura eletrónica qualificada;

iv) Que essa entidade fosse reconhecida pelas partes e por todos os terceiros que eventualmente viessem a ser interessados na assinatura, como possuindo a credibilidade suficiente para emitir a declaração de credenciação das entidades que emitem certificados dessa natureza.

No paradigma do papel a intervenção das entidades dotadas de fé pública é uma certificação formal de que se verificam um conjunto de pressupostos que qualificam a assinatura como reforçada na sua função de vincular um autor ou subscritor a um documento. Essa intervenção é contemporânea da própria assinatura, pelo que transporta para esse momento inicial um grau de certeza jurídica que sem essa intervenção só será possível de alcançar quando, em caso de litígio, uma entidade competente declare que esses pressupostos estavam verificados.

É essa segurança antecipada, apriorística, universal e contemporânea da assinatura, que é necessária para que a assinatura eletrónica possa ser plenamente equivalente à assinatura manual. Caso não exista esse nível de segurança, a assinatura eletrónica será sempre um tipo de assinatura que não oferece as garantias de confiança das assinaturas manuscritas. E essa segurança existirá se existir também um reconhecimento prévio de que uma determinada assinatura eletrónica cumpre os requisitos de ser classificada como qualificada, porque só assim as partes possuem a

segurança acerca da sua eficácia jurídica como instrumento de autenticação de documentos eletrónicos.

E este ato jurídico formal de reconhecimento de uma assinatura como qualificada é o elemento essencial à confiança jurídica, de tal modo que podemos dizer que se trata do núcleo essencial do direito da confiança eletrónica, e por essa razão justifica-se uma análise da evolução desse reconhecimento formal.

Ora a LMAE não prevê a existência de um reconhecimento prévio, formal, e com eficácia universal, nem a definição de uma entidade especializada que seja competente para a avaliação da verificação daqueles pressupostos. Essa lacuna limita a sua eficácia e não permite que se possa afirmar que dela resulta a plena equivalência entre a assinatura eletrónica e a assinatura manuscrita.

A LMAE representa um avanço substantivo e conceptual na formação do conceito e do regime da assinatura eletrónica qualificada, porque densificou os seus requisitos constitutivos. Mas essa previsão não garante, por si só, segurança às partes aos terceiros, de que a assinatura que cumpra esses requisitos se impõe por si mesma como uma entidade que seja capaz de conferir a segurança jurídica que resulta de ser capaz de resistir às contingências da apreciação de terceiros.

A enunciação dos pressupostos substanciais deixa sempre em aberto a questão de se determinar quem serão as entidades com competência para a avaliação da sua verificação, para além dos tribunais, em caso de litígio.[387]

E se esse poder intrínseco e independente é o que carateriza a assinatura manuscrita reconhecida por entidades dotadas de fé pública, então não existirá

[387] Essa questão era referida nos trabalhos da UNCITRAL como a principal causa de insegurança, havendo entendimentos no sentido de que a previsão dos requisitos substanciais não deveria existir, por poder ter o efeito perverso de aumentar a insegurança. Nos comentários ao projeto de UNCUECIC, a delegação do Canadá chamou a atenção para a dificuldade em se entender quem serão as entidades competentes para avaliar o cumprimento dos requisitos substanciais da assinatura qualificada. *"The question is who decides whether it is reliable: the person who chooses to rely on it, or someone outside the transaction in which it was used"*. Para os membros dessa delegação, a assinatura eletrónica é apenas um instrumento de autenticação, e a vinculação jurídica que dela resulta, funda-se apenas na vontade das partes e não em qualquer tecnologia que seja utilizada para assinar. *"The notion of signature does not include a reliability test. A signature is simply the distinctive mark that a person regularly uses to signify his or her intention. Traditionally, that notion does not include a reliability test"*. Em conclusão, refere o Canadá, a necessidade de prova de fiabilidade será um fator de insegurança, mais do que de confiança. *"In our view, this reliability test will do more harm than good. It does not create certainty, but rather reduces it, and thus runs counter to the purpose of the draft Convention"*. A/CN.9/578/Add.15, par.s 8, 7 e 4, respetivamente.

equivalência funcional de resultado para as assinaturas eletrónicas, enquanto estas não forem dotadas, na sua estrutura dogmática, de idêntico poder intrínseco e externo. [388]

Foi esse passo a LMAE não chegou a dar, o que não permitiu que através dela se alcançasse um nível de equivalência funcional pleno relativamente às assinaturas manuscritas.

Essa lacuna é relevante, assumida e induzida pelo facto de, na data em que foi aprovada a LMAE, ser já conhecida a tecnologia das assinaturas eletrónicas e existir já legislação que previa aquela equivalência funcional plena, nomeadamente a Diretiva 1999/93/CE e de países como Portugal, Alemanha e França. A razão para a lacuna da LMAE resulta do facto de o único tipo de assinatura capaz de garantir os pressupostos substanciais nela previstos para as assinaturas seguras, ser a da assinatura digital, e o legislador não pretender distinguir este tipo de tecnologia relativamente às demais tecnologias de assinatura eletrónica.

Foi o temor dessa segregação e a preocupação da salvaguarda do princípio da neutralidade tecnológica numa fase ainda inicial de emergência das assinaturas digitais, que terá estado na origem da opção de a LMAE não prever os requisitos formais de classificação das assinaturas eletrónicas como qualificadas.[389]

Mesmo assim a LMAE prevê, no n.º 1 do art.º 7.º, a possibilidade de os estados consignarem na sua legislação interna a certificação *a priori* da verificação desses pressupostos relativamente a determinados tipos de assinatura, nomeadamente quando as entidades terceiras que emitam os pares de chaves ou os certificados de assinatura eletrónica cumpram aqueles pressupostos.[390] A LMAE prevê a possibilidade de existência de mecanismos de certificação *a priori* de entidades terceiras que, cumprindo todos os requisitos estabelecidos no art.º 6.º da LMAE, ou seja, todos os pressupostos de fiabilidade, possam emitir certificados de assinatura eletrónica que possuem o valor

[388] A falta de intervenção destas entidades não permite que as partes possam adquirir a certeza da segurança na vinculação em razão da assinatura eletrónica, mesmo que cumpra os requisitos substanciais, até porque a própria contraparte pode vir a colocar em causa a verificação de todos os pressupostos legais respetivos. Nesse caso a existência de requisites substanciais sem serem acompanhados de uma previsão de reconhecimento formal a apriorístico, poderia vir a tornar-se uma espécie de "armadilha para incautos". *"A party could try to invalidate his own electronic signature as being insufficiently reliable, in order to invalidate a contract, where it is convenient to him. This would be to the detriment of the other party relying on the signor's signature. This provision then risks becoming a trap for the unwary or a loophole for the unscrupulous"*. "A/CN.9/578/Add.10", par. 14.

[389] Essa preocupação de não discriminação perpassa por vários textos dos trabalhos preparatórios da LMAE, nomeadamente o seguinte: *"Concern was expressed, however, that the draft article should not be interpreted in a manner that would either prescribe mandatory legal effects for the use of certain types of signature techniques, or would restrict the use of technology to those techniques determined to satisfy the reliability requirements of draft articles 6 and 7"*. "A/CN.9/465", par. 93.

[390] Artigo 7.º da LMAE. "A/CN.9/493", pág. 7.

reforçado da fiabilidade e por isso sejam classificadas como assinaturas eletrónicas qualificadas as assinaturas efetuadas mediante a aplicação das correspondentes chaves privadas.[391] Mas trata-se sempre de opções do legislador nacional e não de prescrições da LMAE, ficando compatibilizados, no seu contexto, os princípios da equivalência funcional, da neutralidade tecnológica e da equivalência internacional.

Esta opção de deixar aos estados a decisão de instituírem sistemas de acreditação, acrescida ao facto de se estabelecer o princípio da voluntariedade dessa acreditação, para os prestadores de serviços de certificação, era um instrumento importante para o acesso do maior número possível de agentes económicos a esse mercado.[392]

Por outro lado, entendia-se que não se devia fazer depender do Estado nem dos organismos públicos a qualificação dos prestadores de serviços de confiança, nem o reconhecimento das assinaturas eletrónicas. A LMAE contém uma marcada matriz liberal, deixando aos mercados e à liberdade contratual e de acesso à respetiva atividade, a criação dos instrumentos de confiança.

Mas essa opção tem como consequência a dificuldade dos agentes económicos em acederem a assinaturas eletrónicas com um nível de segurança jurídica mais elevado, dado que, não existindo certificação prévia, nunca se saberá, com certeza, se determinado instrumento de criação de assinaturas cumpre os requisitos de assinatura qualificada.[393] E tem também como consequência as dificuldades de utilização de assinaturas eletrónicas em operações negociais realizadas em jurisdições estrangeiras.

---

[391] Esta determinação apriorística das assinaturas eletrónicas qualificadas é um instrumento fundamental de segurança jurídica e de confiança dos agentes económicos, dado que essa segurança acerca da eficácia vinculativa das assinaturas eletrónicas, é antecipada também para o próprio momento em que ela é aplicada, sendo que, sem ela só depois de uma decisão judicial, em caso de litígio, essa segurança seria completa. Nesse sentido, *"what is required to facilitate the development of electronic commerce is certainty and predictability at the time when commercial parties make use of electronic signature techniques, not at the time when there is a dispute before a court"*. "A/CN.9/WG.IV/WP.88", par. 127.

[392] No preâmbulo da diretiva reconhecia-se de forma expressa esse propósito: *"Para estimular a oferta de serviços de certificação à escala comunitária através de redes abertas, os prestadores de serviços de certificação devem poder fazê-lo sem necessidade de autorização prévia"*. Ponto 10 da Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13/12/1999.

[393] Essa poderá ser uma das razões para que as assinaturas eletrónicas mais seguras não tivessem tido a expansão nos mercados que era expectável. Como um produto mais eficaz em termos de segurança jurídica, as assinaturas reconhecidas proporcionam maior proteção jurídica aos agentes económicos, mas a sua generalização depende sempre da existência mecanismos simples e expeditos de reconhecimento prévio. Só assim os agentes económicos poderão distinguir facilmente as assinaturas mais seguras das restantes. Caso contrário, será sempre mais económica e expedita a utilização das tradicionais palavras passe, apesar de não conferirem o mesmo nível de segurança das assinaturas avançadas ou reconhecidas.

O mecanismo das assinaturas eletrónicas qualificadas só funciona de forma eficiente se existirem entidades credenciadoras que verifiquem e declarem o cumprimento dos requisitos legais de fiabilidade pelos prestadores de serviços que emitem certificados de assinatura eletrónica. Trata-se, portanto, de entidades de confiança de segundo nível, que certificam outras entidades, de primeiro nível, que são aquelas que emitem os pares de chaves e os certificados de assinatura que são utilizados pelos signatários para assinar.

Essa certificação pressupõe a realização de auditorias destinadas a avaliar se essas entidades cumprem os requisitos de fiabilidade para que as assinaturas que vão ser aplicadas pelos dispositivos que entregam aos seus clientes possam ser classificadas de qualificadas. As entidades que efetuam essa avaliação poderão ser entidades públicas, mas poderão também ser entidades privadas.[394]

A configuração desse modelo de certificação de segundo nível, também designado de modelo de credenciação, pode obedecer a três tipos de opções:

i) O reconhecimento público obrigatório, sendo a credenciação uma função de natureza pública. A entidade credenciadora integra a administração pública e a atividade credenciadora é de caráter administrativo. Neste modelo as entidades certificadoras só adquirem o estatuto de prestadores qualificados mediante um ato administrativo que o declare e que tem natureza constitutiva. Trata-se de um modelo de credenciação prévia, que é importante para que os utilizadores desse tipo de assinaturas adquiram desde logo a confiança e certeza de que essas assinaturas possuem um efeito vinculativo que deriva diretamente da lei, e por isso essa certeza é imediata e não depende de terceiros que a venham a apreciar.[395];

ii) O reconhecimento privado obrigatório. As entidades credenciadoras podem ser privadas, mas a credenciação é obrigatória, só adquirindo o estatuto de prestadores qualificados aqueles que tenham obtido essa credenciação prévia;

---

[394] Como se refere no Guia de Transposição da LMAE, *"The second and narrower category is that created by the Model Law. It consists of methods of electronic signature that may be recognized by a State authority, a private accredited entity, or the parties themselves, as meeting the criteria of technical reliability set forth in the Model Law"*. "A/CN.9/WG.IV/WP.88", par. 76.

[395] *"The second option may be helpful to persons engaging in electronic commerce, who would know in advance of acting in reliance on a communication whether such action can be enforced"*. A/CN.9/WG.IV/WP.73, par. 44.

iii) O modelo da participação voluntária, mediante o qual os prestadores de serviços emitem certificados qualificados sem necessidade de se submeterem a qualquer processo de credenciação.

Os dois primeiros modelos conferem uma maior segurança e confiança aos agentes económico na utilização dos meios eletrónicos, por existir a favor dessa segurança uma declaração que faz presumir os efeitos vinculativos da assinatura, sem prejuízo, naturalmente, de que essa presunção possa ser elidida em tribunal, sendo certo, porém, que nesse caso se inverterão, normalmente, as regras do ónus da prova.[396]

O segundo modelo de certificação prévia, sem intervenção do Estado, permite a credenciação por entidades privadas, incluindo pelas entidades certificadoras que emitem, elas próprias, pares de chaves e certificados de assinaturas eletrónicas. Poderiam existir, neste caso, credenciações cruzadas entre entidades diversas.

No terceiro modelo não existe credenciação prévia. As entidades certificadoras que emitem pares de chaves e certificados exercem normalmente a sua atividade, sendo que a eventual avaliação do cumprimento dos requisitos de segurança será efetuada *a posteriori*, em caso de necessidade, de acordo com o princípio da liberdade do exercício de atividade económica. Incluem-se aqui, nomeadamente, as situações de litígio, em que a avaliação do cumprimento dos requisitos da assinatura eletrónica qualificada é efetuada pelos tribunais.

A Diretiva 1999/93/CE previa que os prestadores de serviços viessem a obter uma credenciação da qualidade dos serviços que prestam, nomeadamente no que respeita ao grau de confiança e de segurança dos seus procedimentos e produtos. Mas esse regime tinha três caraterísticas essenciais que afastavam a obrigatoriedade de intervenção dos poderes públicos:

i) Era um regime livre e voluntário, pelo que os agentes económicos só se submetiam a ele se assim o entendessem, podendo os Estados Membros adotá-lo ou não na sua legislação interna;

ii) A credenciação podia ser uma atividade privada ou pública, dependendo do regime que os Estados Membros pretendessem adotar, mas a diretiva manifestava preferência pelo seu carácter privado;

iii) A diretiva não obrigava a qualquer tipo de procedimento de credenciação prévia.

---

396 *"However, the presumption of accuracy may be rebutted by showing that a certificate issued by such an accredited certification authority is, in fact, not accurate or reliable"*. A/CN.9/WG.IV/WP.73, par. 44.

A diretiva adotava o conceito acreditação facultativa, mediante o qual os prestadores de serviços se submetiam a um procedimento de avaliação para avaliação do cumprimento dos requisitos. Dessa avaliação podia resultar a sua classificação como prestadores qualificados de certificação.[397]

Para isso previa-se a possibilidade de os prestadores de serviços recorrerem a *"sistemas voluntários de acreditação"* (n.º 2 do art.º 3.º), tendo em vista, dessa forma, incrementar a confiança dos agentes económicos nas assinaturas eletrónicas. Estes sistemas podiam ser criados pela legislação interna dos Estados Membros, mediante a criação de sistemas de *"supervisão dos prestadores de serviços de certificação estabelecidos no seu território"* que emitiam certificados reconhecidos (n.º 3 do art.º 3.º). Esta norma ia um pouco mais longe do que a mera previsão dessa possibilidade, uma vez que o que ela estabelecia era que os Estados Membros assegurariam a instituição de mecanismos de controlo e de supervisão desses prestadores de serviços.

A diretiva estabelecia também um regime de controlo, mediante organismos de acreditação, que podiam ser públicos ou privados, com a incumbência de controlo dos prestadores de serviços que emitissem certificados qualificados de assinatura eletrónica (n.º 4 do art.º 3.º).

O carácter facultativo dessa acreditação não impunha que ela fosse prévia à emissão dos certificados. A diretiva admitia como possível que os prestadores de serviços que não possuíssem acreditação, pudessem emitir certificados qualificados, desde que cumprissem os requisitos objetivos nela estabelecidos. Esta opção assentava no princípio da não intervenção do Estado nas atividades de prestação de serviços de certificação, num princípio de voluntariedade da acreditação dos prestadores de serviços,[398] e na preponderância da necessidade de se expandir o mercado e de facilitar o acesso à atividade de certificação.

A lei portuguesa da assinatura eletrónica de 1999 consagra também o regime de credenciação voluntária, mas a emissão de certificados qualificados passou a ser exclusiva das entidades que se registassem voluntariamente na autoridade credenciadora. (art.º 9.º e 40.º do Decreto-Lei n.º 290-D/99, de 2 de Agosto, com as

[397] A natureza desta acreditação está definida no n.º 13 do artigo 2.º da Diretiva, nos seguintes termos: "*«Acreditação facultativa», qualquer autorização que estabeleça direitos e obrigações específicos para a prestação de serviços de certificação, concedida, a pedido do prestador, pela entidade pública ou privada encarregada da elaboração desses direitos e obrigações e do controlo do seu cumprimento, quando o prestador de serviços de certificação não possa exercer os direitos decorrentes da autorização antes de ser informado da decisão daquela entidade"*.

[398] Como se refere no ponto 11 do preâmbulo da diretiva: *"os prestadores de serviços de certificação devem ter a liberdade de aderir a estes regimes de acreditação e deles beneficiar"*.

alterações efetuadas pelo Decreto-Lei n.º 88/2009, de 9/4). No que respeita à emissão de certificados qualificados, podiam ser emitidos por entidades prestadoras de serviços de certificação que cumprissem um dos seguintes pressupostos:

i) Lhes tivesse sido concedida credenciação a seu pedido, pela entidade competente.[399] Esta credenciação só era reconhecida nos casos em que a entidade cumprisse todos os requisitos substanciais;

ii) Se tivessem registado previamente na autoridade credenciadora, como emitentes de certificados qualificados, sendo pressuposto desse registo que cumprissem os requisitos substanciais, nos termos do n.º 2 do art.º 9.º.

Em ambos os casos antes referidos, a lei atribuía à autoridade credenciadora poderes de autoridade pública, nomeadamente de controlo, auditoria e inspeção a todas as entidades certificadoras (art.º 32.º). A autoridade credenciadora tinha também poderes sancionatórios para aplicação das coimas por incumprimento do regime jurídico das assinaturas eletrónicas (art.º 36.º-C).

O regime da lei espanhola de 2003 assentava também no princípio da liberdade de acesso, mas consagrava a obrigatoriedade de registo a todos os prestadores de serviços de certificação.[400] Sobre todas essas entidades é estabelecido um poder de auditoria e inspeção à administração pública.[401]

O Regulamento EIDAS veio criar um regime de reconhecimento público prévio, dos prestadores qualificados de serviços de confiança, como anteriormente referimos. Este regime revoga o da Diretiva, pelo que atualmente, e como analisamos mais em pormenor mais adiante (Parte III, Capítulo II, ponto 1.6), as assinaturas eletrónicas qualificadas são apenas aquelas cujos dispositivos são produzidos por prestadores qualificados de serviços de confiança e cujos dispositivos e certificados são também qualificados. E a classificação dos prestadores e dos serviços como qualificados depende do reconhecimento das entidades de supervisão, sendo esse reconhecimento

[399] A entidade credenciadora é a Autoridade Nacional de Segurança, nos termos do artigo 40.º do DL n.º 290-D/99, de 2/8.

[400] O artigo 5.º da "*Ley 59/2003, de 19 de diciembre, de firma Electrónica*", enuncia o princípio, nos seguintes termos: *"1. La prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre competencia. No podrán establecerse restricciones para los servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo"*.

[401] O poder de supervisão está consignado no n.º 1 do artigo 29.º da mesma lei, que tem a seguinte redação: *"El Ministerio de Ciencia y Tecnología controlará el cumplimiento por los prestadores de servicios de certificación que expidan al público certificados eletrónicos de las obligaciones establecidas en esta ley y en sus disposiciones de desarrollo. Asimismo, supervisará el funcionamiento del sistema y de los organismos de certificación de dispositivos seguros de creación de firma eletrónica."*.

prévio e dependente de uma avaliação pelas próprias entidades de supervisão ou por entidades de avaliação de conformidade. Os art.ºs 20.º e 21.º do Regulamento estabelecem um regime de credenciação prévia para os prestadores de serviços que garante que a emissão de certificados qualificados só poderá ocorrer após um ato de reconhecimento constitutivo da entidade supervisora.[402]

Ao optar pelo regime do reconhecimento prévio e por uma entidade pública, o Regulamento EIDAS tem por objetivo promover a máxima confiança na utilização dos meios eletrónicos no tráfego jurídico, disponibilizando ao comércio jurídico uma categoria de assinaturas eletrónicas que asseguram aos agentes a mais elevada segurança acerca do seu efeito vinculativo.

Por outro lado, é nesse nível mais elevado de confiança que o legislador europeu institui um regime imperativo de reconhecimento mútuo dentro de todo o espaço da UE, garantindo que aquela eficácia jurídica opera em todos os Estados Membros.

Os agentes económicos passaram também a poder constatar facilmente se a assinatura que utilizam ou aquelas que constam dos documentos que recebem, são qualificadas, dado que essa menção consta dos próprios certificados. Ao mesmo tempo esse conhecimento é reforçado pela instituição, feita pelo art.º 23.º do Regulamento, da marca de confiança "UE", que pode passar a ser utilizada pelos prestadores qualificados.

Analisamos, no ponto 5.8 do Capítulo V da Parte III, os efeitos da entrada em vigor do Regulamento EIDAS no que respeita aos prestadores qualificados de serviços de confiança.

3.6. O conceito de assinatura na doutrina

O conceito de assinatura também evoluiu na doutrina. Rivero entende que a função da assinatura eletrónica é de autenticação, seguindo o conceito amplo da diretiva

[402] Nos termos do n.º 2 do art.º 21.º, *"A entidade supervisora verifica"* relativamente a cada prestador de serviços, se *"os serviços de confiança por ele prestados cumprem os requisitos estabelecidos no presente regulamento…"*. Em caso afirmativo *"a entidade supervisora atribui o estatuto de qualificado ao prestador de serviços de confiança e aos serviços de confiança por ele prestados"*.

europeia de 1999, mas associa essa autenticação ao conceito de autoria.[403] Esta associação é claramente induzida pela necessidade de fazer corresponder os efeitos da assinatura eletrónica aos da assinatura manuscrita, assumindo essa vinculação da primeira à segunda, mas ambos os conceitos são diferentes, uma vez que a autoria é mais restrita que a autenticação.[404]

Do mesmo modo, Martínez Nadal considera que a assinatura eletrónica é um instrumento utilizado por uma pessoa para se vincular ou autenticar um documento, considerando também que a assinatura eletrónica se destina a produzir os mesmos efeitos da assinatura manuscrita.[405]

Esta prevalência da autoria é também vincada por Ortega Díaz, que admite que essa função é também de identificar a pessoa que a usa e de assumir o ato que assina, mas quando depois especifica quais são aquelas que designa por duas finalidades da assinatura eletrónica, enuncia que afinal é apenas de *"assumir a autoria"* de um documento e *"adquirir os direitos e as obrigações que deste resultam"*,[406] não referindo aquela função de identificação do seu titular.

Alcolea Cantos releva a função de autenticação, dizendo que ela se confunde com a assinatura eletrónica, sendo o seu maior relevo nas transações eletrónicas o de permitir imputar as declarações negociais aos respetivos autores.[407]

No mesmo sentido Zafra Jiménez associa a assinatura eletrónica à autenticação das mensagens eletrónicas, ou seja, a documentos transmitidos. Partindo da definição de sociedade da informação constante da Diretiva 2000/31/CE, o Autor defende que a assinatura eletrónica é o instrumento indispensável para que um recetor qualquer possa,

---

[403] Rivero, D.C. (2006). Op. Cit., página 17, que enuncia: *"entendemos que todas as assinaturas reúnem estes requisitos: possuírem formato electrónico e autenticarem um documento. Qualquer instrumento que reúna estas duas qualidades será uma assinatura digital"*.

[404] O Autor refere que a palavra "*assinatura*" como parte do conceito de "*assinatura digital*" fundamenta a associação desta a um documento, dado que a assinatura manual só se pode conceber como a assinatura de documentos. *"O emprego do termo 'assinatura como parte da denominação de 'assinatura digital', justifica-se porque a autenticação de dados é a principal finalidade da assinatura manuscrita".* Díaz, J.J.O. Op. Cit., pág. 17.

[405] Depois de analisar as definições da legislação, Martinez Nadal enuncia a sua definição da seguinte forma: *"uma assinatura digital seria simplesmente qualquer método ou símbolo, baseado em meios eletrónicos, utilizado ou adoptado por uma pessoa com a intenção de se vincular ou autenticar um documento, cumprindo todas ou algumas das funções características de uma assinatura manuscrita".* Nadal, A.G. (2001). *La Ley de Firma Electrónica*. 2.ª edição, Civitas Ediciones, SL. Madrid, pág. 48.

[406] Díaz, J.J.O. Op. Cit., pág. 36.

[407] O autor afirma que,*"a assinatura eletrónica não é nada mais do que um sistema de autenticação de declarações de vontade entre sujeitos, entre os quais não existe relação física no momento em que essas declarações têm que produzir os seus efeitos jurídicos".* Cantos, J.M.A. (2004). El Control de Calidad de los Servicios de Certificación y de los Productos de Firma Electrónica. Em: Ministerio de Economia. Administración Electrónica y Procedimiento Administrativo. Real Casa de la Moneda. Madrid, pág. 285.

a partir do seu computador, confirmar que um determinado documento por si recebido tem uma determinada origem, com segurança.[408]

Estas construções doutrinárias estavam ainda próximas da necessidade de vincular subjetivamente todo e qualquer tipo de mensagens eletrónicas, tendo como preocupação a solução do problema da falta de conhecimento pessoal e da falta de presença física nas relações estabelecidas à distância, como são as de carácter eletrónico. É por essa razão que os atributos da autenticação e da autoria são a base das conceções jurídicas da assinatura eletrónica. Mas essa preocupação limita claramente o âmbito do conceito, porque não releva as outras duas funções fundamentais da assinatura, que são a identificação do signatário e a integridade do documento. E existiam razões para que assim fosse. Na verdade, no contexto histórico em que nasceu o conceito de assinatura eletrónica, a preocupação principal era a de conferir relevo jurídico às comunicações eletrónicas estabelecidas entre máquinas, sempre sem a presença física das partes, nas quais não funcionavam os mecanismos da identificação e da autenticação que são possíveis nas relações estabelecidas mediante aquela presença física. Sendo essa a preocupação principal, não assumia papel de relevo o conceito de documento, porque o objeto da necessidade de atribuição de relevo jurídico não eram apenas os documentos eletrónicos, mas todos os dados com potencial relevância jurídica, comunicados por meios eletrónicos.

Do mesmo modo, a preocupação de garantir a eficácia jurídica das declarações negociais comunicadas por via eletrónica, deixava para segundo plano o conceito de documento eletrónico e conferia prioridade à necessidade de garantir a determinação da autoria de todo e qualquer tipo de comunicações eletrónicas. Ficavam, porém, de fora nas conceções destes autores, a identificação e a integridade, mas outros havia que lhes conferiam relevo.

José Maria Perales distingue apenas as duas funções de identificação e de vinculação, não se referindo às restantes.[409] O Autor enfatiza a importância da função de

---

[408] O autor afirma que a assinatura eletrónica é o modo de *"o recetor de uma mensagem verificar a autenticidade da origem da informação",* acrescentando que *"a assinatura digital não é apenas um conjunto de dados em forma digital. Como meio de autenticação, a funcionalidade típica dos mecanismos de assinatura digital é, precisamente, ser um instrumento capaz de permitir uma comprovação da procedência e da integridade das mensagens intercambiadas".* Jiménez, A.Z. (2004). El Régimen de Responsabilidad en el Uso de la Firma Electrónica. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid. pág.s 297 e 298.

[409] O Autor afirma que *"As funções tradicionais duma assinatura são: identificar uma pessoa, proporcionar certeza sobre a sua participação pessoal no acto da assinatura e vincular essa pessoa ao conteúdo do documento".* Perales, J.M.A.M. (2005), Op.cit, pág. 95.

identificação da assinatura eletrónica, nas próprias caraterísticas tecnológicas em que assenta. Na verdade a tecnologia é impessoal por essência, pelo que a identificação do titular da assinatura eletrónica é uma função essencial desta e uma caraterística intrínseca.[410]

No que respeita à identificação do emitente de uma comunicação eletrónica, atualmente existe uma clara assunção de que ela é essencial à assinatura eletrónica, porque não pode existir vinculação sem o conhecimento da identidade do emitente sem se conhecer a sua identificação. Mas essa autonomização da função de identificação do autor, que é própria da assinatura eletrónica, não nos pode fazer esquecer uma outra, que é a da mera identificação que é necessária para que, nos casos em que não exista troca de documentos, uma parte possa aceder, por exemplo, a um serviço disponível numa rede eletrónica.

Um dos primeiros autores que distinguiu essas duas dimensões do conceito de identificação foi Linares Gil, separando-as e designando-as como funções de *"autenticação"* e de *"acreditação"* da assinatura eletrónica. O Autor refere que a primeira se aplica aos documentos e à sua associação inequívoca a uma pessoa e a segunda consiste na identificação da própria pessoa perante um sistema ou perante um outro utilizador que está em rede a interagir com ele. Defende também que esta dupla função da assinatura eletrónica a distingue da assinatura manuscrita, considerando também que não tem que existir identidade entre ambos os tipos de assinatura.[411] Esta perceção da diferença entre a assinatura eletrónica e a identificação eletrónica autónoma, separada dos documentos eletrónicos e que é própria para a autenticação de pessoas que operam por meios eletrónico num contexto de relações com relevância

[410] O autor exprime essa caraterística do seguinte modo: *"As assinaturas manuais têm uma associação intrínseca com uma pessoa física determinada, por serem feitas com o punho e a letra do assinante, sendo sempre algo de muito característico e intrínseco de cada pessoa. Mas um jogo de chaves usado para criar uma assinatura digital não tem uma associação intrínseca com ninguém: um byte informático é exatamente igual a outro byte e o par de chaves (pública e privada) não são mais que um par de números (ou algoritmos), que não são associados a ninguém. Por isso são necessários outros instrumentos, como as terceiras partes de confiança (as autoridades de certificação) e os certificados"*, acrescentando mais à frente que *"o certificado é, afinal, uma espécie de bilhete de identidade digital, que funciona como um identificador único dentro da rede"*. Perales, J.M.A.M. (2005), Op. Cit., pág.s 107, 108 e 109.

[411] Esta distinção será muito importante para a futura evolução dos conceitos de identificação eletrónica e de assinatura eletrónica. Como referia o Autor, "*Ainda que acreditação e autenticação não sejam conceitos sinónimos, nas relações digitais são realidades muito associadas, sendo inclusivamente suportados nas mesmas tecnologias. Não acontece o mesmo com o suporte papel, onde a acreditação pode fazer-se, por exemplo, com um documento de identidade ou com testemunhas, enquanto que a autenticação se realiza, normalmente com a assinatura manuscrita"*. Gil, M.I.L. (2004); Op. Cit., pág. 458.

jurídica que não estão suportadas por documentos, é manifestada pelo Autor de forma praticamente pioneira.

E essa distinção marcava uma importante diferença entre a assinatura eletrónica e a assinatura manuscrita. Num contexto em que era necessário autenticar todas as transações eletrónica, mesmo as que não eram suportadas em documentos, o único instrumento que então existia para se alcançar esse resultado, era o da assinatura eletrónica. Criava-se assim uma diferença substancial entre o conceito de assinatura manuscrita, que era um conceito próprio dos documentos, e o de assinatura eletrónica, que se aplicava tanto aos documentos como às comunicações e transações eletrónicas não documentadas.

A autonomização da assinatura eletrónica relativamente à assinatura manual tem como uma das suas causas esta importância crescente da função de identificação da assinatura eletrónica e é enfatizada por Calvinho. Com esse fundamento, associado a outros de carácter tecnológico, este Autor defende a completa autonomização da assinatura eletrónica relativamente à assinatura manuscrita. Embora a definição da função daquela coincidisse com a desta no que respeita à autoria e subscrição dos documentos eletrónicos, a verdade é que a sua natureza seria distinta[412].

Também Lucena López defende essa conceção abrangente, considerando que a principal função da assinatura eletrónica é de "*autentificação*" ou "*autenticação*", segundo o próprio, considerando os dois conceitos equivalentes.[413] O Autor atribui ao conceito de autenticação um sentido amplo, considerando que abrange tanto a identificação como a certificação da autoria.[414]

Das conceções enunciadas é comum a falta de referência à função da integridade dos documentos, porque a preocupação se centrava, como referimos, na atribuição das transações eletrónicas aos respetivos emitentes, ou seja, na função de vinculação ou de autenticação. Alguns autores entendiam mesmo que a autenticação dos

---

[412] Com afirma de forma expressiva Calviño, *"definitivamente o que está subjacente a toda [esta polémica] é uma indevida assimilação da assinatura digital à assinatura manuscrita, iludindo uma adequada configuração da mesma como instituição jurídica peculiar".* E mais diante, *"algumas teorias partem de um preconceito equivocado de assimilação ou comparação da assinatura digital (mecanismo) e caligrafia (realidade) quando, na verdade, não têm similitude, porque partem de conceitos jurídicos e realidades distintas"*. Calviño, R.C. Op. Cit., pág.s 27 e 47, respetivamente.

[413] López, Manuel José Lucena; Op. cit.; pág. 231.

[414] Com afirma expressamente, *"Denominaremos em geral autentificação (ou autenticação) às operações que consistem em verificar, tanto a identidade do nosso interlocutor, como a integridade das mensagens que dele recebemos"*. López, M.J.L. (2009). Op. cit.; pág. 231 e 178.

dados não integra o conceito de assinatura.[415] Só mais tarde esta função foi associada à assinatura eletrónica, existindo até autores que defendiam que ela não é essencial à sua definição.[416]

Como concluiremos quando analisarmos as funções da assinatura eletrónica, já de seguida, no Capítulo III, ela é sempre um instrumento de identificação e de autenticação de documentos, em simultâneo, com base nos dados que constituem os documentos e também a própria assinatura, sendo eles os elementos essenciais à vinculação. A eficácia vinculativa pode variar em função de vários fatores, relevando em especial o da garantia de integridade dos dados. Alguns tipos de assinatura são menos eficazes nessa garantia, mas nem por isso deixam de se poder incluir no conceito de assinatura,

Um dos princípios importantes que consta das diversas legislações é o da identidade funcional entre a assinatura eletrónica e a assinatura manuscrita. Essa correspondência destina-se a conferir eficácia jurídica à assinatura eletrónica e a evitar que seja discriminada negativamente em relação à assinatura manual. Entendia-se que isso não tinha que significar que a assinatura eletrónica tivesse apenas a mesma função que cumpre a assinatura manual, nem a mesma estrutura.[417]

Mas o conceito de assinatura formou-se no paradigma do papel e é um conceito próprio dos documentos. Mas uma coisa são os documentos como suportes de facto jurídicos e outra coisa são as reações jurídicas, sendo que estas, só têm que ser documentada em algumas situações que podemos classificar como pontuais. E isso não

---

[415] Como afirma Mariliana Carrillo, a assinatura eletrónica é *"cualquier método o símbolo basado em médios electrónicos utilizado o adoptado por una parte com la intención de vincularse o autenticar un documento"*, acrescentando mais adiante que esse método inclui desde os mais sofisticados até aos mais simples, *"de muy escassa seguridade"*. Carrillo, M.C., (2012). *El Pago Electrónico en Internet: Estructura Operativa e Régimen Jurídico*. Thomson Reuters, Aranzadi. Pamplona, pag. 213.

[416] Assim, Gutiérrez, depois de vincar a função mais radical de identificação *("La firma es el instrumento jurídico que permite acreditar la identidade"*), acrescenta que *"debemos entender que la definición de firma electrónica (básica) se refere a aquellos sistemas de firma que son capaces de identificar al firmante de los datos pero que no puden garantizar la autenticación de los datos signados"*. Essa definição básica excluiria aqueles tipos de assinatura que permitem *"detectar cualquier cambio ulterior de los datos firmados"*. As assinaturas que garantiriam essas funções seriam já de outros tipos, nomeadamente as avançadas. Gutiérrez, R.M. (2009). *Administración Pública Electrónica*. Civitas, Thomson Reuters, Editorial Aranzadi. Pamplona. pag. 565 e 569, respetivamente.

[417] Continuando a citar Linares Gil, *"Mesmo que se afirme a regra da identidade funcional entre as assinaturas manuscrita e digital, existe uma importante diferença no tráfego jurídico. Enquanto a assinatura manuscrita é habitualmente acompanhada de algum mecanismo de identificação (...) a assinatura digital está dispensada desse requisito, precisamente porque se vincula de per se ao signatário".* Gil, M.I.L. (2004). Op. Cit., pág.s 464, 465. O mesmo autor repete esta formulação teórica, praticamente nos mesmos termos na obra "Modificaciónes del Regimen Jurídico Administrativo del Empleo Massivo de Nuevas Tecnologías. En Particular el caso de la Agencia Estatal de Administración Tributaria", in Derecho de Internet - La Ley de Servícios de la Sociedad de la Información y de Comercio Electrónico", Thomson, Aranzadi, Navarra 2003, pág. 738.

muda quando as relações jurídicas são estabelecidas mediante meios eletrónicos. Não é o suporte eletrónico que obriga a que todas as relações jurídicas sejam documentadas. Podem sê-lo ou não, de acordo com a vontade das partes ou as determinações legais. E se o conceito de assinatura é próprio dos documentos, essa asserção tanto se aplica nos casos em que os documentos são suportados em papel como em meios eletrónicos, pelo que a assinatura se deve referir, em ambos os casos, ao instrumento de autenticação dos documentos e de identificação do respetivo autor ou subscritor. É certo que ficam fora do conceito de assinatura eletrónica as transações efetuadas por meios eletrónicos que não são suportadas em documentos, mas para essas situações seria criada na legislação o conceito de identificação eletrónica, em especial, no Regulamento EIDAS.

As definições de assinatura da doutrina, que analisámos, raramente são completas, centrando-se umas na função de autenticação, outras na de identificação, e outras ainda na função de integridade, mas são escassos os casos em que se apresentam estas funções em conjunto.[418]

Definições mais próximas da sua abrangência são-nos dadas por outros autores. Davara Rodriguez assinala-lhe as funções de identificação, de autenticação e de garantia da integridade dos documentos.[419]

Em Portugal desenvolveu-se uma relevante produção doutrinária no período subsequente à publicação do Decreto-Lei n.º 290-D/99, de 2/8. Assim, Manuel Lopes Rocha releva o caráter percursos da lei portuguesa, referindo que ela assenta, porém, na

---

[418] Galindo Gil referencia apenas as funções de identificação e de autenticação. O Autor distingue claramente ambas as funções, mas a definição que propõe não é completa. *"a assinatura digital tem por finalidade essencial identificar uma pessoa, proporcionar o maior nível de certeza possível quanto à sua participação no acto da assinatura, e vincular essa pessoa ao conteúdo da mensagem assinada …".* Gil, P.G. (2004). La Representación por Medios Electrónicos. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid., pág. 493.

[419] Como afirma o Autor, *"A assinatura digital serve, portanto, para identificar o signatário"*, acrescentando, mais adiante, a importância dessa identificação, que, como vimos, é cada vez maior nas operações eletrónicas: "*A assinatura digital garante que é uma pessoa concreta e determinada quem está a intervir numa determinada transacção"*, enunciando mais à frente a função de autenticação dos documentos que antes era predominante na doutrina e em algumas legislações: *"assim como que o documento está íntegro e corresponde ao conteúdo original, sem ter sido transformado na sua transmissão".* Em forma de conclusão, Davara Rodriguez acrescenta, de seguida, que *"a assinatura digital tem como função básica garantir que nas relações jurídicas estabelecidas por meios eletrónicos, é uma pessoa concreta a que intervém em determinada transacção, assim como que o documento está íntegro e corresponde ao seu conteúdo origina, sem ter sido transformado na transmissão".* Rodriguez, M.A.D. (2005). *La Seguridad en las Transacciones electrónicas: La Firma Electrónica. Universidad Pontificia Comillas. Madrid*., pág. 30. Em forma de conclusão, Davara Rodriguez acrescenta, de seguida, que *"a assinatura digital tem como função básica garantir que nas relações jurídicas estabelecidas por meios eletrónicos, é uma pessoa concreta a que intervém em determinada transacção, assim como que o documento está íntegro e corresponde ao seu conteúdo origina, sem ter sido transformado na transmissão"*

assinatura digital, o que poderia colocar em causa o princípio da neutralidade tecnológica.[420]

Do mesmo modo, Miguel Pupo Correia releva todas as funções de autenticidade e de integridade, e embora não mencione expressamente a função de identificação, que lhe é essencial, ela está pressuposta no texto quando menciona que a autenticidade consiste na "*correspondência entre o autor aparente e o autor real do documento*". Acrescenta, porém, a função de confidencialidade, que não é essencial à assinatura.[421] O Autor identifica essas funções em face dos "*três tipos fundamentais de problemas*" que assinala à "*segurança*" dos documentos eletrónicos, e que seriam a dificuldade de determinação da autenticidade, da integridade e da confidencialidade. Nessa linha defende que as assinaturas avançadas são aquelas que melhor garantem a efetividade aquelas funções, considerando "*formalista*" a separação entre estas e as assinaturas eletrónicas qualificadas, bem como a exigência de dispositivos seguros.[422] Mas reconhece que a função da certificação é um pressuposto essencial para que os documentos eletrónicos possam ter valor probatório.

Pacheco de Andrade define a assinatura como método de "*identificação de uma pessoa*" e de "*indicação de aprovação de um determinado conteúdo*".[423] Afonso Patrão adota uma conceção restrita de assinatura eletrónica, excluindo do conceito as assinaturas por mera menção do nome do autor, bem como as assinaturas digitalizadas,

---

[420] Relativamente ao caráter pioneiro da lei portuguesa refere o Autor: "*Portugal, o país sempre habituado à cauda do pelotão europeu, tornava-se o terceiro país desta área do Globo a adoptar uma lei que representa aquilo a que alguém chamou de "chave" do comércio electrónico*". E no que respeita à neutralidade: "*é óbvia a continuação da situação de favorecimento ou de privilégio de que gozam as assinaturas digitais*". Rocha, M. L.; A assinatura electrónica Uma Via Portuguesa "Original"? http://www.asf.com.pt/winlib/cgi/winlibimg.exe?key=&doc=10038&img=961 (última consulta efetuada em 30/6/2017).

[421] Correia, M. P. (2000). As certificações digitais: factura e assinatura. Privacidade e comércio electrónico. Comissão Nacional de Protecção de Dados, pág. 124. Do mesmo modo não é completa a sistematização final que efetua, de seguida, mencionando que a assinatura eletrónica cumpre"*quatro funções: prova a identidade do autor, não pode ser falsificada, não pode ser copiada, e torna o documento inalterável*". (Ibidem, pág. 129. Ora a verdade é que a função da prova da identidade e certa, bem como da inalterabilidade, mas não se pode dizer que não pode ser falsificada nem copiada, porque essa possibilidade sempre existirá, cabendo à lei reduzir, em maior ou menor de eficácia, esses perigos.

[422] Correia, M. P. (1999). *Assinatura Electrónica e Certificaçao Digital*. http://www.apdi.pt/wp-content/uploads/2016/10/8-ARTIGO_ASSINATURA_ELETRONICA_CERTIFICACAO_DIGITAL.pdf (última consulta efetuada em 30/6/2017), pág. 19: O Autor refere que e lei portuguesa se limitou a fazer uma "*transposição formalista dos conceitos*", referindo, em especial que, relativamente aos dispositivos seguros de criação de assinaturas eletrónicas se pretendeu apenas "*conceptualizar com sabor tecnológico a existência ou não de cautelas quanto à guarda da chave privada*".

[423] Andrade, F. C. P. (2004). A Assinatura Dinâmica Face ao Regime Jurídico das Assinaturas Electrónicas. *Scientia Jurídica, Tomo LIII, n.º 299*, pág. 347

invocando que delas não resulta a prova da autoria.[424] No entanto, os efeitos probatórios das assinaturas eletrónicas variam em função da sua natureza, e não são eles que definem a sua natureza. Assinatura eletrónica é qualquer indicador de identificação, autenticação e integridade de um suporte de informação, sendo a sua eficácia probatória posterior ao reconhecimento da sua natureza e não um elemento definidor da sua essência. Relevam também as obras de Benjamim Rodrigues em matéria probatória dos suportes eletrónicos em processo penal, de Vasco Pereira da Silva e de Pedro Gonçalves no procedimento administrativo, bem como de Garcia Marques e de Francisca Almeida D'Eça, e ainda de Afonso Patrão, que analisamos nos locais próprios.

Relevamos ainda as obras de Luis de Sousa e de David Ramalho sobre o valor probatório dos documentos eletrónicos, e de Gonçalves Sampaio, que também analisaremos nos locais próprios, em especial no ponto 4 do Capítulo III da Parte III.

3.7. O conceito de assinatura na legislação

Também na legislação o conceito de assinatura evoluiu de forma significativa, em sentido idêntico ao da evolução da doutrina. A autenticação de dados em suporte eletrónico era inicialmente a função central da assinatura eletrónica, considerando-se que dados não são documentos formais nem informação, mas suportam-nos a ambos. E como todas as transações eletrónicas operam mediante transmissão de dados, considerava-se que se tratava em todos os casos, simultaneamente, da autenticação de todos os dados e da identificação do seu emitente.

O objeto da assinatura eletrónica podiam ser documentos formais ou declarações de uma pessoa, e podia abranger também suportes de imagem estática ou em movimento, que não têm que possuir as caraterísticas de documentos. O próprio enunciado do nome e da identificação do autor de um documento, ou de qualquer pessoa, são compostos de dados em forma eletrónica, que tal como os dados dos documentos, podem necessitar de ser autenticados, e portanto assinados. A vinculação de dados em suporte digital a uma pessoa é a essência da assinatura eletrónica,

[424] O Autor defende que "*não será uma assinatura eletrónica a aposição a um documento, por via informática, do nome do pretenso autor, porquanto essa introdução não é susceptível de constituir objecto de um direito individual e exclusivo*". Patrão, A. (2012). Assinaturas Eletrónicas, Documentos Eletrónicos e Garantais Reais. Reflexões Sobre a Viabilidade de Constituição de Garantias Imobiliárias por Meios Electrónicos à Luz da Lei Portuguesa. *Revista do Centro de Estudos de Direito do Ordenamento, do Urbanismo e do Ambiente*, página 51.

independentemente das caraterísticas desses dados, e essa função cumpre-se com a sua autenticação, que envolve a determinação da sua origem e a identificação da pessoa que em concreto a produziu ou subscreveu.[425]

Foi a Diretiva 1999/93/CE, de 13/12/1999 que centrou na autenticação a função essencial da assinatura eletrónica, definindo-a como um *"método de autenticação"*.[426] Esta definição seria muito importante para a produção legislativa que se lhe seguiu, dado que antes da Diretiva era bastante errático o sentido das definições da legislação produzida nos diversos países que avançaram com a sua publicação.

Nos países de tradição anglo-saxónica, a definição da função de assinatura eletrónicas anda muito próxima daquela que foi adotada na Diretiva da UE. A primeira lei de assinatura digital da história, publicada em 1995 no Estado do Utah, nos EUA, estabelecia que a função da "*assinatura digital*" consiste no estabelecimento de uma relação segura entre uma pessoa e uma mensagem, sem que seja usado o conceito de autenticação nem de autoria, nem se limitando essas funções aos documentos eletrónicos. Esta limitação da definição da Lei do Estado do Utah compreende-se pela falta de tradição legislativa nesta matéria, bem como pelo facto de as comunicações eletrónicas ainda estarem no início da sua expansão.[427]

Em Portugal, o primeiro diploma legal que regula a assinatura eletrónica, de agosto de 1999, anterior à Diretiva, não utiliza o conceito de autenticação e define assinatura eletrónica como um mecanismo que serve para *"dar a conhecer a autoria de um documento eletrónico"*.[428] A lei portuguesa tinha esta especificidade de incluir na definição de assinatura os documentos eletrónicos, o que era um importante fator de rigor. Porém, a definição de documento era muito ampla, ao ponto de incluir qualquer

[425] Diferente das conceções tradicionais de vinculação é a definição da Lei Russa de Assinatura Eletrónica, de 2003, que centra a sua função na proteção contra a fraude e a falsificação dos documentos, classificando-a como um detalhe de um documento eletrónico. Essa definição legal é a seguinte: *"An electronic document detail intended for protecting the electronic document against forgery …"*, acrescentando que a assinatura se baseia na tecnologia das assinaturas digitais. Kudruavtseva, O.I. (2008). The Use of Electronic Digital Signatures in Banking Relationships in the Russian Federation. *Digital Evidence and Electronic Signature Law Review*. Vol 5, pág. 51.

[426] A Diretiva define Assinatura digital como *"os dados sob forma digital, ligados ou logicamente associados a outros dados eletrónicos, e que sejam utilizados com método de autenticação"*

[427] Nos termos do n.º 10 do capítulo "46-3-103 Definitions", a assinatura digital é definida do seguinte modo: *"'Digital signature' is a sequence of bits which a person intending to sign creates in relation to a clearly delimited message by running the message through a one-way function, then encrypting the resulting message digest using an asymmetrical cryptosystem and the persons private key".*

[428] A alínea a) do artigo 2.º do DL n.º 290-D/99, de 2/8, define a assinatura digital como o *"resultado de um processamento eletrónico de dados suscetível de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico"*.

tipo de comunicação eletrónica. Por outro lado a definição do conceito é limitativa, e menos rigorosa, dado que limita também as funções da assinatura à autoria.

A autoria é um dos factos que a assinatura eletrónica pode revelar, mas a sua função é muito mais ampla. Quando uma pessoa subscreve um documento, assinando-o, não está a assumir a sua autoria, do mesmo modo que quando se pretende associar aos efeitos de um documento produzido por outra pessoa. A função da assinatura é o estabelecimento de um vínculo jurídico entre um documento e uma pessoa, podendo esse vínculo revestir tipologias diversas, incluindo a autoria. Mas a autoria não esgota as causas da vinculação.

Esta formulação da lei portuguesa é claramente tributária da função de aprovação que constava da LMCE, que também era limitativa. O conceito de autenticação engloba as duas funções que antes assinalámos à assinatura eletrónica. Quando se trata de um documento, a autenticação corresponde ao ato de associar esse documento a uma pessoa. Autenticar um documento significa colocar nele um sinal de que determinada pessoa o assume como dela, se assume como seu autor ou subscreve o seu conteúdo como sendo seu, ficando a ele vinculado.

Em Espanha, a lei de 1999 centra também a função da assinatura eletrónica na identificação do titular, não se referindo à função de autenticação.[429] Porém, tal como na lei portuguesa, centra-se a definição na função de identificação, acrescentando que ela consiste na determinação da autoria. Identificar o autor significa estabelecer a vinculação entre a identificação e a autoria do documento. Esta definição sofre também, das limitações de prever apenas a autoria como instrumento de vinculação jurídica, tal como na lei portuguesa.

Do mesmo modo a primeira lei alemã da assinatura, de 1997, não utiliza o conceito de autenticação e adota uma conceção funcional ainda mais restrita da assinatura eletrónica, considerando tratar-se, fundamentalmente, de um mecanismo destinado a identificar o seu titular (o dono da chave desse mecanismo que permite colocar a assinatura).[430] O carácter restrito desta definição é duplo, dado que por um

[429] A definição de assinatura eletrónica consta da alínea a) do artigo 2.º do Real Decreto-Ley 14/1999, de 17/9 e tem a seguinte redação: *«Firma eletrónica»: Es el conjunto de datos, en forma eletrónica, anejos a otros datos eletrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge"*.

[430] Trata-se da Lei da Assinatura Digital aprovada pela Lei Federal de 1/8/1997 (Signaturgesetz Sigg), que define a assinatura digital no n.º 1 do § 2.º do artigo 3.º, como *" um carimbo aposto em dados digitais que é gerado por uma chave privada de assinatura que vincula o dono dessa chave e garante a integridade dos dados, com a ajuda de uma chave pública associada …".* Tradução nossa da versão inglesa: *"For the purposes of this Act "digital signature" shall mean a seal affixed to digital data which is generated by a*

lado limita a função da assinatura à identificação e, por outro, limita o próprio conceito de assinatura à técnica da assinatura digital, diminuindo assim o âmbito de abrangência do conceito de assinatura eletrónica.

A lei italiana de 1997 é a que mais se aproxima do conceito de autenticação, embora não o utilize expressamente. A assinatura eletrónica é definida como *"o resultado de um programa informático que manifesta e torna possível a imputabilidade e integridade subjetiva da informação contida num documento ou num conjunto de documentos"*.[431] A imputação subjetiva da informação é um conceito próximo do de autenticação, sendo que esta definição não limita a natureza do vínculo jurídico à autoria, tendo também o cuidado de não limitar o instrumento da assinatura à assinatura digital, nem a qualquer tipo de outra tecnologia. Do mesmo modo a definição da lei italiana referencia a integridade como função da assinatura.

Nos EUA a lei federal define assinatura eletrónica como um *"símbolo"*, acrescentando também que se pode tratar de um *"processo"* ou de um *"som"*, que está ligado ou logicamente associado a um contrato a um documento, sendo que em todos os casos, para se tratar de assinaturas, devem ter sido executados ou aplicados por uma pessoa com a intenção de assinar o documento respetivo.[432]

O conceito de autenticação só é utilizado, nesta fase pela legislação inglesa, mas utiliza também o conceito limitativo da assinatura digital, pelo que não é neutra relativamente à tecnologia de assinatura que prevê. *O Electronic Comunications Bill*, de 18 de Novembro de 1999, define que a função da "assinatura digital" é a garantia da autenticidade de uma comunicação, tanto quando se trata de um documento como de um conjunto de dados.[433]

O conceito de autenticação seria utilizado, como referimos, na Diretiva 1999/93/CE, com o cuidado de não limitar a assinatura eletrónica a qualquer tipo de

---

private signature key and establishes the owner of the signature key and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority or the authority according to §3 of this Act.". Disponível em http://germanlawarchive.iuscomp.org/?s=digital+signature+act&submit= (última consulta efetuada em 28/1/ 2016).

[431] Trata-se da transcrição da alínea a) do n.º 1 do artigo 1.º da Legge 15/3/1997.

[432] A definição é a seguinte: *"The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record"*. 15 U.S. Code § 7006 – Definitions, https://www.law.cornell.edu/uscode/text/15/7006 (última consulta efetuada em 26/4/2016).

[433] A redação do n.º 7 é a seguinte: *"(1) In any legal proceedings- (a) an electronic signature incorporated or logically associated with a particular electronic communication or with particular electronic data, and (b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data"*.

tecnologia de assinatura. A diretiva estabelece de forma objetiva os pressupostos da autenticação e da presunção da sua eficácia, mas não limita esses pressupostos em função da tecnologia. Na versão inicial do projeto da Diretiva, a definição da função da assinatura eletrónica era muito mais restrita que aquela que viria a ser a definitiva. Essa definição inicial previa que a assinatura era um conjunto de dados e de procedimentos *"que utiliza um signatário para expressar conformidade com o conteúdo [de um documento]*".[434] Na versão final da Diretiva é adotado um conceito mais amplo, de autenticação, com um conjunto de requisitos técnicos menos exigentes, mas criam-se duas categorias de assinatura eletrónica, sendo uma a genérica e outra a assinatura eletrónica avançada, que respeita critérios técnicos mais exigentes e corresponde à definição da versão do projeto.

Esta definição possuía a máxima abrangência, porque incluía todos os tipos de dados, desde aqueles que se consubstanciavam em documentos, a todos os tipos de dados que suportavam as transações eletrónicas, incluindo os de identificação. Todos eles, na verdade, necessitavam de autenticação. Esse facto é confirmado pela circunstância de a Diretiva não definir um conceito de documento eletrónico nem limitar o objeto da assinatura a esse tipo de documentos. Do mesmo modo a definição não inclui nas funções da assinatura a garantia de integridade

A entrada em vigor da diretiva levou alguns Estados Membros a alterarem a sua legislação sobre assinatura eletrónica, incorporando no direito interno os seus princípios. A Alemanha alterou a sua lei em 2001, passando a definir a função da assinatura eletrónica como sendo de *"autenticação"*.[435]

Também em Itália a definição de assinatura viria a ser complementada em 2000, pela entrada em vigor do regime jurídico do documento de identidade eletrónico, fazendo dele parte a assinatura eletrónica do seu titular.[436] A assinatura eletrónica cumpre em Itália as duas funções de garantir a proveniência e integridade de um documento eletrónico, bem como de assegurar a identidade do seu titular.[437]

---

[434] Nadal, A.G. (2001). Op. Cit., pág. 50.

[435] O n.º 1 da secção 2 define assinatura digital como *"os dados em formato eletrónico ligados a outros dados eletrónicos ou logicamente associados a eles, que são utilizados para autenticação"*. Lei de 21/5/ 2001).

[436] Artigos 1.º, 3.º e 4.º do Decreto do Presidente do Conselho de Ministros, de 22/10/1999.

[437] A formulação legislativa de *"tornar manifesto e verificar a proveniência e integridade de um documento eletrónico"* seria acrescentada pelos Decretos do Presidente do Conselho de Ministros de 10/12/2007, que regulou o arquivo e transmissão de documentos eletrónicos, bem como pelo Decreto do Presidente da República de 28/12/2000, sobre documentação administrativa (alínea n) do n.º 1 do artigo 1.º).

Em Espanha a Lei n.º 59/2003, de 19/12, apesar de ter incorporado os princípios da diretiva, manteve o conceito de assinatura eletrónica restrito à função de identificação, definindo-a como *"meio de identificação do assinante"*[438], não se referindo aos conceitos de autenticação nem de autoria, nem mesmo de integridade. Regula-se, porém, o regime do documento eletrónico, definindo que se considera como *"documento eletrónico aquele que foi redigido num suporte eletrónico que incorpore dados que estejam assinados eletronicamente",*[439] ficando, assim, abrangida no mesmo regime jurídico, a assinatura eletrónica como instrumento de vinculação de uma pessoa a um documento. Não é utilizado o conceito de autenticação e a definição assume um carácter mais restritivo do que a de 1999.

Também em Portugal, o regime jurídico da assinatura eletrónica viria a ser ajustado em 2009 à Diretiva europeia, mas não se alterou a definição de assinatura, pelo que ainda hoje enferma das limitações que anteriormente enunciámos.

A definição da lei francesa é provavelmente a mais completa, definindo a função da assinatura eletrónica por remissão para a assinatura em geral dos contratos, que estabelece que a assinatura, em geral, necessária à perfeição de um contrato, identifica quem a apõe no documento (função de identificação) e manifesta o seu consentimento às obrigações dele decorrentes (função de autenticação). Em 2000 foi acrescentado, porém, ao art.º 1316-4 do Código Civil, que quando a assinatura é eletrónica, deverá consistir na utilização de um procedimento fiável de identificação do seu titular, bem como a sua vinculação ao ato a que está associada.[440]

O Regulamento EIDAS muda o paradigma até então vigente e efetua uma separação entre assinatura e identificação eletrónicas, reservando a primeira apenas para os documentos eletrónicos. Assume-se a plena equivalência entre a função da assinatura manuscrita e a assinatura eletrónica e reporta-se o conceito desta apenas para o ato de o

---

[438] O n.º 2 do artigo 3.º da referida Lei tem a seguinte redação*: "A firma eletrónico é o conjunto de dados em forma digital, consignados a outros ou associados entre si, que possam ser utilizados como meio de identificação do assinante"*. Tradução nossa do castelhano: *"1. La firma eletrónica es el conjunto de datos en forma eletrónica, consignados junto a otros o associados con ellos, que pueden ser utilizados como medio de identificación del firmante"*.

[439] É essa a redação do n.º 5 do artigo 3.º da lei n.º 59/2003, de 19/12.

[440] As alterações ao Code Civil foram introduzidas pela Loi n.º 2000-230, de 13/3/2000. A redação do artigo 1316-4 ficou fixada nos seguintes termos:

"Art. 1316-4. - La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à lacte. Lorsqu'elle est électronique, elle consiste en lusage dun procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est crée, l'identité du signataire assurée et lintégrité de lacte garantie, dans des conditions fixées par décret en Conseil d'Etat.".

signatário "*assinar*" (n.º 10 do artigo 3.º). A assinatura eletrónica é um conjunto de dados que estão ligados ou logicamente associados a outros dados em formato eletrónico e que são utilizados pelo signatário para assinar. Não existe, na verdade, uma definição do conceito de assinatura eletrónica, mas uma descrição do mecanismo de ligação de dados ou da sua associação lógica, quando utilizada essa ligação ou associação para o fim de "*assinar*", sendo que o sentido da função de "*assinar*", não é próprio dos suportes eletrónicos, mas comum à assinatura manuscrita.

É essa equivalência a base para a equiparação das assinaturas eletrónicas às manuscritas que se estabelece no artigo 25.º, mas para que a equivalência seja plena, nos termos do n.º 2 desse artigo, estabelecem-se no artigo 26.º, como funções essenciais das assinaturas eletrónicas qualificadas, que garantem essa equivalência, os seguintes:

i) A identificação do signatário;
ii) A vinculação dos dados de criação da assinatura à sua própria identidade;
iii) O controlo exclusivo, pelo signatário, dos dados de criação de criação da assinatura;
iv) A integridade do documento.

Assim, embora isso não resulte expresso dessa forma no texto do Regulamento EIDAS, a identificação, a autenticação, entendida esta como garantia de origem e a integridade, são as funções essenciais do da assinatura eletrónica, e portanto, elementos essenciais da sua definição, para além, da sua base de funcionamento, que são os dados e a sua correlação.

O Regulamento separa também a identificação da assinatura. No entanto, da assinatura faz parte essencial a função identificação, como acabamos de concluir. Mas isso não significa que a identificação eletrónica só se possa efetuar através da assinatura eletrónica. E é nesse sentido que o Regulamento EIDAS autonomiza a função de identificação, separando-a da assinatura eletrónica. Enquanto a primeira serve para se determinar o direito e o controlo do acesso a determinados serviços eletrónicos, incluindo a legitimidade para intervir em procedimentos e em processos, a assinatura serve para a autenticação dos documentos. Mas a identificação não autentica transações. Permite a identificação e a autenticação dos dados de identificação de pessoas, mas a autenticação dos documentos ou dos dados relativos às transações efetuadas depende sempre da assinatura.

Capítulo III – Funções da assinatura eletrónica

1. A função de identificação do titular

Além da função de autenticação documental, a assinatura eletrónica está para as relações estabelecidas em suporte eletrónico como o conhecimento pessoal está para as relações económicas estabelecidas pela presença pessoal das partes, sendo, por isso, mais abrangentes as suas funções que as da assinatura manuscrita.[441]

[441] Como se afirma de forma simples num recente relatório da UNCITRAL, *"In practice, various steps may be taken to verify the identity of the signatory. When the parties are all present at the same place at the same time, they may simply recognize one another by their faces; if they negotiate over the telephone, they may recognize each other's voices and so on. Much of this happens as a matter of course and is not subject to specific legal rules. However, where the parties negotiate by correspondence, or where signed documents are forwarded along a contracting chain, there may be few means of establishing that the signs that appear on a given document were indeed made by the person to whose name they appear to be linked and whether indeed only the duly authorized person was the one who produced the signature supposed to bind a particular person"*. "Promoting Confidence in Legal Issues on International Use of Electronic Authentication and Signature Methods" United Nations Commission on International Trade Law; United Nations, Vienna, 2009, pág. 9.

A pessoalização das relações estabelecidas por meio eletrónico depende, antes de mais, do conhecimento da identidade das partes, que é dado pela sua identificação. Não é possível estabelecer um vínculo entre um documento e uma pessoa sem se conhecer a identidade dessa pessoa. A identificação não assegura a vinculação, mas é um pressuposto essencial dela.

Nas relações estabelecidas mediante a presença física, a identidade apura-se pelo conhecimento pessoal ou pela apresentação dos documentos comprovativos respetivos. Nas relações estabelecidas à distância, quando existe conhecimento prévio entre as partes, essa identificação faz-se pelo conhecimento pessoal.

As relações estabelecidas por meios eletrónicos são também estabelecidas à distância, mas distinguem-se pelo facto de poderem envolver pessoas que não se conhecem entre si, especialmente através das redes abertas. O carácter imediato de muitas dessas relações exige uma forma de identificação que seja, sempre que possível, segura e imediata. Por essa razão a identificação adquire nos suportes eletrónicos uma importância que não possui no paradigma do papel.

Identificar uma pessoa não significa conhecer os seus atos, sejam eles declarações ou a autoria de documentos. A atividade de identificar tem natureza estática, a atividade de relacionar documentos ou atos com uma pessoa tem natureza dinâmica, relacional. Identificar é apenas obter informação acerca de uma pessoa, nada mais. Mas a identificação é um pressuposto essencial a essa função relacional.

Nas redes eletrónicas, a emissão de informação é efetuada mediante a ação de máquinas informáticas, por ação dos sistemas operativos. É certo que as máquinas e os sistemas nunca emitem essa informação se não houver intervenção humana. Essa intervenção pode ser contemporânea da emissão ou anterior, mas é essencial a ela. O problema é que, sendo a máquina um instrumento da ação humana, uma ferramenta utilizada para um determinado fim, não é inerente à comunicação a determinação da ligação entre a pessoa que emite um documento eletrónico e a máquina que executa essa emissão. E daí resulta que o destinatário de uma informação pode recebê-la sem que, com isso, fique a conhecer, com segurança jurídica suficiente, a identidade do responsável pela sua emissão. E este é um dos fatores de insegurança das relações estabelecidas por meios eletrónicos.

É por essa razão que a instituição de um sistema de confiança jurídica nos documentos eletrónicos pressupõe a prévia identificação dos sujeitos que os geram ou

subscrevem. Daí que a função de identificação seja essencial aos sistemas de assinatura eletrónica.

Nas relações pessoais, a identificação é um ato muitas vezes intuitivo e imediato, mas trata-se de um procedimento que não é unívoco e pode não ser simples. Para que uma pessoa se identifique perante nós, é necessário que nos informe do seu nome e, eventualmente, de outros atributos de identificação, mas não é com esses elementos informativos que a pessoa nos proporciona, que procedemos à sua identificação.

Para isso utilizamos dados informativos que nos são proporcionados por terceiros, que são, em último caso, as entidades administrativas competentes para a identificação e o registo civil. Trata-se de entidades dotadas de poderes públicos, que lhes conferem o crédito de serem entidades de confiança, e em cujas declarações e informações acreditamos. Quando alguém nos apresenta os seus elementos de identificação e os confirma mediante a apresentação da informação proveniente dessas entidades, considera-se efetuada essa identificação. Para identificar uma pessoa, não nos basta a informação que ela nos proporciona, sendo sempre necessário o crédito que nos merece a informação proveniente das entidades terceiras competentes nessa matéria.

Nas relações estabelecidas por meios eletrónicos, recorremos também a entidades terceiras para que a identificação seja segura, que são os prestadores de serviços de confiança eletrónica, sendo essa a função dos certificados de assinatura eletrónica.

O Regulamento EIDAS separa a função de identificação da assinatura eletrónica, mediante a qual a assinatura identifica a pessoa que assina um determinado documento eletrónico, da função de identificação eletrónica das pessoas que operam através de meios eletrónicos, nos casos em que essa identificação seja necessária e as transações sejam efetuadas sem recurso à sua documentação.

As transações eletrónicas podem ou não ser documentadas, ou seja, suportadas em documentos eletrónicos e sendo a assinatura o instrumento de autenticação de documentos, a assinatura eletrónica serve apenas para autenticar as transações eletrónicas suportadas em documentos eletrónicos. E é assim que o Regulamento concebe a assinatura eletrónica, sendo que uma das suas funções é, como vimos, a da identificação do signatário.

Essa função de identificação, da assinatura eletrónica, não se confunde com a identificação eletrónica, que é um instrumento autónomo de autenticação pessoal para legitimar o acesso aos serviços eletrónicos.

Mas da assinatura eletrónica faz sempre parte a identificação do signatário, como requisito essencial que é estabelecido de forma expressa para a definição dos conceitos de assinatura eletrónica avançada (alínea b) do art.º 26.º) e de assinatura eletrónica qualificada (alínea c) do anexo I). Essa exigência constava também da alínea c) do anexo I da Diretiva de 1999 para os certificados qualificados. Mas ao mesmo tempo, a identificação eletrónica é autonomizada como uma função específica para a segurança jurídica nas transações eletrónicas, não suportadas em documentos, no capítulo II do Regulamento.

2. A função de aprovação do conteúdo das mensagens eletrónicas

A função de aprovação do conteúdo das mensagens eletrónicas era uma exigência de autenticação que nasceu no contexto do EDI. No contexto histórico da emergência dessa tecnologia, a aprovação do conteúdo era assumida como a principal função da assinatura eletrónica, para além da identificação do seu autor.[442]

Tanto a definição do conceito de assinatura da LMAE como dos pressupostos de equivalência da LMCE, estabelecem que a função da aprovação do conteúdo das mensagens eletrónicas é um elemento essencial da assinatura eletrónica.[443]

Compreende-se esta preocupação da LMCE, cujo objetivo principal foi o reconhecimento jurídico das mensagens EDI e a necessidade de conferir confiança na utilização dos meios eletrónicos. A natureza das mensagens eletrónicas trocadas por esta via, entre máquinas, associada à automatização das operações no seio das empresas, que aquela tecnologia havia proporcionado pela primeira vez, conduziu a que muitas

[442] Este entendimento acerca da imanência da aprovação ao próprio conceito de autenticação era expressa nos trabalhos preparatórios da LMCE do seguinte modo: *"One function of a signature was to indicate to the recipient of the document and to third parties the source of the document. A second function of a signature was to indicate that the authenticating party approved the content of the document in the form in which it was issued and intended to be bound by the content of the document"*. "A/CN.9/WG.IV/WP.55", par. 53.

[443] O artigo 7.º da LMCE refere na alínea a) a assinatura como um método usado para a identificação da pessoa e de indicação de que ela aprovou a informação contida na mensagem: *"a method is used to identify that person and to indicate that person's approval of the information contained in the data message". "Guide to Enactment LMCE (1996)"*, pág. 6. Do mesmo modo a LMAE inclui na sua definição do conceito a função da aprovação: "*indicate the signatory's approval of the information contained in the data message".* "A/CN.9/493".

mensagens expedidas por essa via, de uma empresa para outra, fossem impulsionadas de forma automatizada, mediante programação informática. Nesses casos não existiria iniciativa nem ação humana imediata e individual.

Nesse contexto era importante que se vincasse o carácter pessoal dessas comunicações, apesar de a sua iniciativa poder ser automatizada. Por isso foi manifesta a preocupação de conferir segurança às relações jurídicas, assegurando que as mensagens eletrónicas comunicadas por EDI revelam sempre a vontade das partes. E a forma mais enfática de o fazer foi a consignação da previsão legal de que a parte que emite a mensagem fica a ela vinculada porque a "*aprovou*", relevando-se assim o carácter pessoal das declarações negociais transmitidas, apesar de essa transmissão se operar mediante o funcionamento de máquinas eletrónicas.

Além disso, a inclusão do conceito de aprovação pretende conexionar esses mecanismos automáticos com a intencionalidade e a vontade das empresas. Essas comunicações, não dependendo de um ato de vontade pessoal expresso e específico em cada uma delas, estariam sempre cobertas pela aprovação geral do seu conteúdo, que era dada pela responsabilidade pela determinação do automatismo dos equipamentos eletrónicos.

Mas a verdade é que, apesar desse sentido da LMCE, a determinação da aprovação de uma mensagem não cabe no âmbito da abrangência da determinação da sua origem.

Uma assinatura prova a vontade de vinculação de uma parte a um documento, mas o processo intelectual de formação dessa vontade não é o mesmo que aquele que forma o entendimento que a pessoa tem do seu conteúdo. A vontade de assinar um documento materializa-se com a sua assinatura, mas esse ato não revela necessariamente um acordo ideológico com o seu conteúdo, que é externo e se situa para além da utilização da assinatura como instrumento de vinculação jurídica. Uma assinatura é um facto material que revela uma manifestação de vontade, mas essa manifestação de vontade limita-se à vontade de vinculação.

A função das assinaturas é vincular juridicamente pessoas a documentos e não avaliar qual o entendimento que essas pessoas adotam acerca do seu conteúdo. A assinatura revela que uma pessoa participou voluntariamente na elaboração de um texto ou na sua subscrição, mas não revela nada acerca daquilo que a pessoa pensava do conteúdo do documento na data em que o subscreveu, nem o que pensa atualmente. E essa revelação não ocorre em qualquer tipo de assinatura, seja uma assinatura manual

autógrafa, ou outra. Todas estas formas de expressão da vontade de vinculação revelam o mesmo acerca do entendimento do seu autor acerca do conteúdo de um documento.[444]

Uma pessoa pode vincular-se a um documento com cujo teor não concorda integralmente, ou não concorda simplesmente, mas em determinado momento, por razões que poderão ser de diversa índole, decidiu vincular-se juridicamente a ele. Por outro lado, documentos existirão em que não se coloca a questão de saber se os titulares da assinatura concordam com eles ou não, por serem apenas declarações de ciência ou relato de acontecimentos.[445]

A inclusão do requisito da aprovação do conteúdo das mensagens não foi pacífica nos trabalhos preparatórios, tanto da LMCE como da LMAE. As críticas incidiam particularmente no facto de esse ser um requisito subjetivo, de difícil demonstração, porque não se pode apreciar apenas com base nos elementos objetivos da assinatura. Essa subjetividade é um fator de insegurança para as partes.[446]

Apesar disso, o requisito manteve-se na LMAE, mas deixou de constar das definições do conceito de assinatura eletrónica de outros instrumentos normativos contemporâneos ou posteriores.[447] Um desses instrumentos é a definição de assinatura eletrónica constante do projeto de diretiva do Parlamento Europeu e do Conselho relativamente às assinaturas eletrónicas, que foi citado pela própria UNCITRAL: *"Electronic signatures means data in electronic form attached to, or logically*

---

[444] A função da aprovação do conteúdo do documento foi objeto de controvérsia na elaboração da UNCUECIC, em 2006. *"There might be instances where the law requires a signature, but that signature does not have the function of indicating the signing party's approval of the information contained in the electronic communication"*. "A/CN.9/608/Add.2", par. 32. Releva a posição do Canadá, no sentido de essa expressão de "aprovação" ser substituída, argumentando com o exemplo da participação dos notários e das testemunhas, no ato de assinatura de um documento. Essa participação comprova apenas que a parte assinou regular e efetivamente o documento, não revela qual o entendimento subjetivo que essa pessoa tinha acerca do seu conteúdo, nem qualquer outro tipo de juízos da mesma categoria. *"The signatures of the witnesses merely identify them and associate them with the contents of the document witnessed, but do not indicate their approval of the information contained in the document"*. *Idem*, par. 32.

[445] A rejeição da ideia da aprovação do conteúdo do documento era inclusivamente aceite pelos defensores da manutenção dessa referência no texto do preceito, que entendiam dever manter-se apenas para vincar o efeito de associação do autor ao documento. *"The use of the word "approval" did not necessarily imply any assessment of the subjective intent of the signer with respect, for example, to the contractual or other legal effects of the message. Instead, it was limited to associating the signer with the message"*. "A/CN.9/457", par. 27.

[446] *"Another suggestion was that the use of the term "approval" was too subjective and conducive to uncertainty as it depended on the intentions of the signer at the time of signing"*. "A/CN.9/457", par. 26.

[447] Como referimos atrás, compreendia-se que esse requisito constasse do regime das assinaturas eletrónicas no contexto do EDI, quando emergiram as primeiras comunicações eletrónicas automáticas, muitas vezes sem intervenção humana. Nesses casos era necessário imputar essas mensagens às próprias empresas que eram titulares dos sistemas que efetuavam as comunicações. A utilização do conceito de aprovação era uma forma mais enfática de evidenciar o vínculo jurídico pretendido. Mas a verdade é que para que a vinculação jurídica depende apenas da assinatura, dado que é ela que o estabelece.

associated with, other electronic data and which serves as a method of authentication".[448]

Esta definição da assinatura eletrónica como sendo dados em forma eletrónica juntos ou eletronicamente associados a outros dados eletrónicos, que sirvam de autenticação, abandona o conceito de aprovação e centra-se no de autenticação.[449]

É necessário separar a aprovação, pelo autor de uma mensagem, da própria vontade de ele se vincular a ela. A intencionalidade do autor do documento de a assumir como sua, seja como sendo o seu criador, seja revelando a sua adesão e a sua vinculação ao respetivo conteúdo, é uma função diferente da aprovação. Distinta da aprovação do conteúdo do documento assinado é a vontade de vinculação do autor da assinatura.[450] Esse requisito parece-nos essencial como elemento do conceito de assinatura. A assinatura é sempre um ato de vontade, que traduz a intenção voluntária do titular da assinatura, de se vincular ao conteúdo do documento assinado.[451] Concordamos com os que defendem que essa vontade é um requisito essencial na composição do conceito de assinatura, sendo certo que existem referências nos trabalhos preparatórios da LMAE nesse mesmo sentido.[452]

Daqui resulta que é diferente a aprovação do conteúdo de um documento, do acordo de vinculação de uma pessoa a esse documento. A vontade de vinculação jurídica não tem que exigir como pressuposto um acordo ou uma aprovação da pessoa que assina relativamente ao teor do documento, porque pode uma pessoa concordar em se vincular juridicamente com o conteúdo de um determinado documento, assumindo

---

[448] "A/CN.9/457", par. 26.

[449] Analisaremos o conceito de autenticação no ponto seguinte.

[450] Como afirmam Hatfield e Casamento, mais do que a intenção de aprovar o conteúdo, releva o consentimento e a vontade de se vincular do autor da assinatura. *"The electronic signature process should clearly inform the signer that using such an electronic sound, symbol, or process is how the signer expresses his or her consent to sign such documents thereby evidencing his or her intent to be bound to such terms and conditions"*. Casamento, G. e Hatfield, P.; op. cit, pág. 86.

[451] A utilização do requisito da aprovação destinava-se também a vincar a assinatura como um ato de vontade, face ao carácter instrumental e técnico da operação de assinar um documento eletrónico. Ora essa aplicação pode ser efetuada para outros fins que não os de assinar. É o caso, por exemplo, da aplicação de uma chave sobre um documento para o encriptar ou desencriptar. Essa aplicação não é efetuada com vontade de assinar, pelo que dela não resulta uma assinatura. Este entendimento emergiu em especial na doutrina americana, em especial à volta do conceito de assinatura da UETA. No mesmo sentido, Rivero, D.C. (Mayo 2005); op. cit., pag. 99., notas 233 e 234.

[452] Essa questão foi debatida e consensualizada pelo Grupo de Trabalho. *"It was agreed that the draft guide to enactment should make it clear that the notion of "electronic signature" was intended to cover all uses of a handwritten signature for legal effect, the identification of the signatory and the intent to sign being no more than the smallest common denominator to the various approaches to "signature""*. "A/CN.9/483", par. 63.

como suas as consequências que dele emergem, mas essa vontade de vinculação não tem que significar necessariamente o acordo acerca do seu conteúdo.[453]

Parece-nos que esse conceito de aprovação, que consta da LMAE, deve ser interpretado como a vontade da pessoa que assina, de se vincular ao conteúdo do documento.

Em linha com este nosso entendimento, o requisito da aprovação foi abandonado do conceito de assinatura eletrónica que é utilizado na UNCUECIC. Esse requisito constava das versões iniciais do projeto de convenção, mas viria a ser abandonado na sequência de observações acerca da sua desnecessidade.[454]

Se a assinatura de um documento é um ato pessoal de vinculação que se consuma mediante a utilização de um instrumento eletrónico pessoal e exclusivo, é essencial a essa utilização que se trate de um ato de vontade. Mas esse ato de vontade tem como referente a vontade de assinar e de se vincular ao documento, que não é necessariamente uma vontade de avaliar e de aprovar o respetivo conteúdo.

Sendo a vontade de assinar um pressuposto fundamental da definição do conceito de assinatura eletrónica, coloca-se a questão acerca das consequências que advirão num caso em que uma assinatura não resulte de um ato de vontade, por exemplo nos casos em que a utilização da chave privada foi efetuada inadvertidamente ou quando foi utilizada mediante coação. Nesses casos não se pode entender que o documento se considere assinado, uma vez que não existiu um ato de vontade ou a

---

[453] Nos casos em que a assinatura manuscrita tem o mais elevado grau de segurança, que são aqueles em que ela é reconhecida presencialmente por um notário, o notário não tem que perguntar à pessoa que assina se concorda com o conteúdo do documento assinado. E quando o notário certifica que a assinatura foi colocada no documento na sua presença, não tem que certificar qual o entendimento da pessoa acerca do seu conteúdo, nomeadamente se concorda, e em que medida, com esse conteúdo. Embora referindo-se especificamente ao papel do notário no seu entendimento acerca do conteúdo do documento assinado, é também nesse sentido que se veio a pronunciar a delegação de Singapura nos trabalhos preparatórios de elaboração do projeto de UNCUECIC de 2005: *"For example, many countries have requirements of law for notarization of a document by a notary or attestation by a commissioner for oath. In such cases, it is not the intention of the law to require the notary or commissioner, by signing, to indicate his approval of the information contained in the electronic communication. In such cases, the signature of the notary or commissioner merely identifies the notary or commissioner, and associates the notary or commissioner with the contents of the document, but does not indicate the approval by the notary or commissioner of the information contained in the document".* A/CN.9/578/Add.10, par. 4.

[454] Antes de 2005, estabelecia o n.º 3 do artigo 9.º do projeto de convenção, que eram pressupostos da assinatura eletrónica a existência de um método que assegure a identificação da parte que assina e a sua aprovação da informação que dele consta. Na versão final da Convenção, manteve-se, naturalmente, o requisito da identificação, sendo o requisito da aprovação substituído pelo requisito de que o método de assinatura assegure a indicação da vontade da parte relativamente à informação constante do documento eletrónico. É a seguinte, a redação da alínea a) do n.º 3 do artigo 9.º da Convenção: *"A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication".* "United Nations Convention on the Use of Electronic Communications in International Contracts". United Nations Commission on International Trade Law; United Nations, New York, 2007, pág. 108.

vontade não foi livremente formada. E não tendo sido utilizado como instrumento de vinculação voluntária a um documento, a aplicação da chave privada ao *hash* não constitui, nesse caso, uma assinatura válida.

É verdade que uma vez aplicada essa chave privada estamos perante um procedimento que materialmente é uma assinatura, que revela, normalmente, um ato de vontade de o respetivo titular se vincular a um documento, mas o ato da sua aplicação, não sendo um ato voluntário, não cumpre os requisitos de vinculação, e portanto não se cumprem os requisitos de assinatura.

No entanto, uma assinatura é uma marca pessoal aplicada sobre um documento, que a lei consagra como revelando uma vontade, livre e conscientemente assumida, de vinculação. Podem ocorrer circunstâncias que conduzam à conclusão de que aquela assinatura é inválida ou até inexistente.

Mas uma vez aplicada a assinatura, o apuramento dessas circunstâncias exige, um procedimento probatório conforme, no seio de um processo que sirva para impugnar essa assinatura, cabendo ao autor da assinatura essa prova.[455]

Em conformidade com o entendimento que defendemos, a legislação da UE acerca das assinaturas eletrónicas exclui do conceito de assinatura o requisito da aprovação, como acabámos de verificar no capítulo anterior.

3. A função de autenticação

A função de autenticação dos documentos é diferente da função de identificação. Identificar uma pessoa é conhecê-la, ficar a saber quais os elementos informativos correspondentes à sua identidade. Trata-se de uma função estática, meramente cognoscitiva.

Conhecer a identidade de uma pessoa, mediante a sua identificação, não é a mesma coisa que determinar que essa pessoa foi a autora de um documento. A identificação é um pressuposto essencial à determinação da autoria, mas não é suficiente. Para isso é também necessário que entre a pessoa e o documento exista um vínculo com relevância jurídica. A revelação desse vínculo é uma das mais importantes

[455] Este era também o entendimento do Grupo de Trabalho da UNCITRAL, que considerava que a assinatura constitui uma presunção de autenticação e de que o ato da sua aplicação foi um ato válido e voluntário. *"Thus, by appending a signature (whether hand-written or electronic) to certain information, the signatory should be presumed to have approved the linking of its identity with that information"*. "A/CN.9/WG.IV/WP.88", par. 119.

funções da assinatura que, como acabamos de analisar, tem como uma das suas funções, a de identificação. A outra função é a do estabelecimento deste vínculo.

A função de autenticação é o estabelecimento do nexo entre o autor ou subscritor e o documento. E esse nexo, sendo expresso pela assinatura, que o manifesta, revela a origem do documento e funda o vínculo jurídico entre a pessoa e o documento. Se a identificação é uma função cognoscitiva, a autenticação é uma função transacional, relacional e interativa. Trata-se de uma função que assegura a conexão entre uma pessoa e um documento, que os liga entre si.

O conceito de autenticação provém do paradigma do papel. Em Portugal o Código Civil reserva-o para os documentos definindo-o como a garantia da sua origem, sendo que essa origem é sempre uma pessoa. Essa determinação de origem é o instrumento de vinculação jurídica de uma pessoa a um documento. O n.º 1 do art.º 370.º do Código Civil (sob o título Autenticidade) estabelece que se presume *"que o documento provém da entidade ou oficial público a quem é atribuído, quando estiver subscrito pelo autor com assinatura reconhecida por notário ou com o selo branco do respetivo serviço"*.

No paradigma do papel, qualquer pessoa pode verificar, com os seus próprios meios, se um determinado documento vincula ou não determinada pessoa. Essa verificação é feita mediante a observação do documento e da assinatura que dele consta. Se conhecermos aquela assinatura e a pessoa que a colocou, nós próprios constatamos que o documento onde ela está aposta, vincula essa pessoa. Para essa verificação não necessitamos de instrumentos externos, bastando o nosso conhecimento e a observação que fazemos do documento.

Os documentos em papel possuem autonomia para, por si mesmos, revelarem a sua autenticidade a qualquer pessoa interessada, sem necessidade de recurso a outras pessoas ou a outros instrumentos. Essa simplicidade é muito importante para a segurança jurídica dos agentes económicos e para a rapidez do desenvolvimento das relações negociais.

Apesar disso não é fácil discriminar, nos documentos em papel, a função autenticação da função identificação, ambas incluídas no conceito de assinatura. No papel, a assinatura incorpora-se no suporte documental, e com o conteúdo do documento e o suporte de papel, constituem um objeto único e incindível.

A identificação e a autenticação estão ínsitas na assinatura manual, tal como a observamos no papel. A identificação resulta da associação da assinatura a uma pessoa e

aos elementos informativos da sua identidade que constam dos respetivos documentos. A autenticação é também, nos documentos em papel, uma função transitiva entre a pessoa e o documento, mas ela faz parte essencial da assinatura que integra o documento e a assinatura manual é, também ela, um elemento estritamente pessoal e intrínseco à pessoa. A assinatura manual não é um objeto nem uma entidade estranha, nem sequer extrínseca à pessoa que assina. Entre o documento e o seu autor nada se interpõe, sendo direta a relação, dado que a assinatura não se autonomiza, uma vez que a partir do momento em que é colocada no documento passa a integrá-lo.

Nos documentos em papel, a constatação da identidade do autor da assinatura e a verificação da autenticidade do documento são simultâneas e dificilmente cindíveis, pelo facto de a assinatura integrar o documento e não se poder dele separar. [456]

Nas assinaturas eletrónicas não é assim. A assinatura eletrónica é uma construção e não apenas uma expressão das caraterísticas inatas do seu titular. Trata-se de um sinal objetivado, uma construção própria, autonomizada da pessoa e do documento. Uma entidade que se interpõe entre um objeto, que é o documento e um sujeito, que é o seu autor. Enquanto a assinatura manual não existe enquanto não for manuscrita e logo que o é passa a integrar o documento, a assinatura eletrónica é uma entidade terceira entre o seu titular e o documento. É um verdadeiro instrumento de conexão.

Nas transações eletrónicas, o facto de serem efetuadas à distância, entre máquinas e entre pessoas que não se conhecem, a segurança e a confiança na sua utilização exigem que os elementos necessários tanto à identificação como à autenticação estejam sempre disponíveis.

Nestas transações, a função autenticação separa-se com maior nitidez da função identificação. E se a função identificação se cumpre mediante a verificação dos certificados emitidos pelas entidades que prestam serviços de confiança, que geraram o par de chaves da assinatura, essa operação não serve, por si só para autenticar o documento.

Autenticar significa apurar a origem de determinada informação com segurança, e para isso é necessário que estabeleçam dois vínculos diferenciados.[457] Um,

[456] Esta simplicidade de verificação da identidade e da autenticidade nas assinaturas manuscritas tem a desvantagem de não ser um método absolutamente seguro. *"However, it can be recalled that, even though manual signature, or its physical reproduction by mechanical or other means, is familiar and inexpensive and serves well for transaction documents passing between known parties, it is far from being the most efficient or the most secure method of authentication"*. "A/CN.9/333", par. 53.

entre o documento e a assinatura, ou seja, o sinal ou o procedimento objetivado que evidencia o ato de assinar e outro, diferente, entre esse instrumento e a pessoa que é o seu titular. É dessa dupla conexão que resulta a autenticidade do documento, e ela deve ser sempre possível de ser evidenciada nos documentos em suporte eletrónico.

Ir à procura da origem dos documentos eletrónicos é particularmente difícil, em especial nas redes abertas, exigindo um conjunto de procedimentos mais complexos que aqueles que são utilizados nas relações estabelecidas mediante a presença física. É necessário ultrapassar os fatores de separação e de impessoalização, como são as máquinas com as quais é operada a emissão, a remessa, o transporte, a receção e a leitura dos documentos, bem como o próprio instrumento de verificação das assinaturas, que em si mesmo é um instrumento objetivado.

O problema da autenticação é o de mais difícil resolução nas transações eletrónicas, uma vez que não se trata apenas de definir com rigor o respetivo conceito, mas também de encontrar um modo seguro para a sua determinação.

A autenticação é a função típica da assinatura, porque representa o núcleo essencial de determinação do vínculo de uma informação, de um documento, a uma pessoa que lhe deu origem, e isso justifica que analisemos como evoluiu a sua formulação e as tentativas de encontrar soluções.

3.1. A autenticação eletrónica nos primeiros estudos jurídicos

O primeiro documento da UNCITRAL que utiliza o conceito de autenticação é de 1984, considerando-a o instrumento que permite a um recetor determinar se uma mensagem provém de uma origem de onde diz provir. É essa verificação da origem o elemento essencial da autenticação.[458].

Na transição para os suportes eletrónicos, a segurança acerca da origem dos documentos era uma preocupação central do seu regime jurídico.[459] Partia-se do

[457] É esse sentido de determinação da origem – ou proveniência - que constitui a substância do conceito de autenticação do n.º 1 do artigo 370.º do Código Civil.

[458] A primeira definição de autenticação da UNCITRAL é a seguinte: *"Authentication: The identification of a message in a physical, electronic or other manner which permits the receiver to determine that the message come from the source indicated"*. A/CN.9/250 and Add.1 to 4, pág. 120. A mesma definição foi consagrada na versão final, de 1987. "UNCITRAL Legal Guide on Electronic Funds Transfer", pág. 7.

[459] Esta definição de autenticação, limitada apenas à verificação da origem, era assumida também em 1989, no Relatório do Secretário-Geral, nos seguintes termos: *"The important difference is that 'authentication' as here defined does not include the aspect of validating 'part or all of the text' of a*

paradigma da autenticação formal dos documentos em papel, considerando-a como o instrumento jurídico que confere a um determinado documento a força jurídica de fazer fé perante as partes e terceiros.[460] Nos trabalhos da UNCITRAL distinguia-se a autenticação formal, efetuada por notário ou entidade oficial autorizada, da autenticação informal, que assegura a indicação da origem dos documentos, sem o recurso a essas entidades. Como se trata de um texto sobre mensagens eletrónicas de transferências de fundos, é nesta última modalidade de autenticação que o documento se centra.

Em ambos os casos a autenticação é um atributo que é determinado mediante a colocação, no documento, de uma marca que o passa a integrar de forma permanente e que proporciona ao destinatário a informação sobre a sua origem efetiva.

Esta definição separa a autenticação da função integridade. Determinar a origem de uma mensagem é coisa diferente da determinação da sua eventual alteração posterior à assinatura. Quando apuramos a proveniência de uma mensagem, ficamos a saber quem a gerou, podendo, eventualmente, ser importante, e normalmente é, determinarmos também se ela foi alterada após a sua assinatura. Mas sendo importante esta última determinação, ela não deixa de ser uma função separada.[461] A autenticação serve apenas para determinar a origem do documento, e não a sua completude ou integridade. Do mesmo modo que a função da autenticação se distingue da identificação, distingue-se também da integridade, sendo porém estas as três funções mais importantes da assinatura eletrónica.[462]

---

payment order. This is appropriate, even though most electronic authentication techniques do both, since these Rules also apply to paper-based payments orders". A/CN.9/WG.IV/WP.39)", pág. 92.

[460] "The authentication of a document or a message gives it a legal form which renders it worthy or belief". "A/CN.9/250 and Add.1 to 4", pág. 133. A mesma definição é dada pela pelo Guia Legal da Transferência Eletrónica de Fundos, de 1987. "UNCITRAL Legal Guide on Electronic Funds Transfer", pág. 32.

[461] A questão foi debatida nos trabalhos preparatórios, nos quais ficou clara essa separação. "*For the purpose of this guide, it is immaterial whether authentication may also permit the receiver to determine that the message has not been deliberately or inadvertently altered".* A/CN.9/250 and Add.1 to 4, pág. 120.

[462] O tema da integridade dos documentos eletrónicos é central na segurança jurídica das transações eletrónicas e desempenhará um papel fundamental na construção do conceito de assinatura eletrónica. O relatório que estamos a analisar tem o mérito de ser o primeiro que aponta já para a importância deste tema. *"The design of any electronic funds transfer system should assume the possibility of interception and reading of messages, alteration of genuine messages and the introduction of false messages"*. Aponta também um caminho possível na procura de instrumentos jurídicos e técnicos de segurança, aventando a possibilidade de utilização da criptografia (*"The first line of protection against such fraud is encryption"*), embora revele algum cepticismo, em face da rápida evolução da tecnologia e dos conhecimentos técnicos disponíveis da época (*"an encryption standard which is highly secure today may be rendered insecure within a few years by the development of more powerful computers and new techniques for factoring the large numbers on which encryption is based."*). "A/CN.9/250 and Add.1 to 4", pág. 144.

Embora essa separação seja clara nos trabalhos da UNCITRAL, ela não o era em termos gerais, dada a necessidade que nessa época já se sentia, de segurança jurídica nas mensagens eletrónicas. A definição de autenticação no Documento DIS 7982 considera a autenticação como um código, previamente acertado pelo emitente e pelo recetor, existente numa mensagem, que serve não só para validar a sua origem, como também para assegurar que o seu conteúdo não foi alterado.[463],[464]

A determinação da origem é uma função diferente da determinação da competência ou da legitimidade do emissor para proceder à geração e envio da mensagem.[465] Também esta matéria foi discutida nos trabalhos preparatórios e se optou por essa separação. Pelo contrário, a norma *ISO Banking Comittee*, considera que a autenticação consiste no processo de determinação de que a mensagem provém de uma pessoa com autoridade para a emitir ou para proceder ao seu envio.[466] Apesar disso, ficou expresso na Lei Modelo dos Pagamentos Internacionais de 1991, que a autenticação se limitava à determinação da origem das mensagens.[467]

Questão diferente é a do método de determinação da origem das mensagens eletrónica, que evolui com a utilização dos seguintes métodos:

i) A assinatura manual autógrafa colocada no suporte físico do qual constam os documentos eletrónicos.

ii) A confirmação da receção da mensagem, mediante telefonema do destinatário ao emissor;

iii) A utilização de cartões de plástico com bandas magnéticas associadas a códigos numéricos inseridos pelos utilizadores em máquinas que efetuam a leitura da banda magnética e a comparam com o código individual, os tradicionais cartões de débito e de crédito. Os clientes

---

463 "*A code in a message between the sender and the receiver used to validate the source and the full text of the message*". " A/CN.9/250 and Add.1 to 4", pág. 120.

464 A preocupação centrada na origem das mensagens eletrónicas centra-se nas ordens de pagamento e de transferências financeiras *"The purpose of an authentication procedure is to permit the receiving bank to determine whether the payment order was issued by the purported sender"*. O sentido da definição é a responsabilização do emitente, como se extrai do trecho seguinte: *"The authentication provided is a commercially reasonable method of security against unauthorized payment orders"*. A/CN.9/346), pág. 61.

465 "*The authentication of a message does not necessarily indicate that the message as received was authorized or that the person sending the message had authority to do so."* A/CN.9/250 and Add.1 to 4, in Yearbook of the United Nations Commission on International Trade Law, 1984, volume XV, pág. 120.

466 *"The process of determining that a message comes from a source authorized to originate messages of that type"."*A/CN.9/250 and Add.1 to 4", pág. 120.

467 *"'Authentication' means a procedure established by agreement to determine whether all or part of a payment order or a revocation of a payment order was issued by the purported sender"*. A/CN.9/344, pág. 210.

bancários emitem, operações sobre a sua conta, em equipamentos informáticos que expedem mensagens eletrónicas ao sistema central, com a segurança jurídica de que foram geradas pelo titular da conta.[468] A autenticação advém de dois factos, por um lado a utilização de um determinado código secreto e de um cartão associado e, por outro lado, pela existência de uma convenção prévia entre o banco e o seu cliente, mediante a qual se estabelece que todas as mensagens recebidas nos sistemas do primeiro com aqueles atributos se consideram ter origem no próprio cliente.[469]

iv) O estabelecimento de redes fechadas de comunicação eletrónica entre as entidades bancárias, mediante convenção prévia de assinatura, cabendo às respetivas entidades cumprir a obrigação de verificar a autenticidade das mensagens recebidas, como pressuposto essencial de exoneração de responsabilidade.[470]

Todos os mecanismos enunciados eram vulneráveis à fraude, pela possibilidade de os respetivos instrumentos, incluindo os cartões, serem utilizados indevidamente por terceiros, como se fossem os seus titulares legítimos.[471] Essa vulnerabilidade era agravada por ser prática, na atividade económica, nem sequer se proceder à verificação da autenticidade das assinaturas quando se tratava de transações de baixo valor.[472]

---

[468] "*Current models of cash dispensers, automated teller machines and point-of-sale terminals require the convergence of two items to authorize the transactions, i. e. a plastic card with magnetic stripe containing certain information and the entry by the bank customer of a personal identification number (PIN)"*. "A/CN.9/250 and Add.1 to 4", pág. 143.

[469] *"Protection against fraud in the use of customer-activated terminals is, therefore, a joint endeavor of the bank and the customer"*. "A/CN.9/250 and Add.1 to 4", pág. 143.

[470] Esta obrigação é expressa na Nota do Secretariado, de 27/8/1987, nos seguintes termos: *"verification of the authentication of the instruction would include examination of signature or of the electronic authentication used"*. A/CN.9/WG.IV/WP.37, pág. 59.

[471] *"Mechanical forms of signature on paper documents and various techniques for authentication of an electronic funds transfer instruction can be authenticated in a proper form by an unauthorized person or by a person exceeding his authority. If such a person had access to the legitimate stamp, perforation device, test key, encryptation key or plastic card and PIN, the instructions which he caused to be issued would be identical to those issued under proper authorization"*. "A/CN.9/250 and Add.1 to 4", pág. 134.

[472] Os custos dos sistemas de autenticação são sempre relevantes, nomeadamente nos mercados financeiros em que as transações podem ser de valores reduzidos. No papel muitos dos documentos nem sequer eram verificados, utilizando-se técnicas de amostragem, mas nos suportes eletrónicos essa verificação deve ser exaustiva e sistemática. Discutia-se a forma de diminuir os custos de insegurança dos sistemas de autenticação eletrónica e apontava-se como solução a partilha, pelas entidades bancárias, desses custos com os seus clientes, assumindo a obrigação de serem elas a suportá-los, mas apenas a partir de um determinado limite mínimo. "*An alternative approach, which has been most evident in respect of some consumer-oriented systems, has been to allow the bank to debit the consumer's account for the fraudulent transfer, up to a limit of a relatively small amount*". "A/CN.9/250 and Add.1 to 4", pág. 144.

A necessidade de adoção de um mecanismo seguro de autenticação era também intensificada pela necessidade de diminuir os custos do seu funcionamento, compatibilizando rapidez, segurança e economia de custos.[473]

Existia também a necessidade de maior densificação legislativa das regras de segurança nas mensagens eletrónicas, pela menor adequação do quadro legal aplicável aos documentos em papel.[474] Ponderou-se, inclusivamente, a possibilidade de dispensar a exigência legal de autenticação, deixando para as entidades bancárias e financeiras a definição de mecanismos que assegurem a defesa dos seus direitos em caso de litígio.[475]

Esta problemática refletia apenas a inexistência de instrumentos seguros de autenticação de documentos eletrónicos.[476] [477] Concluiu-se no sentido de que não se deveria prever uma forma obrigatória de autenticação, deixando-se a possibilidade às partes interessadas de escolherem a que entenderem mais adequada aos seus interesses.[478]

3.2. O conceito de autenticação na LMCE.

[473] "*An electronic form of authentication can be verified at an acceptable cost for even the smallest of transactions. Moreover, a well designed authentication system and rigorous adherence to the procedures necessary to keep the system secure can reduce to a minimum the likelihood that the funds transfer instructions containing unauthorized authentications will be honoured*". "A/CN.9/250 and Add.1 to 4", pág. 134.

[474] A perceção dessa necessidade conduziu a que a UNCITRAL apresentasse, pela primeira vez em 1985, um articulado de questões jurídicas emergentes das comunicações eletrónicas de fundos no Guia Legal aplicável à transferência eletrónica de fundos, onde reconhecia essa necessidade: *"Since electronic funds transfers are not carried out in a manner identical to paper-based funds transfers, changes in law to adjust to the new procedures should be expected."* A/CN.9/266/Add.2", pág. 6.

[475] *"It may be thought to be desirable to require by law that all funds transfer instructions, including those in electronic form, must be authenticated. However, it may also be thought to be unnecessary since a bank could not substantiate a debit to an account unless it had a funds transfer instruction in a form on which it could rely in case of later dispute"*. "A/CN.9/266/Add.2", pág. 21.

[476] Essa aparente esperança vem afirmada de forma subliminar no texto do relatório, na parte em que enuncia que os tipos de autenticação então disponíveis são frágeis e rapidamente se podem tornar obsoletos com a evolução tecnológica. *"Can be expected to become weaker while new and more secure forms of authentication can be anticipated"*. "A/CN.9/266/Add.2", pág. 21.

[477] No final da década de 1980 já estavam em curso experiências com soluções tecnológicas que permitissem conferir segurança nas transações eletrónicas em redes abertas, incluindo a autenticação simultânea da origem e da integridade dos documentos eletrónicos. Fala-se, pela primeira vez, do conceito de assinaturas dinâmicas. *"Dynamic signatures analysis by computer and other techniques based on characteristics personal to the individual are in experimental use as a replacement for the PIN"*. "UNCITRAL Legal Guide on Electronic Funds Transfer", pág. 33.

[478] *"Any statutory provision concerning the authentication of an electronic funds transfer instruction should do little more than to authorize the use of means appropriate to the type of instruction involved."*. "A/CN.9/266/Add.2", pág. 21.

Tanto a LMCE como a LMAE postulam a autenticação, como a função que revela a aprovação do conteúdo da mensagem eletrónica pelo seu autor,[479] em razão da necessidade de reforçar o efeito jurídico da vinculação das mensagens eletrónicas expedidas por sistemas automatizados.[480] [481]

O requisito da aprovação separa-se, claramente, da autenticação do emissor da mensagem. Autenticar significa determinar a origem, o autor dessa emissão. O conhecimento acerca da aprovação do conteúdo da mensagem enviada vai para além do conhecimento acerca da pessoa que efetuou o envio, porque entra no domínio do conteúdo da mensagem e da avaliação que dela faz essa pessoa.[482] Na elaboração da LMCE essas duas funções são claramente distintas, mas optou-se por alargar o conceito a ambas, em face da necessidade de conferir segurança à utilização do EDI.[483]

A LMCE não define o conceito de autenticação eletrónica, tal como não define o de assinatura eletrónica. Estava em causa apenas, no contexto da sua elaboração, a equivalência funcional dos suportes eletrónicos ao papel. Mais do que exigências legais

---

[479] A imanência da aprovação ao próprio conceito de autenticação era expressa nos trabalhos preparatórios da LMCE, que a definiam como a segunda função da assinatura, para além da identificação, do seguinte modo: *"One function of a signature was to indicate to the recipient of the document and to third parties the source of the document. A second function of a signature was to indicate that the authenticating party approved the content of the document in the form in which it was issued and intended to be bound by the content of the document"*. "A/CN.9/WG.IV/WP.55", par. 53.

[480] O Grupo de Trabalho considerava ter a assinatura essa dupla função de identificação e de vinculação de uma pessoa a uma mensagem. *"A method that identifies the originator of a data message and confirms that the originator approved the content of that data message"*. "A/CN.9/WG.IV/WP.64", par. 69.

[481] Essas duas funções da assinatura eletrónica estão enunciadas na alínea a) do n.º 1 do artigo 7.º da LMCE: *"a method is used to identify that person and to indicate that person's approval of the information contained in the data message"*. Era esse o sentido consensualizado nos trabalhos preparatórios, que relativamente à norma acima transcrita referiam que: *"focuses on the two basic functions of a signature, namely to identify the author of a document and to confirm that the author approved the content of that document"*. "A/CN.9/426", par. 66.

[482] Essa questão foi objeto de análise na preparação da LMCE. *"In the preparation of uniform rules on the issue of authentication, it might be useful to bear in mind a distinction between the authentication of a message with respect to its source (i.e., the identity of its sender) and the authentication with respect to the content of a message"*. "A/CN.9/373", par. 74.

[483] Era este o entendimento inicial dominante nos trabalhos da UNCITRAL. *"Authentication of a transaction document serves to indicate to the recipient and to third parties the source of the document and the intention of the authenticating party to issue it in its current form. In case of dispute, authentication provides evidence of those matters"*. A/CN.9/WG.IV/WP.53, par. 62. Este entendimento persistia no ano seguinte, mas com o cuidado de se acrescentar uma segunda função, para além da determinação da origem ou da iniciativa do envio, que era a da aprovação do conteúdo: *"One function of a signature was to indicate to the recipient of the document and to third parties the source of the document. A second function of a signature was to indicate that the authenticating party approved the content of the document in the form in which it was issued and intended to be bound by the content of the document"*. "A/CN.9/WG.IV/WP.55", par. 53.

de autenticação, estava em causa conferir relevância jurídica aos suportes eletrónicos, em especial as mensagens de EDI.[484]

E como o EDI era um sistema fechado de comunicações que pressupõe a prévia concertação entre elas, a autenticação, enquanto certeza da origem, está facilitada, pelo que a via mais adequada para o reconhecimento jurídico era a da prevalência do método de autenticação estabelecido por acordo entre as partes.

Consagra-se o primado da autonomia contratual, na alínea a) do n.º 3 do art.º 13.º da LMCE, fazendo prevalecer as convenções de autenticação como instrumento fundamental de autenticação.[485] Não sendo possível transpor as assinaturas manuscritas para os suportes eletrónicos, e na ausência de soluções tecnológicas, esta solução da LMCE equipara as convenções a assinaturas, considerando-se os respetivos documentos assinados.[486] Mas essas técnicas, para além de inseguras e aplicáveis apenas entre agentes económicos com conhecimento prévio entre si, não consistiam em si mesmas numa assinatura.[487] [488]

Para os casos em que não exista esse acordo teria a LMCE que estabelecer também uma previsão, apesar de na época serem escassas essas situações. E não havendo uma solução tecnologicamente sustentada, não podia a LMCE ser muito pormenorizada.

---

[484] A necessidade da existência de meios de autenticação segura das mensagens eletrónicas era expressa em vários textos, como no seguinte trecho: *"As concerns the issues of authentication, it is clear that the legal reliability of EDI techniques requires that high standards be implemented achieving legal certainty as to the identity of the sender, its level of authorization and the integrity of the message"*. "A/CN.9/350", par. 89.

[485] A prevalência das convenções de autenticação entre as partes, que já era frequente nas praticas passou a ser acolhida nos trabalhos da UNCITRAL de forma genérica. *"Although an authentication required by law must be in the form prescribed, an authentication required by the parties can consist of any mark or procedure they agree upon as sufficient to identify themselves to one another"*. "A/CN.9/265", par. 49. Esse princípio perdurou posteriormente, como o mesmo conteúdo em A/CN.9/333", par. 50.

[486] Esta equiparação dos meios de autenticação eletrónicos a assinaturas é muito importante no processo de formação do quadro jurídico da assinatura eletrónica, pelo que a adoção pela UNCITRAL desta solução representa um importante marco histórico. *"The legal problem, therefore, rests primarily with those laws which state that a document must be "signed". Where it is not possible to interpret the law so as to consider an electronic form of authentication as a "signature", it may be desirable either to indicate in the law that an electronic form of authentication is a "signature" or to permit documents to be authenticated" by electronic means"*. "A/CN.9/265", par. 58.

[487] *"Two parties who anticipate communicating frequently by computer-to-computer telecommunications may agree in writing beforehand on the form of the communications and the means to be used to authenticate the documents"*. "A/CN.9/265", par. 54.

[488] Chegou a utilizar-se o conceito de "qualquer acordo pertinente", no projeto de redação da parte final da alínea b) do n.º 1 do artigo 7.º da LMCE. *"The notion of an "agreement between the originator and the addressee of a data message" is to be interpreted as covering not only bilateral or multilateral agreements concluded between parties exchanging directly data messages (e.g. "trading partners agreements") but also communication agreements (e.g. "third-party service agreements") involving intermediaries such as networks"*. "A/CN.9/WG.IV/WP.64", par. 73.

A primeira opção foi reportar o método de autenticação para as circunstâncias de cada caso. Ponderou-se que a LMCE utilizasse o conceito de *"autenticação comercialmente razoável"*, em vez de se estabelecer um tipo de assinatura nas comunicações eletrónicas como instrumento de autenticação.[489] Defendia-se que a previsão legal deveria ser suficientemente abrangente para admitir qualquer forma de autenticação, desde que ela seja adequada ao tipo de relação jurídica estabelecida e à necessidade de segurança em cada operação em concreto.[490] Nessa linha, as partes poderiam adotar entre si métodos adequados ao tipo de relações que estabeleciam, sem necessidade de a lei impor um método específico,[491] sendo que esses métodos podiam consistir numa mera indicação da origem, tal como ocorria no contexto do papel.[492],

O reporte para o conceito de *"autenticação comercialmente razoável"* apela a um conjunto vasto de circunstâncias, incluindo a natureza das operações realizadas, a dimensão dos intervenientes, o valor e a dimensão das transações, a existência, ou não, de uma convenção prévia de autenticação, a capacidade dos seus sistemas informáticos, a disponibilidade de outros meios de autenticação, etc.[493]

Do que se trata é de conferir relevância jurídica às comunicações eletrónicas, reportando para os casos em concreto a apreciação da prova da vinculação, nos casos em que a autenticidade seja colocada em causa[494] Estabelece-se um mínimo denominador comum em termos tecnológicos, que não exclui nenhuma forma possível de autenticação dos documentos eletrónicos, incluindo aquelas que era já então

---

[489] Como se referia nos trabalhos preparatórios, *"There existed a need to eliminate the mandatory requirements of signatures in EDI communications. It was also agreed that there existed a need to promote the use of electronic authentication procedures regarding the source and the content of EDI messages, and that such procedures should be adapted to the nature of the message"*. "A/CN.9/WG.IV/WP.55, par. 57.

[490] Preferia-se uma formulação maleável e ajustada a cada situação em concreto, em vez de uma modelo rígido. *"It was also agreed that there existed a need to promote the use of electronic authentication procedures regarding the source and the content of EDI messages, and that such procedures should be adapted to the functions served by an electronic message"*. "A/CN.9/333", par. 75.

[491] Era esse o propósito consignado nos trabalhos preparatórios. *"Parties should be allowed to determine the nature of such authentication procedures within the realm of commercial reasonableness. Wide support was given to the idea that legislative provisions might be needed to establish the principle of "commercial reasonableness"*. "A/CN.9/WG.IV/WP.55", par. 57.

[492] Na verdade a assinatura dos documentos não é uma necessidade universal. *"However, it may be noted that in the context of EDI communication as in the context of paper-based communication, commercial partners should be free to exchange information that is not authenticated but merely bears an indication of origin (e.g., a letterhead)"*. "A/CN.9/WG.IV/WP.55", par. 51.

[493] Um elenco completo de elementos que podem integrar o conceito de autenticação comercialmente razoável consta do document de trabalho *"A/CN.9/WG.IV/WP.55"*, par. 59.

[494] *"It was stated in reply that the notion of "commercial reasonableness" was useful in that it provided a minimum standard of authentication to be complied with in the absence of other requirements resulting from contractual arrangements or regulatory requirements"*. "A/CN.9/373", par. 68.

expectável que se viessem a desenvolver no futuro,[495,] mas assegurando ao mesmo tempo a não discriminação dos suportes eletrónicos.[496] [497] A preocupação não era ainda estabelecer um elevado nível de segurança jurídica, mas habilitar os suportes tecnológicos a possuírem idoneidade jurídica para a documentação dos negócios e dos atos jurídicos. Tratava-se então era de eliminar as barreiras jurídicas à expansão da utilização do EDI nas atividades empresariais.[498]

Na redação final da LMCE não ficou consagrada nenhuma referência ao conceito de autenticação comercialmente razoável mas, com uma formulação idêntica, a alínea b) do n.º 1 do art.º 7.º estabeleceu que um documento eletrónico se considera assinado, cumprindo por isso os requisitos legais de assinatura, quando o método utilizado para identificar a pessoa é o apropriado para os fins em razão dos quais a mensagem eletrónica foi gerada ou comunicada.[499]

O problema, também aqui, é o de determinar com se apura esse carácter apropriado dos métodos de autenticação utilizados e a sua razoabilidade em função do fim a que se destina a mensagem, bem como quem possui a competência para apurar

---

[495] *"It may be thought less appropriate for the form of the authentication to be specified, as signature has often been specified in the past, since there are many possible means to authenticate an EDI message and new means will evolve in the future"*. "A/CN.9/WG.IV/WP.55", par. 53.

[496] *"Thus, article 6 may be regarded as establishing a minimum standard of authentication for EDI messages that might be exchanged in the absence of a prior contractual relationship"*. "A/CN.9/WG.IV/WP.64", par. 72.

[497] Como se referia nos trabalhos preparatórios da UNCITRAL, em 1990, existiam já diversas técnicas de autenticação utilizadas pelos agentes económicos. *"Some new techniques have been developed to authenticate electronically transmitted documents. As regards identification of the transmitting machines, telex and computer-to-computer telecommunications often employ call back procedures and test keys to verify the source of the message"*. "A/CN.9/333", par. 54. Dois anos mais tarde, além das técnicas tradicionais falava-se já nas assinaturas digitais. *"The methods ranged from a technically simple verification of the address of the owner of the computer that had sent or received a message to sophisticated "digital signatures". Some of those methods were designed to verify only the source of the message, while others could verify both the source of the message as well as whether the message received was identical to the message sent"*. "A/CN.9/360", par. 114.

[498] Tal como consta dos trabalhos preparatórios, o objetivo desta definição de assinatura era apenas o de estabelecer um modelo mínimo de autenticação: *"as establishing a minimum standard of authentication for EDI messages"*. "A/CN.9/426", par. 69.

[499] Tentando densificar o conceito de meio técnico apropriado, nos trabalhos preparatórios foram identificados um conjunto de 14 fatores jurídicos que deveriam ser tidos em conta para se avaliar da adequação dos métodos de autenticação utilizados. Alguns desses fatores que anteriormente reproduzimos, e que nos dispensamos de repetir, que constam do "A/CN.9/WG.IV/WP.55", par. 59, são acrescentados os relativos ao nível técnico dos sistemas informáticos utiulizados pelas partes, e ainda os seguintes: *" (9) compliance with trade customs and practice; (10) the existence of insurance coverage mechanisms against unauthorized messages; (11) the importance and the value of the information contained in the data message; (12) the availability of alternative methods of identification and the cost of implementation; (13) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and (14) any other relevant factor"*. "A/CN.9/426", par. 68.

essa fiabilidade. [500] Não havendo métodos seguros, ficaria sempre na margem de livre apreciação dos tribunais essa decisão, em caso de litígio, mas o objetivo mais importante da LMCE era a equivalência e não discriminação.

Reconhecia-se já a necessidade de uma hierarquia legalmente tipificada de formas de autenticação, que em função dos seus graus de segurança confira aos respetivos documentos uma força probatória proporcional e legalmente consagrada.[501] E essa hierarquização, nomeadamente para efeitos probatórios, é importante para que as partes possam por elas optar, tendo também em conta os respetivos custos, financeiros ou outros, nomeadamente temporais.[502]

Essa hierarquia não podia estabelecer-se, porém, enquanto não estivessem disponíveis meios de autenticação tecnologicamente seguros, e é essa a razão pela qual a LMCE não a estabelece.[503]

No trabalhos de elaboração da LMCE foram ponderadas várias possibilidades de adoção de uma definição de autenticação, desde a invocação de um qualquer procedimento,[504] à mera indicação do nome.[505] Mais tarde, já em 1994, mantinha-se a

[500] A LMCE considera assinado um documento eletrónico ao qual tenha sido aplicado um método de identifique o autor e a sua aprovação do conteúdo, quando esse método seja fiável à luz dos fins para que o documento foi gerado: *"that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement"* (alínea b) do n.º 1 do artigo 7.º). O problema que aqui se levanta é o da determinação da fiabilidade do método, nomeadamente no que respeita ao conceito definidor dessa fiabilidade e à competência para a sua determinação. Esta questão foi levantada pela Banking Federation of the European Union, nos comentários que enviou, ao projeto de LMCE. *"Who decides whether this method is reliable?"*. "A/CN.9/409", pág. 15.

[501] *"The identification of uniform criteria is particularly needed in view of the possibility that national authorities might provide different types of authentication procedures or different criteria by which to measure the adequacy of each type of authentication of EDI messages in use"*. "A/CN.9/WG.IV/WP.55", par. 53.

[502] As vantagens dessa hierarquização eram reconhecidas nos trabalhos da UNCITRAL. *"It might be desirable to develop functional equivalents for the various types and levels of signature requirements in existence. Such an approach would increase the level of certainty as to the degree of legal recognition that could be expected from the use of the various means of authentication used in EDI practice as substitutes for "signatures""*. "A/CN.9/426", par. 65.

[503] Essa ausência de meios técnicos capazes de formarem o quadro de contexto que permitisse essa hierarquização é reconhecida nos trabalhos da UNCITRAL. *"However, the notion of signature is intimately linked to the use of paper and there might exist no technical solutions for accommodating all existing types and uses of "signature" in a dematerialized environment"*. "A/CN.9/426", par. 65.

[504] Foi formulada a seguinte sugestão: *"Any method of authentication which purports to have been used by or on behalf of that person shall be a sufficient authentication for that purpose"*. "A/CN.9/373", par. 76.

[505] *"Any method of authentication which purports to have been used by or on behalf of that person in place of signature shall be treated as a sufficient authentication." Ibidem*.

sugestão de uma definição aberta,[506] mas já era manifesta a necessidade de maior segurança jurídica.[507]

3.3. A autenticação e identificação nas redes abertas

Nas redes abertas, a problemática da autenticação não tem por objeto apenas os documentos. Ela alarga-se também à identificação das pessoas.

A Internet e as chamadas redes sociais não se limitam atualmente à comunicação de suportes documentais. A generalização da utilização das redes abertas alterou o paradigma inicial das redes eletrónicas, marcado pelo EDI e pela transmissão das mensagens. Atualmente as redes abertas são espaço público, mais do que canais de comunicação. Locais de presença, de manifestação, de expressão e de cidadania.

As redes eletrónicas são atualmente uma extensão do espaço público ao domínio da eletrónica.[508] Como afirma Roques-Bonnet, vivemos atualmente numa espécie de e-República, em que a Internet se assume, cada vez mais, como uma espécie de *ágora* que estava na base da polis da antiga Grécia, espaço privilegiado do exercício da cidadania e de participação na vida social.[509]

Essa transformação do papel das redes eletrónicas na atividade social e económica produz uma importante transformação no modo de juridificação dessas relações.[510]

---

[506] *"Authentication means a procedure to determine whether a data message was issued by the person indicated as the originator."* "A/CN.9/406", par. 155.

[507] *"Authentication means a process by which a communicating party obtains information that gives assurance that a message received from another communicating party: "(a) originates from that party; and "(b) is received with [exactly] the same information content as when it was forwarded by that party"*. *Ibidem.*

[508] Como refere Gálvez, *"Está emergiendo uma nueva cultura: Telépolis"*. Gálvez, J.F.P. (2007). Incidencia de las Nuevas Tecnologías en el Procedimiento Administrativo Español. Em: Parra, A.M (dir). e Lebrón, M.J.G (Coord). *Derecho Patrimonial e Tecnología*. Marcial Pons, Ediciones Jurídicas. Madrid., página 602.

[509] Citando a autora, *"L'Internet offre la perspective d'une sorte d'agora, une place publique, como dans la polis grécque où chacun descendait quando bon lui semblait pour discuter avec le tout-venant des affaires de la cité, et où se formait la l'opinion des citoyens"*. Roques-Bonnet, M.C. (2010). Op. cit, pág. 135.

[510] Na lição de Habermas, a sociedade da informação atual implantou *"uma simultaneidade abstracta de uma rede virtualmente sempre presente de conteúdos de comunicação muito afastado no tempo e no espaço e colocando as mensagens de todos à disposição de contextos multiplicados".* Habermas, J. (2003). *Teoría de la Acción Comunicativa*. Santillana Ediciones Generales. Madrid, paginas 552 e 553.

No que respeita à identificação dos documentos, não basta que a ordem jurídica faça apelo às convenções de autenticação estabelecidas entre as partes, dado que a inovação das redes abertas é a possibilidade de se estabelecerem relações jurídicas com pessoas que não se conhecem, com as quais não existe aquela convenção.

Relativamente às pessoas, a possibilidade de se efetuarem transações eletrónicas com relevância jurídica torna indispensável a sua identificação e vinculação jurídica a essas transações, em especial nos casos em que essas transações não são suportadas em documentos eletrónicos.

Quando disponibilizamos os elementos informativos da nossa identificação numa transação eletrónica, ela só é confirmada pela outra parte se constatar, por confronto desses elementos com a sua origem, que eles são verdadeiros. Ora, os elementos informativos da nossa identificação não são gerados por nós, mas pelas autoridades administrativas competentes que são as entidades do registo civil e dos serviços de identificação. Essas entidades emitem documentos contendo esses elementos para poderem ser exibidos, como é o caso do documento de identidade. Essa operação consiste na determinação da origem desses elementos informativos da identificação. E essa operação designa-se de autenticação, garantindo que aquela pessoa é quem afirma ser.

Em muitos sistemas informáticos, essa autenticação é efetuada mediante uma palavra-passe, sendo a introdução desse código solicitada pelo sistema informático, depois de o utilizador inserir o seu nome.

Nestes casos, em que a palavra-passe assenta num criptograma simétrico, ela é gerada por uma das partes, normalmente aquela que vai receber informação por via eletrónica de outra parte, procedendo, de seguida, à sua entrega a esta (remetente). A geração desse código é efetuada mediante uma convenção prévia de identificação, em que o remetente entrega ao destinatário os elementos de identificação, que o destinatário guarda, gerando, de seguida, a palavra-passe, que entrega ao remetente. A partir daí, este utilizá-la-á para se identificar nas comunicações que efetuar para o destinatário.

Nas comunicações que efetuar, o remetente identifica-se perante o sistema informático que a vai receber. Quando o sistema informático recebe o nome do utilizador e a palavra passe, confirma que ambos estão associados e autentica, deste modo, a informação acerca do nome que o utilizador havia fornecido. A partir daí pode ser estabelecida uma sessão segura, porque as transações que forem efetuadas (que consistem em informação trocada em suporte eletrónico) podem ter relevância jurídica,

porque é suscetível de vinculação ao respetivo autor, ou seja, está autenticada, porque se conhece com rigor a sua origem.

A autenticação da identificação eletrónica consiste na confirmação, mediante um protocolo informático, da origem da informação relativa aos elementos que identificam uma pessoa, ou seja, aos seus atributos. Essa confirmação é efetuada mediante um processo inverso, a partir dos elementos informativos invocados pela pessoa, até à sua origem, sendo esta, em última instância, uma autoridade pública competente para a identificação ou um seu sucedâneo.

A identificação eletrónica pode ser também obtida mediante a utilização do certificado da assinatura eletrónica de uma pessoa, dado que as assinaturas eletrónicas identificam, também elas, os signatários. E embora se trate de transações não suportadas em documentos, que portanto não necessitam de ser assinadas eletronicamente, pode-se utilizar a função de identificação do signatário constante do dispositivo de assinatura eletrónica, para se obter a sua identificação eletrónica.

Quando se utiliza como sistema de autenticação uma assinatura avançada ou qualificada, para os fins da identificação eletrónica, o utilizador disponibiliza ao sistema informático do seu computador, o suporte onde se encontra a sua chave privada e o certificado. De seguida o sistema efetua a geração de um documento eletrónico de forma automatizada, que pode ser um suporte informativo não formal, mas apenas um mero pretexto para servir de suporte à encriptação. Esse documento é assinado com a chave privada, sendo nele colocado o certificado de assinatura eletrónica emitido pela entidade que gerou o par de chaves, e do qual consta a identificação do respetivo titular. Essa identificação é segura porque a entidade que emite o certificado é prestadora de serviços de confiança e autenticou, ela própria, esses dados quando gerou o par de chaves.

A partir daí, o sistema informático reconhece que todas as transações que forem efetuadas o estão a ser com uma pessoa identificada, existindo segurança acerca da sua identificação.[511]

---

[511] Santiago Segarra Tormo enuncia que *"os serviços que oferece o servidor de páginas Web da administração fiscal espanhola podem ser classificados em serviços personalizados e serviços abertos. Para estes é irrelevante conhecer quem acede ao serviço. Nos serviços personalizados é necessário identificar electronicamente o usuário. Para isso utilizam-se os certificados de identificação digital emitidos por uma autoridade de certificação"*. Tormo, S.S. (2004). Utilización de la Firma Electrónica en la Administración Española I: La Agencia Estatal de la Administración Tributaria. Em: Ministerio de Economia. Administración Electrónica y Procedimiento Administrativo. Real Casa de la Moneda. Madrid.

Estes procedimentos são efetuados de forma automatizada pelos sistemas informáticos, nomeadamente pelos *sítios web* com os quais os clientes das empresas ou os cidadãos operam.

O processo de identificação nas redes abertas é, na sua essência, um processo de autenticação dos dados de informação acerca da identificação de uma pessoa. Mas isso não converte a função de identificação na função de autenticação, porque uma coisa é a autenticação dos elementos identificadores de uma pessoa, que designamos identificação e outra coisa, de natureza diferente, é a determinação da autenticação de um documento gerado por essa pessoa. É certo que em ambos os casos, do que se trata é de determinar a origem de dados informativos, mas a função e os efeitos são diferentes.

3.4. O conceito de autenticação no Regulamento EIDAS

O Regulamento EIDAS veio operar uma importante evolução na definição legal do conceito de autenticação. Enquanto a diretiva de 1999 postulava a autenticação como a função principal da assinatura eletrónica, o regulamento opera uma separação desse conceito.

Embora muitas vezes os instrumentos sejam idênticos, a verdade é que a autenticação de um documento e da identidade de uma pessoa são realidades distintas. A assinatura é um instrumento de mediação e de vinculação entre um documento, que é uma entidade autónoma da pessoa, e a própria pessoa.

O conceito de identidade eletrónica autonomiza-se do de assinatura eletrónica e é mais abrangente do que ela, sendo que esta se deve limitar à sua função natural que é a de autenticar documentos eletrónicos.

É essa uma das mais importantes inovações do Regulamento. Ao contrário dos restantes diplomas legislativos até então existentes, que se centravam na assinatura eletrónica como instrumento de segurança jurídica nas transações eletrónicas, o Regulamento centra-se antes na identificação eletrónica, sendo esta o pilar fundamental dos chamados serviços de confiança eletrónica, que incluem, também:[512]

i) As assinaturas eletrónicas;[513]

[512] Os serviços de identificação eletrónica são regulados no capítulo II do regulamento, artigos 6.º a 12.º.
[513] Reguladas na secção 4 do capítulo III, artigos 25.º a 34.º.

ii) Os selos eletrónicos, que são instrumentos eletrónicos de autenticação de documentos gerados por pessoas coletivas;[514]

iii) Os selos temporais, que servem para conferir segurança acerca da data da prática de atos. São importantes nas assinaturas eletrónicas, porque os instrumentos da sua criação, sendo objetos, podem ter validade limitada e podem ser suspensos ou revogados. Os selos temporais certificam a data e a hora da aplicação da assinatura, mas podem certificar outros acontecimentos, incluindo a data de envio de uma comunicação, a data da sua receção ou a data de uma autenticação;[515]

iv) Os documentos eletrónicos;[516]

v) Os serviços de envio eletrónico registado, que asseguram o envio de comunicações eletrónicas, mediante uma certificação de envio, garantida por uma entidade terceira e;[517]

vi) A certificação dos sítios web, que garante a identidade e a segurança de determinados *sites*.[518]

O Regulamento engloba estes serviços na categoria de serviços de confiança eletrónica, correspondente ao universo de necessidades de segurança jurídica na utilização dos meios eletrónicos no atual contexto tecnológico.

Nesta nova configuração legal, a autenticação é definida pelo regulamento, de forma mais genérica como *"o processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou coletiva ou da origem e integridade de um dado em formato eletrónico a confirmar"*.[519]

O conceito de autenticação alarga-se a todos os serviços de confiança eletrónica e a todos os tipos de dados que possam circular na rede e nos meios eletrónicos, incluindo os dados relativos à identificação de uma pessoa ou à sua assinatura. O conceito de assinatura é definido como o instrumento de verificação da identificação, da determinação de origem e da garantia de integridade dos dados.

A inclusão da função de determinação da integridade dos dados no conceito de autenticação tem como efeito uma exigência mais elevada de segurança, o que, na

[514] Os selos eletrónicos são regulados na secção 5 do capítulo III do regulamento, artigos 35.º a 40.º
[515] Regulados na secção 6 do capítulo III do regulamento, artigos 41.º e 42.º.
[516] Previstos no capítulo IV do regulamento, artigo 46.º.
[517] Regulados na secção 7 do capítulo III do regulamento, artigos 43.º e 44.º.
[518] Regulados na secção 8 do capítulo III do regulamento, artigo 45º.
[519] N.º 5 do artigo 3.º do regulamento.

prática, limita os tipos de instrumento de segurança eletrónica à tecnologia da assinatura digital.

Neste novo contexto, o conceito de assinatura reconduz-se à sua função original de assinar documentos, e o regulamento define esse conceito como *"os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar"*.[520]

É esta ligação entre os dados pessoais da assinatura, que é a chave privada e a pessoa do seu titular, que é assegurada por uma entidade competente, e entre esses dados e os dados de um documento determinado, que é também assegurada por essas entidades, que asseguram a vinculação de uma pessoa a um documento. Esse documento é sempre um conteúdo de dados, qualquer que ele seja, e independentemente do fim para que sirva, dado que o que é relevante é a segurança da vinculação da objetividade dos dados à pessoa que a eles se decidiu vincular.

Os meios tecnológicos de confiança eletrónica, que proporcionam a segurança de autenticação exigida pelo Regulamento são os mesmos que analisámos a propósito da assinatura eletrónica, com destaque para a assinatura digital. Esses meios são utilizados, da mesma forma, nomeadamente, para a identificação eletrónica e para a autenticação dos sítios *web* e só se tornaram disponíveis com a tecnologia das assinaturas digitais, que permite a conexão segura entre dados e pessoas. Por essa razão, a partir do momento em que existe esta tecnologia disponível nos mercados, a ordem jurídica passou a poder densificar de forma mais rigorosa o conceito de autenticidade, adaptando-o às finalidades dos diversos serviços de confiança eletrónica atualmente existentes.

Quando se trata da autenticação de documentos mediante a assinatura eletrónica, essa autenticação é dupla. Por um lado autentica-se a identidade do signatário, verificando-se, através do certificado, e mediante a informação nele disponibilizada pelo prestador de serviços de confiança, se a identidade invocada pelo signatário corresponde à que consta do certificado. E como a que consta do certificado resulta, em última instância, daquela que advém das entidades públicas competentes para a identificação, fica determinada a origem dessa informação e a sua credibilidade. É essa operação metodológica de desconstrução inversa, até à origem, da informação relativa à identificação, que se designa de autenticação da identidade do signatário.

[520] N.º 10 do artigo 3.º do regulamento.

Por outro autentica-se o próprio documento, mediante a ligação dos dados que o compõem aos dados da criação da assinatura eletrónica. Tanto o documento como o instrumento de assinatura (a chave privada e o mecanismo de *hash*) são dados separados, que uma vez submetidos a um ato de assinatura eletrónica produzem um novo conjunto de dados. A autenticação do documento eletrónico consiste em idêntica metodologia de desconstrução inversa do procedimento de assinatura, usando-se a chave pública para se desencriptar o *hash* encriptado e aceder à chave de criação deste, criando-se, de seguida, um novo *hash*, assim se determinando que os dados do documento que deram origem ao *hash* encriptado são exatamente os mesmos.

Assim, a função de autenticação da assinatura eletrónica é, na verdade, uma dupla autenticação de dados, fazendo parte de uma ação jurídica que designamos de verificação e de validação da assinatura eletrónica (artigo 32º do Regulamento EIDAS), que analisaremos no capítulo VI da Parte II.

4. A função de garantia da integridade do documento

A segurança jurídica acerca dos documentos eletrónicos não se alcança apenas com a autenticação desses documentos e da identificação do seu autor. É também necessário que o próprio conteúdo do documento seja autenticado, de tal forma que os agentes económicos adquiram a confiança de que o seu conteúdo é exatamente o mesmo que foi gerado pela pessoa que a ele se vinculou quando o assinou.

A segurança jurídica acerca da identidade e do vínculo estabelecido entre uma pessoa e um documento deve ser acompanhada da segurança da perenidade dessa autenticação. E para isso é necessária a certeza de que o documento não foi alterado ou falsificado depois da sua assinatura ou da colocação do instrumento de autenticação. É ainda necessário que se garanta que em caso de alteração ou falsificação, seja possível a sua deteção por qualquer interessado. A integridade corresponde, assim, a uma garantia dinâmica de autenticidade, que acompanha o documento ao longo da sua existência.

A integridade foi logo considerada importante na LMCE, mas a sua enunciação era ainda relativamente vaga.[521] Os meios tecnológicos que não permitiam autenticar,

[521] A relevância da integridade era já assinalada no relatório do Secretário-Geral, de 1985, que analisa o valor jurídico dos registos eletrónicos, referindo que a autenticação também envolve o pressuposto da intencionalidade da parte que faz a autenticação, de emitir o documento "*na forma actual*", ou seja, com o conteúdo exato que ele possuía na data da assinatura. É aqui manifesta a preocupação acerca da

não garantiam também a integridade, e este é mais um constrangimento na definição do conceito de autenticação que deveria constar da LMCE. [522]

Por essa razão a LMCE adotou uma solução legislativa assente numa presunção de que a mensagem recebida pelo destinatário continha o mesmo conteúdo tal como foi enviada pelo emitente, não tendo sofrido qualquer alteração entretanto.[523] Partia-se do princípio de que a informação constante de um documento permanece completa e inalterada desde a sua geração, com exceção dos endossos e das alterações inerentes ao seu processo de comunicação, arquivo e de apresentação.[524]

O problema da integridade é maior nos documentos eletrónicos do que no papel, desde logo pela facilidade com que aqueles se podem alterar e isso aproxima, no paradigma eletrónico, o problema da integridade do da identificação e da autenticação, ou seja, da assinatura.[525] Por essa razão a integridade é um conceito fundamental no direito da segurança eletrónica.[526]

---

importância que a inalterabilidade dos documentos autenticados possui nos casos em que o seu suporte é o eletrónico. *"Authentication of a transaction document serves to indicate to the recipient and to third parties the source of the document and the intention of the authenticating party to issue it in its current form"*. "A/CN.9/265", par. 49.

[522] No paradigma do papel não existe qualquer instrumento efetivo que garanta a inalteração de um documento após a sua autenticação. A deteção de alterações ou falsificações pode ser efetuada visualmente, mas dificilmente existirá garantia absoluta dessa deteção. Mesmo os mecanismos utilizáveis para os documentos eletrónicos, não podiam ser aplicados aos documentos em papel. *"However, since those techniques are available only by use of computers, they are available neither for those electronic funds transfers which do not rely on the use of computers nor for paper-based funds transfers"*. "A/CN.9/250 and Add.1 to 4", pág. 133.

[523] Essa presunção foi objeto de acordo nos trabalhos da Comissão, no ano de 1991. *"The Working Group decided that, in its discussion of article 4, it would consider issues having to do with verification that the contents of a payment order as received were the same as the contents of the payment order as sent"*. A/CN.9/346), pág. 61. O emissor de uma ordem de pagamento é, assim, responsável pelo seu conteúdo tal como foi recebido pelo destinatário. A definição de autenticação, nesta versão limitada à certificação da origem, foi mantida nos trabalhos seguintes. A/CN.9/341, em especial os par.s 81 (pág. 152) e o par. 102 (pág. 154).

[524] A alínea a) do n.º 3 do artigo 8.º da LMCE ficou com a seguinte redação: *"The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display"*. "Guide to Enactment LMCE (1996)", pág. 6.

[525] Apesar disso, a assinatura manuscrita feita num documento em papel não garante, também ela, de forma universal, capacidade para se detetar a sua integridade. *"A handwritten signature provided neither a guarantee of the integrity of the document to which it was attached nor a guarantee that any change made to the document would be detectable"*. A/CN.9/467, par. 73.

[526] A introdução de uma definição do conceito de integridade foi considerada e abandonada nos trabalhos preparatórios da LMAE, mas a base dessa definição era consensual em redor da proposta apresentada pelos EUA, centrada nos conceito de permanência da completude do documento e da sua inalteração: *"The criteria for assessing integrity shall be whether the infonnation has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display"*. "A/CN.9/WG.IV/WP.77", pág. 5. O requisito da integridade foi sinteticamente definido num dos documentos mais recentes da UNCITRAL, como a garantia de que um documento eletrónico permanece "completo e inalterado". *"To remain complete and unaltered"*. "A/CN.9/804", par. 29.

A função da integridade tem como finalidade garantir a inalteração de um documento depois da sua assinatura pelo seu autor ou subscritor, ou então a deteção dessas eventuais alterações quando tenham ocorrido. A integridade reporta-se ao documento, incluindo à sua forma e ao seu conteúdo, à sua essencialidade e à sua substância. Foi sobre ele que se projetou a vontade de vinculação do titular da assinatura quando o assinou, e é a salvaguarda do respeito por essa vontade que a função da integridade visa proteger.

Não é uma função relacional, como o é a função da assinatura eletrónica, na sua essência, mas apenas uma função de segurança relativamente ao conteúdo e à forma, objetivados de um documento. A integridade é um dado, objetivo e de segurança, uma constatação de permanência e de inalteridade.

A integridade protege o autor ou subscritor do documento contra as adulterações que tenham em vista estender a sua vinculação para além do âmbito da sua vontade expressa pela sua assinatura, mas protege também o destinatário contra situações de repúdio pelo autor ou subscritor, com fundamento na alegada alteração posterior do documento assinado. Não existindo segurança contra essa alteração, existirá sempre vulnerabilidade relativamente à possibilidade de repúdio pelo autor ou subscritor.

A importância que a integridade desempenha na confiança dos agentes económicos na utilização dos meios eletrónicos é uma das razões que conduziram a que ela fosse incorporada como uma das funções de alguns tipos de assinaturas eletrónicas.

Mesmo depois de se instituir a assinatura eletrónica como um instrumento fundamental dos documentos eletrónicos, persiste o problema da segurança jurídica em razão da possibilidade de alteração dos documentos. E a resolução deste problema é indispensável para que exista confiança na utilização dos meios eletrónicos, em especial no contexto das redes abertas.

O efeito de segurança da assinatura eletrónica no que respeita à vinculação do seu autor seria eliminado logo de seguida, se não fosse resolvido o problema da integridade dos documentos. Por essa razão, em termos funcionais, as funções da assinatura eletrónica e da integridade dos documentos estão associadas.

Foram estes problemas que conduziram a que algumas tecnologias de assinatura eletrónica passassem a incorporar nas suas funções, também a resolução do problema da integridade, como é o caso das assinaturas digitais. O destinatário de um documento eletrónico constata, mediante a aplicação da chave pública, quem foi a

pessoa que assinou o documento, mas ao mesmo tempo, constata também se esse documento foi alterado, uma vez que o sistema informático, ao mesmo tempo que desencripta o resumo do *hash*, determina imediatamente se ocorreu alguma alteração no documento após a sua assinatura e assinala esse facto.

A deteção das eventuais alterações aos documentos, ocorridas depois da assinatura é efetuada mediante a aplicação da chave simétrica que esta inserida no *hash* encriptado, ao documento em claro. Essa aplicação repete aquela que foi efetuada pelo autor e produz um novo *hash*, que deverá ser exatamente igual ao que aquele criou. Se o for está garantida a integridade, caso contrário o documento foi alterado depois da assinatura e esta não será válida. Estas operações são efetuadas automaticamente pelos sistemas informáticos e assinaladas de imediato aos respetivos utilizadores.

Nas assinaturas digitais, a determinação da integridade de um documento é efetuada em simultâneo com a determinação da sua autenticidade e da identificação do seu autor ou subscritor. Essa deteção é inerente ao próprio procedimento de determinação da autoria.

Essa simultaneidade não existe nos restantes tipos de assinatura eletrónica, como é o caso da utilização das palavras-passe ou dos métodos biométricos, nem tem que existir, porque a função da integridade do documento não é uma função própria da assinatura.

A função de integridade não é essencial à assinatura.[527] Ela projeta-se apenas sobre o documento e por isso é de natureza apenas objetiva e não relacional. Nos suportes eletrónicos esta função compara o estado dos documentos entre dois momentos, aquele em que foram assinados e cada um dos momentos posteriores em que foram alterados, a fim de detetar eventuais alterações à sua forma e conteúdo. Por essa razão, tanto em termos temporais como em termos concetuais, a integridade é uma função posterior e externa à assinatura.[528] A integridade é um requisito do documento, não um requisito da assinatura.

Por essa razão, foi contestada, no contexto de elaboração da LMAE, a necessidade de o requisito da integridade dos documentos constar da legislação que

[527] Esta separação era clara desde logo nos trabalhos preparatórios da LMAE: *"While verification of data integrity was an important result of the use of the certificate in the context of a digital signature process, it was not a characteristic element of the certificate itself"*. "A/CN.9/446", par. 72.

[528] A LMAE reporta a integridade apenas à mensagem e não se refere a esse conceito na definição do regime da assinatura especificamente. Essa foi uma opção analisada e consensualizada nos trabalhos preparatórios: *"After discussion, however, it was generally agreed that the Uniform Rules should focus on the integrity of the message only"*. "A/CN.9/454", par. 56.

regula a assinatura eletrónica.[529] Essa contestação fundamentou-se na sua desnecessidade e também no princípio da neutralidade tecnológica, dado que a única tecnologia que naquela data garantia o controlo da integridade dos documentos era a da assinatura digital. Fundamentou-se também no facto de a assinatura manuscrita não garantir, de forma necessária, e na sua essência, a integridade dos documentos em suporte de papel. Essa contestação teve sucesso, e a definição de assinatura eletrónica e o seu regime não estabelecem a integridade como requisito da sua validade, tal como não consta nem é garantido pelas assinaturas manuscritas.[530]

O problema é que apesar de a assinatura cumprir a sua função nos documentos eletrónicos, a sua eficácia como instrumento de segurança jurídica poderá ser escassa, se não for possível assegurar também a integridade do respetivo documento. A vulnerabilidade destes documentos a alterações com elevado nível de perfeição é muito elevada, e isso torna-os vulneráveis também à insegurança, nos casos em que não seja possível detetar essas alterações posteriores à assinatura.

Para que os documentos eletrónicos possam ser utilizados no tráfego jurídico com o mesmo nível de segurança dos documentos em papel, é necessário que se garanta a sua integridade, para além, naturalmente, da identidade do seu autor ou subscritor, bem como da sua autenticidade. Mas sendo esse um requisito dos documento em si mesmo, não tem que afetar a eficácia das assinaturas eletrónicas nem que as discriminar. A integridade é um requisito de equiparação de documentos em formato eletrónico a documentos em papel, nos casos em que a lei contém exigência formal de assinatura, não um requisito de equivalência de assinaturas em cada um desses formatos. Por essa razão o princípio da equivalência funcional é aplicado aos documentos eletrónicos que cumprem o requisito da integridade, fazendo-os equivaler aos documentos originais em papel.[531]

---

[529] Essa questão foi levantada em várias ocasiões, das quais destacamos a seguinte referência: *"It was observed that including the requirement for integrity of the information in draft article 6 suggested the use of one particular technology, which would be inconsistent with the principle of technology neutrality"*. "A/CN.9/467", par. 74.

[530] Essa especificação consta do próprio Guia de Transposição da LMAE: *"Since a handwritten signature provides neither a guarantee of the integrity of the document to which it is attached nor a guarantee that any change made to the document would be detectable, the functional equivalence approach requires that those concepts should not be dealt with in a single provision"*. "UNCITRAL Model Law ... 2001", par. 124.

[531] Um documento eletrónico que cumpre os requisitos da integridade corresponde a um documento original, dado que a exigência da originalidade dos documentos em papel é um instrumento destinado a garantir essa mesma integridade naquele suporte. *"It links the concept of originality to a method of authentication and puts the focus on the method of authentication to be followed in order to meet the requirement. It is based on the following elements: a simple criterion as to "integrity" of the data; a*

Ora, os requisitos de integridade podem ser cumpridos mediante a utilização de um ou vários instrumentos que a assegurem. E um desses instrumentos podem ser as próprias assinaturas.

A integridade do documento distingue-se da integridade da assinatura. A assinatura de um documento é, no seu núcleo essencial, e segundo o modelo da assinatura digital, o *hash* encriptado com a chave privada do seu autor ou subscritor. Este produto encriptado é assinalado no documento assinado, com um símbolo que está associado a ele. Esta assinatura serve só para aquele documento em concreto, e não pode ser utilizada em qualquer outro documento. Se o for perde a sua integridade, por exemplo, mediante cópia do ficheiro de onde consta o símbolo da assinatura, para outro documento diferente, sendo certo que a deteção dessa perda é relativamente simples.

Pelo próprio modo de funcionamento das assinaturas digitais, sempre que se perde a integridade da assinatura perde-se a integridade do documento.[532] Mas nas outras modalidades de assinatura é possível que seja quebrada a integridade do documento sem que se quebre necessariamente a integridade da assinatura.

O Regulamento EIDAS estabelece a função da garantia da integridade como um requisito essencial para as assinaturas eletrónicas avançadas e também para as qualificadas (alínea d) do artigo 26.º e n.º 12 do artigo 3.º). Mas a formulação desta função revela que o legislador do Regulamento a entende como externa à assinatura, porque a designa como a função que torna "*detetável qualquer alteração posterior dos dados*", ou seja, qualquer alteração posterior à assinatura. Trata-se, então, de uma função que faz perdurar no tempo, de forma sucessiva, os efeitos da assinatura, operando após o ato da sua aposição no documento, mas que é essencial à própria função de assinatura nos documentos eletrónicos.

5. A função de não repúdio

description of the elements to be taken into account in assessing the integrity; and an element of flexibility in the form of a reference to the surrounding circumstances". E mais adiante: *"Thus when an electronic certificate is added to the end of an "original" electronic communication to attest to the "originality" of that electronic communication"*. "A/CN.9/608/Add.2", par. 41 e 42, respetivamente.

[532] *"Where a signature was attached to a document, the integrity of the document and the integrity of the signature were so closely related that it was not possible to conceive of one without the other. In other words, where a signature was used to sign a document, the idea of the integrity of the document was inherent in the use of the signature"*. "A/CN.9/467", par. 72.

A função de não repúdio é derivada das anteriores e desenvolve-se em duas vertentes – o não repúdio na origem e o não repúdio no destino. Através dela, as partes nas transações eletrónicas adquirem a segurança da estabilidade e continuidade da vinculação a um documento ou a uma transação, mantendo-se para o futuro a vinculação resultante da autenticação. Esta função garante que o seu autor ou subscritor não possa mais tarde vir a alegar que afinal esse vínculo não existe. [533]

A estabilidade dessa vinculação ao longo do tempo aplica-se ao autor ou subscritor dos documentos, garantindo assim aos restantes interessados que a autoria está assegurada e que não é vulnerável à passagem do tempo, à alteração das circunstâncias ou à mudança da vontade do autor.

A função de não repúdio separa-se em dois domínios. Por um lado a que é própria dos documentos eletrónicos e garante a estabilidade da vinculação do signatário aos documentos por ele assinados, como acabamos de analisar. Por outro lado, a que se aplica às comunicações eletrónicas. No estudo do direito da assinatura eletrónica e dos instrumentos jurídicos de confiança e de segurança nas transações eletrónicas, devemos ter sempre em conta que a separação entre os documentos e as comunicações, entre os factos e as transações. Os documentos são estáticos, possuem uma ontologia específica e fechada. Pelo contrário, as transações são operações dinâmicas, acontecimentos relacionais e assentes em comunicações.

Devemos também ter sempre em conta que o direito da segurança jurídica eletrónica nasceu no seio das comunicações eletrónicas e não dos documentos eletrónicos. Estes só mais tarde se autonomizaram daquelas. Na sua origem, do que se tratava, era de conferir segurança jurídica nas comunicações eletrónicas, desde o EDI, até antes, às comunicações entre máquinas informáticas, e até ao telégrafo. Era nas comunicações eletrónicas que se centrava o centro das investigações jurídicas e técnicas destinadas a conferir-lhe segurança jurídica, e nesse contexto a função de não repúdio assumia importância fundamental, tanto no que respeita ao remetente de uma comunicação eletrónica (não repúdio na origem), como ao seu destinatário (não repúdio no destino), como analisamos de seguida.

[533] *"O não repúdio na origem deve oferecer-nos evidências digitais sobre o autor de uma transacção concreta, evidencia que encontramos ao verificar a chave privada"*. Velásquez, R.R., Sau, C.R. e Muñoz, R.M. (2004). Op. cit., pág. 187.

5.1. A função de não repúdio na origem

Relativamente aos documentos eletrónicos, a função do não repúdio na origem emerge diretamente da assinatura, sendo ela assegurada pelas funções de identificação, de autenticação do documento e da sua integridade. Todas elas estão orientadas para essa função final do não repúdio pelo seu autor ou subscritor.

Nas comunicações eletrónicas não documentadas, como eram aquelas em que nasceu o direito das assinaturas eletrónicas, não existiam instrumentos técnicos nem jurídicos que assegurassem a função de não repúdio. Por isso, na fase do EDI a função de não repúdio na origem consistia apenas numa qualificação jurídica. E a LMCE distingue duas possibilidades:

i) Nas mensagens enviadas de forma não automatizada, estabelece que o seu autor é sempre o remetente.[534] Este é o princípio geral – a mensagem provém da pessoa que a enviou, ou seja, o autor de uma mensagem é a pessoa em nome de quem foi enviada. Trata-se de uma aplicação do conceito de autenticação suportada na comunicação EDI, mas aplicável de forma genérica, tanto às comunicações estabelecidas em redes fechadas como abertas, e tanto nos casos em que exista, como naqueles em que não exista, uma convenção prévia de autenticação ou uma relação precedente.[535]

   Mas as mensagens eletrónicas são sempre enviadas através de máquinas, pelo que é necessário estabelecer a conexão entre o remetente e a máquina. Trata-se de responder à questão sobre como pode o destinatário de uma mensagem saber quem procedeu ao seu envio. A LMCE fá-lo no n.º 3 do art.º 13.º, apelando sempre à

[534] Esse princípio geral é estabelecido no artigo 13.º da LMCE, que tem como epígrafe *"Attribution of data messages"*. O princípio está estabelecido no n.º 1, que tem a seguinte redação: *"A data message is that of the originator if it was sent by the originator itself".* "Guide to Enactment LMCE (1996)", pág. 8.

[535] Embora a causa direta da LMCE fosse a juridificação das mensagens EDI, havia a consciência de que as suas normas se aplicariam a qualquer tipo de suporte eletrónico. *"If the addressee applies any authentication procedures previously agreed by the originator and such application results in the proper verification of the originator as the source of the message, the message is presumed to be that of the originator. That covers not only the situation where an authentication procedure has been agreed upon by the originator and the addressee but also situations where an originator, unilaterally or as a result of an agreement with an intermediary, identified a procedure and agreed to be bound by a data message that met the requirements corresponding to that procedure".* "A/CN.9/426", par. 91. No mesmo sentido, "Guide to Enactment LMCE (1996)", par. 86.

existência de uma relação subjacente e prévia entre as partes. O destinatário deve considerar que a mensagem provém de determinado remetente sempre que tenha chegado a essa conclusão mediante a aplicação sobre ela de um procedimento de autenticação previamente estabelecido entre ambos.

O convénio de autenticação específico pode consistir, por exemplo, em colocar nas mensagens uma composição numérica sequencial, sempre com os mesmos carateres previamente estabelecidas por ambas as partes, ou com os carateres variáveis que resultem do conteúdo do documento. Todas as mensagens que respeitassem essas regras e proviessem de um determinado computador ou sistema, legitimariam o destinatário a considerá-las emitidas pela outra parte que com ele estabeleceu esse convénio de autenticação.[536] Outra forma de autenticação é a utilização, por acordo mútuo, dos serviços de um terceiro especializado, que é comum nos sistemas de EDI, bem como de assinatura digital, com base na alínea a) do n.º 3 do art.º 13.º da LMCE.

ii) Quando a mensagem é enviada de forma automatizada, considera a LMCE que o seu autor é a pessoa que é responsável por esse sistema.[537] O destinatário pode considerar sempre as mensagens autenticadas, desde que elas:

   a. Provenham de um sistema informático que ele conheça;
   b. Esse sistema esteja previamente programado para emitir essas mensagens de forma automática, e que;
   c. Essa programação seja da responsabilidade da pessoa que é considerada o emitente da mensagem.

O regime da LMCE é lacunar, deixando para as partes, em caso de litígio, um trabalho difícil de atividade probatória. Mas a ambição da LMCE era apenas a de conferir relevo jurídico às mensagens EDI.[538]

---

[536] Essa regra consta da alínea a) do n.º 3 do artigo 13.º da LMCE."Guide to Enactment LMCE (1996)", pág. 9.

[537] A LMCE prevê o modo de autenticação deste tipo de mensagens no n.º 2 do artigo 13.º. *Ibidem*.

[538] Essa lacuna é assumida pelo próprio Guia de Transposição da LMCE, quando se refere que *"However, it should be noted that paragraph (3)(a) applies only when the communication between the originator and the addressee is based on a previous agreement, but that it does not apply in an open environment"*. "Guide to Enactment LMCE (1996)", par. 86.

Com a emergência da assinatura digital, a garantia do não repúdio na origem considerou-se resolvida como sendo um produto da assinatura eletrónica, em face da segurança na vinculação que aquela tecnologia permite.

Só o Regulamento EIDAS vem autonomizar, com temos referido anteriormente, as transações eletrónicas não suportadas em documentos, para as quais estabelece que o modo de vinculação jurídica é mediante a identificação eletrónica, reservando a assinatura eletrónica para aquelas que são suportadas em documentos.

A função do não repúdio na origem assume particular relevância nas comunicações, nomeadamente nos casos em que delas resultam efeitos jurídicos. É o caso das notificações efetuadas por meios eletrónicos, cuja validade e eficácia jurídica dependem da garantia de origem da sua emissão. Analisamos no capítulo VI da Parte II o regime do serviço de envio registado eletrónico que o Regulamento EIDAS estabelece no artigo 43.º A autonomização deste serviço como um dos serviços de confiança eletrónica corresponde também a uma manifestação específica da função do não repúdio na origem.

Do mesmo modo esta função se aplica aos serviços prestados por agentes económicos ou organismos públicos mediante sítios *web*. Nas transações que qualquer interessado pretenda estabelecer é necessário garantir que o titular desses serviços eletrónicos fique vinculado às transações que se estabelecem por seu intermédio, garantindo-se também a função de não repúdio na origem. O Regulamento EIDAS estabelece o respetivo regime no artigo 45.º, como analisaremos no capítulo VI da Parte II.

5.2. A função de não repúdio no destino

A função de não repúdio no destino garante que uma pessoa que recebeu uma comunicação não possa mais tarde vir arguir que não a recebeu. Trata-se de uma segurança relativa às comunicações e não aos documentos, pelo que não tem correspondência na assinatura manuscrita. Podendo ser assegurada por instrumentos tecnológicos acessórios da assinatura eletrónica, esta função não é intrínseca à assinatura eletrónica.

Nas comunicações tradicionais, em papel, a garantia da receção pelo destinatário de um documento é dada pela entidade que efetua o seu transporte e a sua

entrega, normalmente os serviços de correio. A garantia da entrega dos documentos e da correspondência é comprovada pela data de entrega do correio registado.[539] Essa segurança necessita de ser replicada também nas comunicações eletrónica.

A data e o lugar do envio e da receção de declarações negociais têm relevância no tempo e no lugar da celebração dos contratos e tem efeitos jurídicos precisos, nomeadamente no momento da perfeição dos contratos, da constituição, da transmissão e da extinção de direitos que deles resultam, e ainda a determinação da lei aplicável. Também o local de envio e de receção das mensagens eletrónicas pode ser determinante para a verificação da lei territorial aplicável às relações jurídicas que delas emergem.[540]

Estas questões ganharam dimensão com a generalização da utilização do EDI, pelo que a LMCE se ocupa cuidadosamente desta matéria.[541] Na falta de soluções tecnológicas de confirmação das datas de remessa e receção das mensagens, a LMCE adota também soluções assentes na equivalência funcional, na tecnologia do EDI então disponível, bem como no princípio da autonomia contratual.[542]

A LMCE trata separadamente a definição temporal do momento da expedição das mensagens eletrónicas e do momento da sua receção.[543]

---

[539] Os artigos 28.º e 30.º do DL n.º 176/88, de 18 de maio, estabelecem o regime de entrega e da respetiva documentação de prova, do correio registado e do correio registado com aviso de receção.

[540] A importância da determinação da data e do local de envio e de receção das mensagens eletrónicas foi relevada no decurso dos trabalhos preparatórios, como se evidencia, de forma exemplificativa no seguinte trecho: *"Parties to a contract have a practical interest in knowing, with some certainty, where and when the contract is formed. When the contract is formed, the parties become bound by the legal obligations they have agreed upon and the contract may start producing effects. (...) In some countries, the place where the contract is formed may also be relevant for determining the applicable customary practices; the competent court in case of litigation; and the applicable law in private international law"*. "A/CN.9/333", par. 69.

[541] Esta problemática colocou-se nas relações administrativas e nos processos judiciais, quando as comunicações eletrónicas passaram a ser utilizadas nos correspondentes procedimentos e processos. A utilização das comunicações eletrónicas para a entrega de documentos pelos cidadãos aos órgãos da administração pública, por exemplo de declarações de impostos e de entrega de petições e peças processuais em procedimentos administrativos e processos judiciais, colocou a questão da determinação da data e do lugar em que essas diligências se consideram consumadas. Em sentido inverso, a mesma questão se coloca quando os órgãos administrativos emitem notificações por via eletrónica e nos processos judiciais os tribunais procedem à citação e notificação das partes por essa via.

[542] Nos trabalhos preparatórios da LMCE foram analisadas as possibilidades de adoção de duas teorias no que respeita à perfeição dos contratos celebrados mediante a emissão de declarações negociais comunicadas por via eletrónica. Por um lado a teoria da receção que considera que a declaração negocial comunicada pelo emitente a um destinatário, só produz efeitos quando este último, depois de a aceitar, remeter uma mensagem de aceitação ao emitente e este a receber. Por outro lado a teoria da declaração, segundo a qual, os efeitos se produzem logo que o destinatário emite a declaração de aceitação, sem necessidade de ter que se aguardar pela confirmação da sua chegada ao remetente da primeira declaração. *"Two main theories (...). The receipt rule (...). The declaration rule (...) states that the contract is formed when the offeree declares or sends his acceptance of the offer to the offeror. In the case of written mail, many legal systems have adopted some form of the dispatch rule"*. "A/CN.9/333", par. 72.

[543] Trata-se do artigo 15.º, que sob o título *"Time and place of dispatch and receipt of data messages".* "Guide to Enactment LMCE (1996)", pág. 11.

i) O momento da remessa é definido como aquele em que uma mensagem eletrónica entra num sistema informático que não esteja sob o domínio do remetente nem de alguém que tenha enviado a mensagem em seu nome, por exemplo, um prestador de serviços. Considera-se feita a expedição no momento em que a mensagem entra no sistema informático para onde foi enviada, pelo que a expedição e a receção ocorrerão tendencialmente no mesmo momento.[544] Esta exigência destina-se a proteger as expectativas do destinatário contra uma qualquer inoperacionalidade dos sistemas informáticos e de comunicações.

A LMCE não define o conceito de entrada da mensagem eletrónica no sistema informático do destinatário nem a forma de o determinar mas, nos trabalhos preparatórios e nas notas explicativas, define-se esse conceito do ponto de vista funcional, como o momento em que a mensagem pode ser tratada pelo sistema informático de destino.[545]

ii) O momento em que uma mensagem eletrónica se considera recebida é aquele em que a mensagem entrou no sistema informático do destinatário, nos termos do n.º 2 do art.º 15.º da LMCE.[546] O conceito de entrada tem também aqui o sentido do momento em que a mensagem é recebida e fica na disponibilidade do destinatário.[547]

---

[544] Essa simultaneidade é expressamente mencionada nas notas explicativas: *"If dispatch occurs when the data message reaches an information system of the addressee, dispatch under paragraph (1) and receipt under paragraph (2) are simultaneous"*. "Guide to Enactment LMCE (1996)", pág. 55, par. 101.

[545] Como se refere nas notas explicativas, *"A data message enters an information system at the time when it becomes available for processing within that information system"*. "Guide to Enactment LMCE (1996)", pág. 56, par. 103.

[546] Os comprovativos de receção são declarações de ciência e de verificação de um facto, pelo que não revelam qualquer vontade do destinatário que os emite, seja ela no sentido da aceitação ou no sentido de rejeição de uma eventual proposta negocial. O objeto do comprovativo eletrónico é apenas o de constituir prova de entrega da comunicação eletrónica enviada. Como se refere linearmente nos trabalhos preparatórios, *"Acknowledgement of receipt merely confirms that the original message is in the possession of the receiving party and is not to be confused with any decision on the part of the receiving party as to agreement with the content of the message"*. "A/CN.9/333", par. 49. Do mesmo modo, *"For example, where an originator sends an offer in a data message and requests acknowledgement of receipt, the acknowledgement of receipt simply evidences that the offer has been received"*. "A/CN.9/426", par. 98.

[547] A LMCE consagra a teoria da receção, segundo, aliás, o regime do Acordo TEDIS: *"As far as the formation of a contract is concerned, a contract by EDI is deemed to be concluded at the time and place where the EDI message constituting the acceptance of an offer is made available to the information system of the recipient (reception rule)"*. "A/CN.9/350", par. 99. Esse foi o consenso estabelecido nos trabalhos preparatórios: *"As to the definition of a possible rule to be applied in the absence of a prior*

Embora não seja unívoco este conceito nos sistemas informáticos, a LMCE confere relevância determinante ao exato momento em que a mensagem é depositada no sistema informático do destinatário, sendo que os processamentos subsequentes a efetuar internamente por este são já posteriores.[548] A mensagem considera-se recebida no momento em que ficou disponível para ser processada pelo sistema do destinatário. Do que se trata na LMCE é apenas de determinar quando se concretiza o momento de emissão e de receção de uma mensagem eletrónica.[549]

Caso a mensagem seja enviada para outro sistema do destinatário, só se considera recebida *"no momento em que o destinatário a recupere"* (ponto ii) da alínea a) do n.º 2 do art.º 15.º), ou seja, apenas quando passe a estar na disponibilidade do destinatário.

A confirmação de receção pelo destinatário pode ser expressa ou implícita, automática ou manual, por exemplo nos casos em que sejam comportamentos concludentes do destinatário que só podem ser consequência da receção da mensagem subjacente. É, por exemplo, o caso da expedição, do destinatário para o remetente, das mercadorias correspondentes à encomenda que este efetuou através de envio de uma comunicação eletrónica. Tratando-se das mesmas mercadorias que foram encomendadas, a sua remessa ao emitente da mensagem eletrónica que continha a encomenda, comprova que o destinatário desta a recebeu.[550] Os comprovativos de entrega e de receção são documentos eletrónicos normais, que só mais tarde viriam a ter regulamentação jurídica específica.

---

agreement between the parties, it was agreed that the main purpose of such a rule should be to provide certainty to all parties involved. Some support was expressed in favour of the theory of receipt". "A/CN.9/360", par. 89.

[548] A precisão da definição do momento relevante de entrada foi considerada com cuidado nos trabalhos preparatórios, como evidencia o seguinte trecho: *"A data message enters an information system at the time when it becomes available for processing within that information system. Whether a data message which enters an information system is usable by the addressee is outside the purview of the Model Law"*. "A/CN.9/WG.IV/WP.64", par. 103.

[549] Foi nesse sentido que se orientaram os trabalhos preparatórios da LMCE: *"It was felt that the Model Law should not create a more stringent requirement than currently exists in a paper-based environment, where a message can be considered to be received even if it is not intelligible for the addressee or not intended to be intelligible to the addressee (e.g. , where encrypted data is transmitted to a depository for the sole purpose of retention in the context of intellectual property rights protection)"*. "A/CN.9/426", par. 109.

[550] Os recibos de entrega estão regulados no artigo 14.º da LMCE que, sob o título "*Acknowledgement of receipt"*. "Guide to Enactment LMCE (1996)", pág.s 9 e 10..

O regime da LMCE, sendo prudente, não deixa de ser desequilibrado em termos de composição de interesses entre o remetente e o destinatário. É na esfera deste último que se centra o controlo do momento em que se consumam os pressupostos jurídicos da expedição das mensagens e da sua receção, sendo também ele que dispõe dos elementos de prova. Apesar de esses elementos ficarem sempre registados no sistema do destinatário e poderem ser objeto de auditorias ou perícias, eles ficam sempre na disponibilidade do destinatário, pelo que dele dependerá sempre a sua existência. E esse facto pode deixar desprotegidos os interesses do remetente das mensagens eletrónicas, em favor do destinatário.

A evolução jurídica e tecnológica viria a proporcionar novas soluções para o problema do não repúdio no destino. Essas soluções utilizam dois instrumentos jurídicos:

i) Os selos temporais, que são instrumentos eletrónicos de vinculação de um conjunto de dados a uma determinada data e hora, que foram recentemente consignados pelo Regulamento EIDAS, como analisaremos no Capítulo VI desta Parte I;[551]

ii) A instituição das chamadas notificações eletrónicas, cujo regime jurídico adquiriu novos fundamentos do Regulamento, mediante a criação do serviço de envio registado eletrónico, que assegura a certificação do envio e da receção das comunicações eletrónicas, bem como a integridade dos dados enviados e recebidos.[552]

A garantia do não repúdio no destino não é uma função típica da assinatura eletrónica, mas uma função essencial à confiança jurídica na utilização dos meios eletrónicos e um requisito de segurança jurídica nas comunicações eletrónicas. Apesar de não se tratar de uma função da assinatura eletrónica, os procedimentos técnicos que dos quais emerge a sua qualificação jurídica são idênticos, nomeadamente no que respeita à vinculação de dados mediante utilização da criptografia.[553]

---

[551] O n.º 33 do artigo 3.º do Regulamento define os selos temporais do seguinte modo: *"«Selos temporais»: os dados em formato eletrónico que vinculam outros dados em formato eletrónico a uma hora específica, criando uma prova de que esses outros dados existiam nesse momento"*.

[552] O n.º 36 do artigo 3.º do Regulamente define da seguinte forma os serviços de envio registado eletrónico. *"«Serviço de envio registado eletrónico»: um serviço que torne possível a transmissão de dados entre terceiros por meios eletrónicos e forneça prova do tratamento dos dados transmitidos, nomeadamente a prova do envio e da receção dos mesmos, e que proteja os dados transferidos contra o risco de perda, roubo, dano ou alteração não autorizada"*.

[553] Nesse sentido se pronuncia Nadal em Nadal, A.G. (2009). Op. cit, pag. 55.

6. A função de confidencialidade

A função de confidencialidade não é típica da assinatura eletrónica, tal como não o é nas assinaturas manuscritas. Quando um destinatário recebe um documento assinado eletronicamente, ele recebe o documento de base em claro, perfeitamente legível quando se trate de um texto.

Também nas comunicações de documentos físicos, em papel, através de correio, a confidencialidade não depende da assinatura nem é um atributo do documento, mas do canal de comunicação usado para a transmissão. Nas comunicações por correio físico a confidencialidade é garantida pelo envelope e pelo serviço de correios, não pelo documento nem pela assinatura.[554]

Nas redes eletrónicas abertas a confidencialidade é uma necessidade fundamental. Nelas, os documentos não circulam fechados, como acontece nas comunicações por correio tradicional. Também a utilização das comunicações eletrónicas pelas administrações públicas faz com que circule na Internet e noutras redes locais, informação sujeita a especiais deveres de sigilo.[555] Em todos estes casos de comunicações e transações estritamente pessoais é necessário garantir a sua confidencialidade.

Como a assinatura digital assenta na criptografia e esta é a ciência da ocultação da informação, pode então a mesma tecnologia da assinatura digital prestar esse serviço da confidencialidade aos interessados.

A confidencialidade dos documentos eletrónicos é assegurada com a sua encriptação pela chave pública do destinatário dado que só pode ser desencriptado pelo destinatário, através da sua chave privada.

Como analisámos no capítulo referente à assinatura digital, um documento assinado é um conjunto composto por três documentos separados - o original em claro e

[554] Como afirma Baygual, *"se utilizarmos um paralelismo entre o envio de uma carta em suporte papel e assinada manualmente, a assinatura equivaleria a estampar a rubrica na correspondente carta, enquanto que a encriptação implicaria colocar a carta no correspondente envelope fechado. Um envelope pode conter uma carta, assinada ou não; uma carta assinada pode fechar-se num envelope, ou não"*. Baygual, Francesc A. Op. Cit., pág.s 1283 e 1284.

[555] As transações eletrónicas com a administração pública são de grande relevo, por exemplo a entrega das declarações de impostos, nomeadamente do IRS através da Internet, em que os contribuintes declaram factos da sua vida privada e mesmo íntima, sujeitos a sigilo. As necessidades de segurança excedem o domínio da confidencialidade dos dados. Em matéria fiscal, é necessário assegurar que quem entrega uma declaração de IRS é mesmo o titular dos rendimentos obtidos e não qualquer outra pessoa. Só assim existe certeza de que mais ninguém entrega declarações fiscais ao Estado em nome de outrém, constituindo-o assim no encargo de uma dívida que não é sua. Essa garantia só pode ser dada quando a autenticação é forte e segura.

legível, o resumo *hash* encriptado pela chave privada e o certificado de assinatura eletrónica do autor.

Para garantir a confidencialidade, o autor do documento, obtém do seu destinatário a chave pública da sua assinatura eletrónica e aplica-a sobre o conjunto documental antes referido, ficando esse conjunto encriptado com essa chave. [556]

Ao receber o documento, o destinatário desencripta o conjunto documental, aplicando sobre ele a sua chave privada.[557] De seguida, aplicando a chave pública do autor ou emitente do documento obtém o resumo e a chave simétrica com a qual foi gerado esse resumo. Aplicando de novo essa chave privada sobre o documento original obtém um novo resumo, que vai comparar com o resumo que lhe foi enviado pelo autor ou emitente. Se forem iguais, o documento considera-se validamente assinado.

Esta função de confidencialidade é um resultado colateral da utilização da criptografia na construção da assinatura digital.[558] Trata-se também de um produto jurídico importante para a confiança dos agentes na utilização das comunicações eletrónicas, mas é externo e autónomo da assinatura eletrónica.

---

[556] A confidencialidade não é uma função da assinatura eletrónica. Ortega Diaz afirma, nomeadamente que *"ao assinar um documento eletrónico mediante um criptograma assimétrico, tanto o emissor como o recetor terão a segurança de que só eles poderão conhecer o conteúdo da mensagem*". Díaz, J.J.O., Op. Cit., pág. 48. Vimos já anteriormente que não é assim. A confidencialidade só é garantida com a encriptação da mensagem com a chave pública do destinatário, porque a partir daí só este pode proceder à sua desencriptação. Nesse sentido Perales: *"Se, posteriormente, o conjunto formado pelo documento e pela assinatura digital se encripta com a chave pública do destinatário, ficará garantido que só este último terá acesso ao conteúdo do documento transmitido, aplicando previamente, para desencriptá-lo a sua chave privada"*. Perales, J.M.A.M. (2005), Op. Cit., pág. 97. Do mesmo modo Garnacho afirma que *"o processo de assinatura não proporciona confidencialidade às mensagens"* e mais adiante *"o processo de encriptação não tem como objetivo conferir confidencialidade a uma mensagem, mas apenas provar a autoria e garantir a sua integridade"*. Garnacho, A.R. (2002). Op. Cit., pág. 1324. Também Baygual distingue claramente as funções de confidencialidade e de autenticação da criptografia, considerando que são duas funções separadas, que não têm que andar associadas. Baygual, Francesc A. Op. Cit., pág.s 1283 e 1284.

[557] Como anteriormente referimos, a chave privada também desencripta o produto encriptado pela chave pública.

[558] Essa separação entre as funções da assinatura eletrónica e a função da confidencialidade que é proporcionada pela utilização da criptografia, é enunciada num dos documentos da UNCITRAL, no trecho seguinte: *"While the use of cryptography is one of the main features of digital signatures, the mere fact that a digital signature is used to authenticate a message containing information in digital form should not be confused with a more general use of cryptography for purposes of confidentiality. Confidentiality encryption is a method used for encoding an electronic communication so that only the originator and the addressee of the message will be able to read it. In a number of countries, the use of cryptography for confidentiality purposes is limited by law for reasons of public policy that may involve considerations of national defense. However, the use of cryptography for authentication purposes by producing a digital signature does not necessarily imply the use of cryptography to make any information confidential in the communication process, since the encrypted digital signature may be merely appended to a non-encrypted message"*. "A/CN.9/630/Add.1", nota de rodapé 2.

Capítulo IV – Os certificados de assinatura eletrónica

A principal função dos certificados de assinatura eletrónica é dar a conhecer, a qualquer terceiro, a identidade do titular de um par de chaves de assinatura eletrónica. Estes certificados desempenham, nas relações jurídicas estabelecidas por meios eletrónicos, o papel que o conhecimento pessoal entre as partes assume nas relações jurídicas estabelecidas por meios tradicionais.

As tecnologias eletrónicas vieram proporcionar aos agentes económicos a possibilidade de realizarem negócios com outras partes que não conheciam anteriormente. Nas relações administrativas, permitiram que os cidadãos se relacionem com os órgãos respetivos sem necessidade de se deslocarem fisicamente às suas instalações, e que os serviços prestados por esses órgãos estivessem acessíveis por via eletrónica permanentemente e em qualquer lugar.

Como as relações jurídicas estabelecidas por meios eletrónicos operam através de máquinas que se interpõem entre as pessoas, é indispensável à existência de um vínculo jurídico seguro, a certeza acerca da identidade da pessoa que é responsável pela emissão da declarações ou das transações eletrónicas. Esse conhecimento é assegurado

pela assinatura eletrónica, mediante a existência de um par de chaves conexas entre si, de que é titular exclusivo uma determinada pessoa.

A função do certificado é confirmar a identidade dessa pessoa.[559] Essa identificação necessita de ser suficientemente segura, dado que muitas relações estabelecidas por meios eletrónicos, em especial nas redes abertas, envolvem partes que não se conhecem. Por essa razão a informação acerca da identidade das partes necessita de ser emitida por uma entidade com suficiente credibilidade para ser de confiança de todas as pessoas que pretendam estabelecer relações jurídicas através dessas redes. Esse é o papel das entidades que prestam serviços de certificação.

A origem dos certificados de assinatura eletrónica funda-se na atividade financeira e bancária. A necessidade de os comerciantes aceitarem pagamentos com cartões de crédito ou de débito, de clientes que até então não conheciam foi viabilizada mediante a emissão de um cartão, por uma entidade financeira, onde se identificasse a ela própria, bem como ao titular do cartão, certificando que essa pessoa possuía uma conta bancária associada ao cartão. Esta certificação conferia ao comerciante uma garantia de confiança no seu cliente.[560] Foi esta solução que serviu de modelo para a assinatura eletrónica utilizasse um mecanismo idêntico. De seguida analisamos as funções dos certificados.

1. A função dos certificados de assinatura eletrónica

[559] A LMAE define o certificado eletrónico como um documento eletrónico ou outro registo que confirme a vinculação entre uma pessoa que seja titular de uma assinatura e os dados de criação dessa assinatura, ou seja, o par de chaves correspondente. Alínea b) do artigo 2.º da LMAE: *"(b) "Certificate" means a data message or other record confirming the link between a signatory and signature creation data"*. "A/CN.9/WG.IV/WP.88", pág. 7.

[560] Este modelo de certificação de uma identidade, assente num mecanismo de segurança que opera com a intervenção de entidade terceiras que são independentes, pode ser reforçado se intervierem outras entidades de nível superior que, por sua vez, certifiquem a identidade dessas entidades terceiras e assim sucessivamente, segundo uma cadeia de confiança. O modelo teve origem na norma ISO X.509, da International Telecommunication Union (ITU), disponível em file:///C:/Users/jp01918/Downloads/T-REC-X.509-201210-I!!PDF-E.pdf (consulta efetuada em 30/11/2015), que por sua vez resultou da norma ISO X.500, cuja emissão tem origem no ano 1984. *"One common use of digital certificates employed a standard (ISO X.509), which allowed for a hierarchy of trusted entities to be used to authenticate parties. This approach was often referred to as the credit card model, as it reflected the business model underlying the credit card industry"*. "A/CN.9/446", par. 98. O facto de esta tecnologia ter tido a sua aplicação desde logo nos sistemas de pagamento por cartões de crédito, permitiu que ela se aplicasse com as necessárias adaptações, naturalmente, aos pagamentos efetuados por transações em redes abertas. Essa modalidade de pagamentos teve a sua origem no Protocolo SET ("Secure Electronic Transaction"), estabelecido em 1997, disponível em http://www.maithean.com/docs/set_bk1.pdf. (consulta efetuada em 30/11/2015).

Já verificámos, no capítulo referente à assinatura digital, que a aplicação, pelo destinatário, da chave pública do remetente só lhe permite saber vincular este ao documento, porque uma entidade terceira lhe identifica o titular dessa chave privada.

O procedimento criptográfico garante certeza acerca de duas vinculações:

i) Do documento à chave privada que o encriptou;

ii) Da chave pública que o desencripta àquela chave privada.

Mas a vinculação do titular identificado à chave privada é externa ao par de chaves, não podendo ser de natureza matemática. Ela é assegurada pelo certificado de assinatura eletrónica.[561]

Um certificado eletrónico é um documento eletrónico emitido por um prestador de serviços de confiança, para conhecimento geral, onde declara a identidade de um titular de uma chave pública de assinatura eletrónica.[562] É uma declaração de ciência, pública, proferida por uma entidade especializada na prestação de serviços de confiança.

O conhecimento dessa pessoa por aquela entidade advém do facto de ter sido ela a gerar o par de chaves de assinatura eletrónica e a entregar-lhe o respetivo dispositivo. Esses atos de geração e de entrega pressupõem a prévia identificação segura dessa pessoa por aquela entidade. É essa identidade, de que a entidade certificadora tem conhecimento, que ela certifica mediante a emissão do certificado.[563] Analisaremos, no ponto 1.1.2, do Capítulo II da Parte III do nosso trabalho o nível de rigor que é indispensável a essa função dos prestadores de serviços de confiança eletrónica, na identificação dos titulares da assinatura eletrónica, bem como de outros serviços de confiança.

Através deste documento, os eventuais destinatários de uma mensagem ou de um documento eletrónico ficam a conhecer, com elevado grau de segurança, a

---

[561] Como afirma de forma sintética Nadal, *"La función central del certificado es, efectivamente, vincular un dato de verificación de firma (una clave pública en el caso de criptografia assimétrica) a una persona determinada"*. Nadal, A.G. (2009). Op. cit, pag. 137.

[562] A identidade da pessoa que assina é apenas dada pelo certificado. A operacionalidade de ambos os pares de chaves nada nos diz acerca da identidade do seu titular. Essa identidade é dada pelo certificado, que é o documento onde a entidade que emitiu o par de chaves atesta essa identidade. Como se refere na proposta de diretiva da UE acerca das Assinaturas Eletrónicas, *"A verificação da autenticidade e da integridade dos dados não prova necessariamente a identidade do signatário que cria as assinaturas eletrónicas"*. ("COM(1998) 297 final").

[563] O certificado é, na sua essência, uma declaração mediante a qual uma determinada entidade dá a conhecer um facto de que tem conhecimento. *"The meaning of "certificate" as used in the context of certain types of electronic signatures differed little from the general meaning of a document by which a person would confirm certain facts"*. "A/CN.9/483", par. 65. Do mesmo modo *"The term "certificate" as used in the context of certain types of electronic signatures and as defined in the Model Law differs little from its general meaning of a document by which a person would confirm certain facts"*. "A/CN.9/WG.IV/WP.88", par. 94.

identidade de uma parte com quem podem estabelecer relações jurídicas.[564] Esse conhecimento é essencial para a vinculação jurídica.[565]

Os certificados são emitidos no momento em que os prestadores de serviços de confiança efetuam a geração de um par de chaves para assinatura eletrónica de uma determinada pessoa devidamente identificada, e a pedido desta. Para que o certificado seja seguro e a informação que dele consta seja autêntica, é assinado com a assinatura eletrónica da entidade certificadora.[566]

O certificado de assinatura eletrónica desempenha um papel essencial na personalização das relações jurídicas estabelecidas por meios eletrónicos. Trata-se do instrumento fundamental de personalização das relações estabelecidas por meios eletrónicos.[567] Como o certificado acompanha o documento ou, mais rigorosamente, a assinatura, esse conhecimento fica acessível de imediato, mesmo que o destinatário não possuísse qualquer conhecimento pessoal nem sequer da existência do respetivo autor.

É o certificado que permite que o estabelecimento de relações jurídicas nas redes abertas, mesmo entre pessoas que anteriormente não se conheciam, e entre as quais não existia qualquer convenção prévia de autenticação.[568] [569]

---

[564] Como se enuncia no Guia Para a Transposição da LMAE, a finalidade essencial dos certificados é reconhecer e revelar o vínculo existente entre os dados de criação de uma assinatura eletrónica (a chave privada e a chave pública) e uma pessoa determinada e devidamente identificada. *"The purpose of the certificate is to recognize, show or confirm a link between signature creation data and the signatory. That link is created when the signature creation data is generated"*. "A/CN.9/WG.IV/WP.88", par. 95.

[565] A definição utilizada pela LMAE, de certificado, é a de dar certeza acerca da identidade de um titular de assinatura eletrónica. *"The Working Group agreed that the main function of a certificate in the context of electronic signatures was to provide certainty regarding the existence of a link between a given signature creation device (for example, a private cryptographic key or a biometric indicator) and a signatory"*. "A/CN.9/483", par. 65.

[566] Essa confirmação é muito importante, porque assegura a autenticidade do certificado. *"To assure the authenticity of the certificate with respect to both its contents and its source, the certification authority digitally signs it"*. "A/CN.9/WG.IV/WP.71", par. 36. Do mesmo modo, *"The principal function of a certificate is to bind a public key with a particular holder"*. "A/CN.9/WG.IV/WP.88", par. 53.

[567] É assim que é definido nos trabalhos da UNCITRAL.*"A certificate's principal function is to bind a public key with a particular holder"*. "A/CN.9/WG.IV/WP.71", par. 36.

[568] O restante procedimento do destinatário dos documentos eletrónicos já o conhecemos. Estabelecida a vinculação do autor à assinatura, o destinatário confirma a vinculação da assinatura ao documento, concluindo pela vinculação do autor ao documento. Essa conexão entre a assinatura e o documento é efetuada mediante a aplicação da chave pública ao *hash* e, depois, mediante a aplicação da chave simétrica que acompanha o *hash* sobre o documento em claro, para obter um novo *hash*, que se for igual ao que recebeu do autor do documento confirma que esse documento foi assinado por aquele autor e não foi alterado desde essa assinatura.

[569] Como refere Carron, os certificados eletrónicos operam *"com un verdadeiro passaporte electrónico que permite a sus usuários identificarse en Internet o en cualquer red privada a fin de poder transmitir datos, asegurando la confidencialidad e integridad de tales intercâmbios, y permitiendo identificar al autor del mensage"*. Carron, C.F. (2010). Empleo de las Nuevas Tecnologías en el Proceso Civil Francés: Algunas Ideas Generales. Em: Motilla. C.S. (Coordinadora). *Presente y Futuro de la e-Justicia en Espanha y la Unión Europea. Thomson Reuters*. Aranzadi. Pamplona, pag. 497.

Os certificados de assinatura podem ser consultados publicamente em diretórios disponibilizados pelos prestadores de serviços nas suas páginas na Internet.

Sendo essenciais à identificação do autor da assinatura, os certificados são dispensáveis nos casos em que existe confiança e as partes se conhecem. Ambas as partes podem trocar entre si mensagens autenticadas com assinatura eletrónica, sem necessidade de intervenção terceiros. Em ambos os casos existirá conhecimento da identidade do titular de um par de chaves de autenticação, que é essencial à vinculação jurídica, nomeadamente à garantia do não repúdio das mensagens e das transações eletrónicas.

No ponto 3.5.3.1.2 do Capítulo II da Parte II analisámos os requisitos e os efeitos dos certificados qualificados, sendo certo que a sua função é típica da de qualquer certificado de assinatura eletrónica.

A Diretiva Europeia da Assinatura Eletrónica estabelecia, no seu Anexo I um conjunto de requisitos objetivos para que um certificado fosse classificado como qualificado. O Regulamento EIDAS tipifica também, no seu Anexo I, requisitos idênticos, mas acrescenta o requisito determinante de que só podem emitir certificados qualificados os prestadores qualificados de serviços de confiança. Esta exigência traduz um mais elevado nível de garantias de segurança, que é a que resulta da sujeição destes prestadores de serviços a um controlo preventivo e sucessivo da sua atividade pelas entidades de supervisão, como analisaremos no ponto 1.6 do capítulo II da Parte III do nosso trabalho.

2. O conteúdo dos certificados de assinatura eletrónica

O certificado de assinatura eletrónica é composto por quatro elementos fundamentais:[570]

i) Identifica a entidade que o emitiu;

[570] Pela sua importância, o conteúdo dos certificados deve ser regulado por lei. A definição desse conteúdo foi consensualizada no Grupo de Trabalho da LMAE, em 1997, nos seguintes termos: *"A certificate is a data message that purports to be a certificate, identifies the certification authority, contains the public key of the user, names the user and is digitally signed by the certification authority".* A/CN.9/437, 12 March 1997, par. 101. Do mesmo modo, e de forma mais precisa: *"The elements regarded by the Working Group as the basic components of a certificate, namely, that a certificate should: be a data message; identify the certification authority; contain the public key of the holder; identify the holder; and be digitally signed by the certification authority"*. A/CN.9/WG.IV/WP.73, par. 51.

ii) Identifica a chave pública correspondente à chave privada do titular;

iii) Identifica o titular do par de chaves, o autor da assinatura eletrónica;

iv) Contém a assinatura eletrónica da entidade que o emitiu.

Outro elemento muito importante que deve constar do certificado é a data da sua de validade, para que se possa determinar se estava válido na data da assinatura.[571]

A eficácia do certificado depende do grau de confiança que nele depositam os terceiros interessados, que advém, por sua vez, do grau de confiança que lhes merece a entidade certificadora que o emite, bem como a qualificação do certificado. É essa a razão de ser da necessidade de constar do certificado a identificação desta entidade, bem como a sua assinatura eletrónica.

Mas o objeto do certificado é a identificação do titular da assinatura eletrónica. Essa identificação é uma função essencial da assinatura eletrónica, pelo que antes de a declarar no certificado, o prestador de serviços de confiança que o emite, tem o dever de rigorosamente o signatário, de forma tão segura que garanta a todos os interessados que o signatário é efetivamente a pessoa que consta do certificado.

Feita essa identificação, o prestador de serviços emite o par de chaves e o dispositivo de assinatura, autenticado com a sua própria assinatura eletrónica avançada, assegurando-se, de seguida, que entrega, exclusivamente a esse titular, esses elementos.[572] Fica assim fechado o ciclo da unicidade da ligação entre a identidade de uma pessoa e o instrumento que utiliza para assinar documentos eletrónicos. O certificado é uma declaração de ciência acerca dessa ligação.

O Regulamento EIDAS veio tipificar o conteúdo dos certificados de assinatura eletrónica, como especificamos no ponto 3.5.3.1.2 do Capítulo II da Parte II do nosso trabalho. Esse conteúdo destina-se a comprovar, perante terceiros interessado, que:

i) A encriptação do *hash* que consta do documento assinado foi efetuada pela chave privada que corresponde à chave pública que consta do certificado;

ii) O titular da chave privada é a pessoa identificada no certificado;

---

[571] O artigo 29.º do DL n.º 290-D/99, de 3/8, enuncia todos os elementos que devem constar do certificado, nomeadamente, a identificação do titular, a qualidade em que intervêm (se é em nome próprio ou em representação (e neste caso a identificação dos representados), a identificação da entidade credenciadora que emitiu o certificado, a chave pública, o número de série do certificado, o início e termo da sua validade, os algoritmos da chave pública, etc..

[572] Como refere o Grupo de Trabalho, *"To assure the authenticity of the certificate with respect to both its contents and its source, the certification authority digitally signs it"*. "A/CN.9/WG.IV/WP.71", par. 37.

iii) A identidade do prestador de serviços de confiança assegura essa vinculação;

iv) A fiabilidade desse prestador de serviços pode ser verificada através da sua chave pública;

v) A natureza do certificado.

3. Os tipos de certificados de assinatura eletrónica

A assinatura eletrónica não é um instrumento inato à pessoa, nem sempre igual como a manuscrita, mas um mecanismo que se aplica mediante um dispositivo que é um objeto. Quando o autor autentica um documento aplica a sua chave privada sobre ele, e o resultado será sempre diferente para cada documento.

Por outro lado, nada impede que uma mesma pessoa possua vários objetos desse tipo, sendo, por exemplo, um deles utilizado para assinar em nome próprio e outro ou outros como representante, legal ou voluntário, de uma entidade ou de um órgão da administração pública.

Nos casos em que a pessoa que assina o faz em representação de outra pessoa ou entidade, é possível e desejável que o certificado mencione esse facto, assim se aumentando a segurança e os níveis de confiança dos terceiros que confiam na assinatura.[573]

Os certificados identificam sempre uma pessoa que é o sujeito dos direitos e das obrigações que emergem de um determinado documento ou transação eletrónicos, mas o meio de vinculação pode ser diferenciado, em conformidade com a natureza dos certificados, que também são indicados no próprio certificado.[574] Em função desse meio existem os seguintes tipo de certificados:[575]

---

[573] Trata-se dos chamados certificados de atributos, em que o autor da assinatura atua no exercício de uma função de representação *"The use of a digital signature might in some cases be restricted to certain types of transactions, for example as a result of limitations on the authority of the signor to bind the company in the name of which the transaction was made"*. "A/CN.9/437", par. 109.

[574] O Regulamento EIDAS veio retirar às pessoas coletivas a possibilidade de possuirem assinatura eletrónica, reservando esta para as pessoas singulares. Em comtrapartida foi criada a figura dos selos eletrónicos, que tecnicamente são instrumentos idênticos às assinaturas eletrónicas, mas se destinam a autenticar documentos emitidos por pessoas coletivas.

[575] *"Such a linkage may be done directly, by naming the holder of the public key in the certificate. It can also be done indirectly by describing certain attributes about the holder (e.g., a purchasing agent with authority to contract for purchases up to a given amount), or by describing a machine, device, or software agent under the control of the holder"*. A/CN.9/WG.IV/WP.73, par. 50.

i) Certificados de identificação. Identificam um titular de dispositivo de assinatura eletrónica que se autentica em seu próprio nome. São os certificados mais comuns, em que os respetivos titulares assinam em seu próprio nome;[576]

ii) Certificados de atributos.[577] São os certificados relativos a pessoas que assinam no exercício de representação ou mandato.[578] Nesses casos os certificados, para além de identificarem a pessoa que assina, mencionam o estatuto com que a assinatura é aplicada;[579]

O desenvolvimento dos serviços eletrónicos veio criar novos instrumentos de confiança na utilização dos suportes eletrónicos. São os casos, que analisaremos, mais adiante, no Capítulo VI desta Parte II do nosso trabalho, dos selos eletrónicos e da autenticação dos sítios web. No primeiro caso trata-se de certificados de pessoas coletivas ou organismos públicos que autenticam os documentos que emitem ou subscrevem com os selos eletrónicos, despenhando função idêntica à das assinaturas eletrónicas. No segundo caso trata-se de instrumentos de confiança que asseguram às partes que demandam serviços eletrónicos em sítios *web*, que as transações que efetuam são feitas com uma pessoa, singular ou coletiva que é titular do referido *sítio*. Também aqui a identificação dessa pessoa e a segurança acerca da sua vinculação àquele sítio, são garantidas pela emissão de um certificado por uma entidade prestadora de serviços de confiança.

4. Fiabilidade dos certificados e das assinaturas eletrónicas. Os certificados qualificados.

[576] Todos os certificados são de identificação, porque a função deles é a identificação da pessoa que fica vinculada com a aplicação de uma chave privada correspondente a uma determinada chave pública, num documento ou numa transação eletrónicas. *"The concept of identity may be more than a reference to the name of the signature holder, and may refer to other significant characteristics, such as position or authority, either in combination with a name or without reference to the name"*. A/CN.9/WG.IV/WP.82, par. 29.

[577] Também designados com certificados de autoridade, porque identificam o nível de autoridade que essa pessoa possui e com o qual assina um determinado documento, *"To establish the level of authority of a person ("authority certificates")"*. "A/CN.9/446", par. 72.

[578] *"Other uses of digital signatures, e.g., to establish the level of authority of a person ("authority certificates")"*. A/CN.9/WG.IV/WP.76, par. 20.

[579] *"For example, a certificate may be issued to an employee of a corporation specifying only the limits of such employee's purchasing authorization"*. A/CN.9/WG.IV/WP.73, par. 50.

A fiabilidade mede o nível de confiança que as partes devem conferir às transações eletrónicas. Essa medida é determinada pelo grau de cumprimento das obrigações legais de segurança no procedimento de criação do par de chaves.

Nesta matéria há que distinguir a fiabilidade do próprio certificado de assinatura eletrónica, da fiabilidade da própria assinatura.[580] A fiabilidade do certificado é garantida pela confiança que merece a entidade que o emitiu, e essa confiança assenta no cumprimento, por essa entidade, dos procedimentos de segurança que são certificados e auditados por outras entidades, numa hierarquia de credenciação das entidades certificadoras. Uma das informações que contém o certificado é a identificação entidades que credenciaram o prestador de serviços que o emitiu. Através dela, os terceiros interessados podem verificar o grau de confiança que podem extrair do certificado, em face do comprometimento das entidades credenciadoras na certificação da credibilidade da entidade certificadora. O grau de fiabilidade do certificado respeita à vinculação que a ele tem o prestador de serviços que o emitiu e a veracidade das declarações de ciência que nele emite, que são da sua responsabilidade.[581]

Por outro lado, a fiabilidade da própria assinatura, que é dada pelo cumprimento de um conjunto de formalismos que a lei estabelece para conferir às assinaturas eletrónicas uma força probatória mais ou menos elevada. É o caso, por exemplo, das assinaturas eletrónicas qualificadas, que possuem a virtualidade de conferir um grau mais elevado de segurança, por ser a própria lei a estabelecer os pressupostos que, uma vez verificados, permitem que se possam considerar *a priori* como mais seguras ou qualificadas. Esse facto deve constar do certificado, para que todos os interessados possam verificar e beneficiar de um índice acrescido de segurança na vinculação da parte que assinou, ao conteúdo do documento assinado.

Analisámos, no ponto 3.5.3.1.2 do Capítulo II da Parte II, os elementos constitutivos da qualificação dos certificados de assinatura eletrónica como qualificados. Essa classificação é essencial para o estabelecimento da presunção da

---

580 *"The reliability of the signature creation device (which was dealt with in the substantive provisions of the uniform rules) should be distinguished from the reliability of the link recognized in the certificate"*. "A/CN.9/483", par. 68.

581 Pode acontecer que se venha a verificar não ser seguro um certificado, após a sua emissão, por exemplo no caso de o respetivo titular ter falsificado os dados referentes à sua identidade e ter conseguido enganar a entidade certificadora, ao ponto de esta ter o ter emitido com uma identidade que não estava correta. *"Once issued, a certificate may prove to be unreliable, for example in situations where the signatory misrepresents its identity to the certification services provider"*. "A/CN.9/630/Add.1", par. 24. Nesse caso deve a entidade que o emitiu proceder à sua revogação logo que tenha conhecimento dessa falsificação.

autenticidade das assinaturas eletrónicas, bem como para o seu reconhecimento mútuo no espaço de toda a União Europeia. Um dos requisitos essenciais dessa classificação é que tenham sido emitidos por prestadores qualificados de serviços de confiança, sendo que esse estatuto depende de prévio reconhecimento.

Desta forma, todas as assinaturas eletrónicas qualificadas são reconhecidas e podem ser utilizadas como assinaturas eletrónicas qualificadas, pelas partes em todos os Estados Membros, resultando esse reconhecimento diretamente do n.º 3 do artigo 25.º Regulamento.

Os certificados qualificados são a base de confiança das assinaturas eletrónicas qualificadas, que possuem o efeito jurídico de serem legalmente equiparadas às assinaturas manuscritas, nos termos do n.º 2 do artigo 25.º. Do mesmo modo, o regime de responsabilidade dos prestadores de serviços pelos danos causados por incumprimento das normas do Regulamento EIDAS, faz presumir a sua responsabilidade quando se trate de um prestador qualificado, em conformidade com o artigo 13.º do Regulamento.

5. Revogação, suspensão e caducidade dos certificados

Os certificados de assinatura eletrónica devem ser sempre temporários e caducar ao fim de um período de tempo determinado, por razões de segurança. Tratando-se de um instrumento suscetível de posse, o dispositivo de assinatura eletrónica pode ficar acessível a terceiros não autorizados, o que pode vulnerabilizar a segurança que é dada a todas as pessoas pelo facto de o acesso ao dispositivo ser exclusivo do seu titular.

Nesses casos, uma regra de segurança que se utiliza habitualmente é a obrigação de o titular da assinatura eletrónica solicitar a emissão de um novo par de chaves periodicamente.[582]

Por outro lado, quando o titular constate que o dispositivo pode ter sido vulnerabilizado e o acesso a ele pode ter ficado à disposição de um terceiro não autorizado, deve requerer de imediato à entidade certificadora que o suspenda ou

[582] As assinaturas eletrónicas devem possuir uma certificação temporal, que explicite e guarde de forma segura a data e a hora em que que o document foi assinado. *"Should generally be reliably time-stamped to allow the verifier to determine reliably whether the digital signature was created during the "operational period" stated in the certificate"*. "A/CN.9/WG.IV/WP.71", par. 38.

cancele, a fim de que, se for utilizado, qualquer terceiro possa constatar que o certificado não está vigente e que a assinatura não é legítima nem válida.[583]

Nestes casos, um problema que se coloca é o da forma e da rapidez com que a informação acerca da suspensão ou do cancelamento do certificado deve chegar aos terceiros que confiam e que sejam eventualmente destinatários e documentos ou transações eletrónicas indevidamente assinados com esses certificados.

Para garantir os procedimentos de comunicação pelo titular das situações de risco, de cancelamento e de suspensão, bem como de divulgação por terceiros, é necessária a existência de um sistema de gestão das assinaturas eletrónicas, que deve ser assegurado pelas entidades certificadoras.[584]

A revogação dos certificados deve ocorrer sempre que cesse a razão da sua existência, por exemplo nos casos em que ocorre o falecimento do seu titular ou, tratando-se de pessoa coletiva, para os casos em que são admitidos, a partir do momento em que se extinguiu a sua personalidade jurídica. Essa revogação é importante para evitar que outrem tenha acesso à chave privada e inicie uma utilização abusiva, nomeadamente fazendo-se passar pela pessoa falecida. Nestes casos a revogação deve ser efetuada a pedido dos representantes legais das pessoas falecidas ou das pessoas coletivas extintas, mas deve também ocorrer por iniciativa da entidade certificadora quando esta tenha conhecimento desses factos. O mesmo deve ocorrer relativamente aos certificados de atributos, por exemplo de uma pessoa enquanto representante de uma pessoa coletiva, a partir do momento em que deixa de exercer essas funções.

A revogação pode também ser desencadeada por iniciativa da entidade certificadora nos casos em que constate que o certificado está viciado ou contém erros, nomeadamente porque identifica erradamente um titular, bem como nos casos em que a entidade certificadora é conhecedora de factos que o titular lhe devia ter comunicado, não o fez, e eram causa suficiente da sua revogação. São exemplo desses casos a perda

---

583 *"If the private key is "compromised", for example through loss of control of the private key by its holder, the certificate may lose its trustworthiness or become unreliable, and the certification authority (at the holder's request or even without the holder's consent, depending on the circumstances) may suspend (temporarily interrupt the operational period) or revoke (permanently invalidate) the certificate"*. "A/CN.9/WG.IV/WP.71", par. 40.

584 *"Once the certificate expires or is revoked, the corresponding public key loses its validity, even if the key pair was not compromised. Accordingly, a PKI scheme would require a digital signature management system to ensure the availability of the signature over time"*. "A/CN.9/630/Add.1", par. 28.

ou extravio dos dados de assinatura eletrónica, nomeadamente a chave privada, bem como o acesso ou o perigo de acesso de terceiros a esses dados.[585]

A suspensão dos certificados deve ocorrer logo que uma entidade certificadora receba um pedido de revogação do titular e durante o período em que executa os procedimentos tendentes à decisão de revogação.

Uma das formas mais utilizadas para garantir o conhecimento pelos terceiros interessados de que os certificados foram suspensos ou revogados é a existência de registos de certificados que estejam nessa situação, a par da existência de registos de certificados vigentes.[586]

Em correspondência, devem as assinaturas eletrónicas conter uma marca temporal, da qual conste a data e a hora em que o documento foi assinado ou a transações eletrónica foi efetuada, para se poder auditar, no futuro, se nessa data e hora o certificado era válido e estava vigente. Essa marca designa-se selo temporal, e a sua colocação nas assinaturas eletrónicas mais um dos serviços que é prestado pelas entidades certificadoras.[587]

A LMAE não estabelece normas rígidas no que respeita à rapidez com que o titular da assinatura eletrónica deve comunicar ao prestador de serviços o pedido de revogação do certificado na sequência da sua exposição a um acesso ilegítimo de terceiros. Também não estabelece prazos para que o prestador de serviços proceda à sua revogação e à disponibilização da informação correspondente nas listas públicas de revogação. Esses dois atos de comunicação e o de revogação são fundamentais para a confiança dos agentes e a fiabilidade de todo o sistema de assinaturas eletrónicas.

A LMAE estabelece, porém, a obrigação de o titular da assinatura eletrónica qualificada informar, *"sem dilação indevida"*, que os seus dados de criação de

---

[585] Os anteprojetos da LMAE chegaram a contemplar uma disposição normativa que estabelecesse a previsão dos pressupostos da revogação e da suspensão dos certificados, mas foi entendido que se trataria de normas com elevado grau de pormenor, que não seriam necessárias, pelo que foram eliminadas da sua versão final. *"The suggestion was made that all three articles could be deleted on the grounds that: they were too specific, detailed and limited in their application"*. "A/CN.9/454", par. 165.

[586] A LMAE prevê a obrigação de as entidades certificadoras disponibilizarem a todos os interessados, nomeadamente os terceiros que confiam, listas de certificados vigentes e válidos, que estejam acessíveis, em registos que são designados como registos centralizados, na alínea c) iii) do n.º 1 do artigo 9.º. Do mesmo modo estabelece que estas entidades devem também disponibilizar em registos centralizados, a todos os terceiros que confiam, listas de certificados revogados ou que não estão válidos, na alínea d) do n.º 1 do artigo 9.º. *"Yet another suggestion was that, among its basic duties, the certification authority should be under an obligation to operate a certificate revocation list (CRL)"*. "A/CN.9/457", par. 113.

[587] *"Reliably time stamped to allow the verifier to determine whether the digital signature was created during the "operational period" stated in the certificate"*. "A/CN.9/630/Add.1", par. 22.

assinatura ficaram em risco, incorrendo em responsabilidade em caso negativo.[588] Do mesmo modo os prestadores de serviços asseguram que a informação que disponibilizam relativamente ao ciclo de vigência e de gestão dos certificados está atualizada, incorrendo em responsabilidade em caso de incumprimento. Essa responsabilidade inclui a disponibilização dos meios para que os titulares de assinatura possam comunicar as situações de risco ou de acesso indevido e para que os terceiros possam consultar as listas de certificados vigentes e revogados.[589] A Diretiva 1999/93/CE estabeleceu esse regime de responsabilidade como sendo o mínimo obrigatório que as legislações dos Estados Membros devem adotar, de relativamente às assinaturas eletrónicas qualificadas consagrarem a responsabilidade das entidades certificadoras, salvo quando provem que atuarem com a devida diligência.

A lei espanhola da assinatura eletrónica de 2003,[590] prevê a extinção dos certificados a pedido do seu titular, bem como quando tenham sido violados ou colocados em perigo a segurança e o segredo dos instrumentos de criação da assinatura (a chave privada e o próprio dispositivo), ou os dados detidos pela entidade certificadora. Extingue-se ainda o certificado, nomeadamente, pelo decurso do prazo de validade, por decisão judicial, pelo falecimento do titular e por cessação da atividade da entidade prestadora de serviços.[591]

A produção de efeitos da extinção ocorre, nos casos de extinção do período de validade, na data respetiva e, nos restantes casos, na data em que a entidade certificadora publicitar a revogação no serviço de publicitação eletrónica que deve constar em diretório próprio.

A lei espanhola prevê ainda a suspensão dos certificados entre a data do pedido de revogação e a data da publicação desta.[592] Também a suspensão produz efeitos a partir da data da sua publicitação no diretório eletrónico disponibilizado para o efeito na Internet, pela entidade prestadora de serviços.

A lei portuguesa tem um regime idêntico de suspensão e de revogação dos certificados, relevando os casos em as informações deles constantes eram, ou deixaram de ser erróneas ou falsas, ou quando a confidencialidade dos dados de criação de

[588] Alínea b) do n.º1 e n.º 2 do artigo 8.º da LMAE.
[589] Alíneas b), c) e d) do n.º 1 e n.º 2 do artigo 9.º da LMAE.
[590] Ley 59/2003, de 19 de diciembre, de firma eletrónica.
[591] Artículo 8.º da Ley 59/2003, de 19 de diciembre, sob o título *"Extinción de la vigencia de los certificados eletrónicos"*.
[592] Artigo 9.º da Ley 59/2003, de 19 de diciembre.

assinatura não está assegurada.[593] A suspensão ocorre no período que decorre desde a deteção das situações que geraram a dúvida acerca da fiabilidade dos dados ou da confidencialidade, até que esses factos se confirmem, caso em que o certificado é revogado. Não estabelece, porém, a lei portuguesa, um prazo nem o modo para os prestadores de serviços de certificação procederem à suspensão ou à revogação dos certificados.

O Regulamento EIDAS estabelece um prazo limite, de 24 horas, para os prestadores de serviços publicitarem a revogação dos certificados, contando-se esse prazo desde o momento em que essa revogação foi solicitada. Esta norma é importante porque estabelece um limite rigoroso que salvaguarda os interesses de terceiros, que só com a publicitação conhecem essa revogação, e também porque não existiam anteriormente prazos fixos.[594]

O Regulamento estabelece ainda o princípio da irreversibilidade da revogação dos certificados qualificados, no n.º 4 do artigo 28.º, bem como a usa invalidade durante o período de suspensão nos casos em que esta tenha ocorrido (n.º 5 do artigo 28.º).

Uma importante inovação do mesmo Regulamento é a possibilidade de a verificação da validade dos certificados ser verificada de forma eletrónica e mesmo automática. Para isso a alínea j) do Anexo I estabelece a obrigatoriedade de os certificados qualificados contar a localização dos serviços aos quais de pode recorrer para inquirir dessa validade. Trata-se de um modelo de verificação mais eficiente, rigoroso e simples do que a tradicional existência de listas de certificados suspensos e revogados.

[593] Artigo 30.º do DL n.º 290-D/99, de 2/8.
[594] Este regime está previsto no n.º 3 do artigo 24.º do Regulamento.

Capítulo V – Identificação eletrónica e assinatura eletrónica. O regime europeu

A assinatura eletrónica nasceu como instrumento de autenticação e de juridificação das transações eletrónicas e não apenas dos documentos eletrónicos, mas a assinatura, em sentido estrito, é um conceito jurídico relativo aos documentos. Por outro lado as transações eletrónicas que deram origem à emergência do direito das assinaturas eletrónicas eram ainda transações não suportadas em documentos. É por essa razão que os primeiros instrumentos legislativos não previam especificamente a existência das assinaturas eletrónicas, mas apenas regimes de equivalência das transações eletrónicas às transações não eletrónicas. Só mais tarde surge o conceito de assinatura eletrónica. E quando este conceito surge, a sua abrangência é também genérica a todas as transações eletrónicas.

O Regulamento EIDAS vem redefinir o âmbito do conceito da assinatura eletrónica, equiparando-a à assinatura manuscrita e reserva o conceito de assinatura para

os documentos eletrónicos.[595] Analisamos, de seguida, os traços essenciais dos conceitos de assinatura eletrónica que acabámos de enunciar.

Opera-se uma verdadeira cisão dogmática entre as transações eletrónicas documentadas e as não documentadas e entre os instrumentos necessários à sua autenticação. No primeiro caso as assinaturas eletrónicas e no segundo caso a identificação eletrónica. Esta autonomização da identificação eletrónica é muito importante, porque, sem prejuízo da segurança jurídica, permite uma maior flexibilidade e simplicidade no comércio eletrónico.

Dedicamo-nos neste capítulo ao estudo da identificação eletrónica.

A identificação eletrónica era apresentada como o instrumento fundamental para eliminar os problemas de interoperabilidade dos sistemas de assinatura eletrónica nos vários Estados Membros da UE, nomeadamente os que resultam da fragmentação existente entre os regimes jurídicos de identificação e de autenticação eletrónicas existentes nos vários Estados Membros. Eliminar esta fragmentação era considerado um instrumento fundamental para a sedimentação de um novo conceito de cidadania digital.[596] Era também considerada um instrumento fundamental para a criação de uma verdadeira cidadania europeia.[597] Foram apresentados como exemplos os problemas de falta de reconhecimento dos sistemas de autenticação de um estado membro nos outros, nos casos da submissão eletrónica de candidaturas a concursos públicos por agentes económicos candidatos sedeados noutros Estados Membros, bem como o acesso aos dados de saúde de um cidadão que se desloca aos serviços de saúde de outro estado membro, e ainda a possibilidade de um estudante efetuar a matrícula numa universidade de outro estado membro, utilizando o mesmo sistema de identificação que usa no seu país.[598] Do mesmo modo é apresentada como exemplo a possibilidade de um cidadão de

[595] A definição do Regulamento é a seguinte: *"«Assinatura eletrónica»: os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar".* N.º 10 do artigo 3.º do Regulamento EIDAS).

[596] Refere-se neste documento, a adoção de medidas no sentido de *"further address esignatures and to ensure mutual recognition of e-identification (eID) and e-authentication so as to eliminate fragmentation and lack of interoperability, enhance digital citizenship and prevent cybercrime"*. SWD(2012) 136 final, ponto 1.

[597] A origem da ideia de uma identidade eletrónica europeia radica no designado Programa de Estocolmo, onde se declara, nomeadamente que *"A mobilidade deve ser reforçada eliminando os obstáculos que ainda se deparam aos cidadãos quando decidem exercer o seu direito à livre circulação indo estudar, trabalhar, criar uma empresa, fundar uma família ou reformar-se num Estado-Membro diferente do seu país de origem".* COM(2010) 171 final, pág. 4.

[598] Como exemplo da necessidade de um sistema de identificação eletrónica que seja interativo no plano europeu, foi apresentado na proposta de Regulamento foi o da saúde em linha, aprovada pela Diretiva 2012/24/EU, de 9/3. Para se alcançar a praticabilidade desse desiderato é essencial a possibilidade de a identificação e a autenticação do serviço de origem, possa ser utilizada pelos cidadãos no serviço onde

um país apresentar uma declaração para efeitos fiscais noutro estado membro, utilizando o sistema de autenticação que usa no seu país de origem.

O Regulamento viria a ser aprovado em 2014[599] e representa um importante marco no direito da segurança jurídica na utilização dos suportes eletrónicos. Pela primeira vez estabelece-se uma separação entre a assinatura eletrónica e a identificação eletrónica, autonomizando-se esta daquela e criando-se um quadro jurídico específico que a regula.[600]

No que respeita à identificação eletrónica estabelece-se um regime de reconhecimento mútuo de alguns meios de identificação eletrónica entre os Estados Membros. Esse reconhecimento assenta no princípio de que os serviços eletrónicos das administrações públicas dos Estados Membros podem utilizar, para fins de identificação e de autenticação dos respetivos utilizadores, os meios de identificação produzidos noutros Estados Membros, desde que se cumpram um conjunto de requisitos.

Esse reconhecimento é um dever jurídico, estabelecido imperativamente pelo n.º 1 do artigo 6.º do Regulamento, pelo que o serviço público correspondente deve aceitar que os cidadãos utilizam, para se identificarem perante os seus sistemas eletrónicos, meios de identificação eletrónica produzidos noutros Estados Membros.

Daqui resulta que se criam as condições para que se venha a formar um direito correspondente dos cidadãos à utilização transfronteiriça, nos Estados Membros, de um único meio de identificação eletrónica. Este meio de identificação e um instrumento fundamental para o acesso a serviços eletrónicos, tanto os de natureza comercial como de natureza administrativa ou pública. A identificação é essencial para a avaliação da legitimidade e do direito ao acesso, e é, portanto, fundamental para o tráfego jurídico eletrónico.

É certo que o Regulamento não vai tão longe ao ponto de consagrar expressamente o direito a uma única identificação eletrónica europeia, mas ele decorre da submissão dos Estados e dos organismos públicos á obrigatoriedade daquele reconhecimento, apesar de ele depender de um conjunto de pressupostos, um dos quais

---

solicita o tratamento de saúde. *"O reconhecimento e a aceitação mútuos da identificação e da autenticação eletrónicas são fundamentais para tornar realidade a prestação de cuidados de saúde aos cidadãos europeus a nível transnacional. Quando as pessoas se deslocam a outro país para receberem tratamento, é necessário que os seus dados médicos estejam acessíveis nesse país. Para isso, é indispensável que exista um quadro sólido, seguro e de confiança para a identificação eletrónica"*. COM(2012) 238 final, pág. 13.

[599] Regulamento EIDAS.

[600] Esse quadro normativo é complementado pelo Regulamento de Execução (EU) 2015/1502, de 5/9/2015.

é a existência de um ato prévio de reconhecimento desses sistemas por cada Estado membro. Este direito representa um importante avanço na criação de um mercado eletrónico eficiente e seguro em todo o espaço da União Europeia.

Através dele limita-se a necessidade de os cidadãos europeus terem que se submeter à criação de novos meios de identificação eletrónica só pelo facto de mudar de estarem a utilizar serviços eletrónicos de outros Estados Membros.

Utilizando este instrumento, os cidadãos podem aceder a serviços eletrónicos de administrações públicas de outros Estados Membros mediante a utilização de um único meio de identificação eletrónica que já possuam e que utilizem num deles. Por exemplo, um cidadão português que utilize o cartão do cidadão como meio de identificação perante um serviço da administração pública portuguesa pode utilizá-lo no acesso a serviços eletrónicos das administrações públicas de outros Estados Membros. Esses serviços passam a utilizar esses meios de autenticação para verificarem a identidade do utilizador e adquirirem segurança de que se trata da pessoa cuja identidade invoca. Esta possibilidade torna mais simples e eficiente a utilização transfronteiriça de serviços eletrónicos, aumenta o universo de potenciais utilizadores desses serviços e diminui os custos das entidades prestadoras, que não necessitam de proceder à criação de novos meios de identificação. Relativamente aos utilizadores, diminui os custos que teriam que suportar se tivessem que criar novos meios de identificação de cada vez que pretendessem aceder a serviços eletrónicos das administrações de outros Estados Membros e aumenta a rapidez e facilidade de acesso aos serviços de que necessitam.

1. – Pressupostos do reconhecimento mútuo

A instituição de um sistema jurídico de reconhecimento mútuo de meios de identificação eletrónica no espaço da União Europeia depara-se, desde logo com a elevada multiplicidade de sistemas de identificação eletrónica que as entidades públicas e privadas foram criando à medida das suas necessidades.

Essa diversidade inclui os níveis da segurança que é proporcionada por cada um desses sistemas contra o risco de fraude na identificação pelos respetivos utilizadores. As entidades que prestam serviços gratuitos, por exemplo, quando disponibilizam o acesso a documentos por elas publicados e necessitam de conhecer

quem são os seus leitores, adotam sistemas que não necessitam de níveis de segurança elevados. Nesses casos a identificação dos interessados faz-se apenas mediante a indicação do seu nome e de uma palavra-chave, a partir de dados diretamente fornecidos, por via eletrónica, pelos interessados.

As entidades que prestam serviços com relevância jurídica, por exemplo entidades públicas, necessitam de utilizar sistemas mais seguros, por exemplo nos casos em que a disponibilização do acesso a procedimentos e a dados sigilosos ou pessoais detidos por essas entidades depende da prévia confirmação da legitimidade de quem pretende a eles aceder, e isso depende sempre da sua identificação. Também aqui é ainda habitual a utilização de palavras-chave, mas esses organismos adotam procedimentos de mais elevada segurança na sua geração, nomeadamente porque não se limitam a aceitar os dados fornecidos por via eletrónica pelos interessados, mas exigem a sua confirmação com documentos oficiais que provam a sua identidade, ou então, quando exigem a presença física dos interessados para efetuarem uma identificação segura e só depois emitirem a palavra-chave.

Em ambos os casos antes referidos, a palavra-chave é o único instrumento de autenticação, mediante o qual a entidade que presta o serviço eletrónico confirma a identidade do interessado. Essa singularidade é um fator de risco porque a apropriação, por um terceiro, desse instrumento, torna o sistema vulnerável à fraude.

Os níveis mais elevados de segurança de identificação pressupõem a existência de sistemas de autenticação que utilizem mais do que uma credencial, por exemplo, mediante a utilização de códigos enviados pelo sistema de autenticação para um contacto fornecido pelo utilizador. É o caso dos códigos enviados por mensagem para números de telefone previamente identificados (*token*) ou então a utilização dos designados cartões-matriz, com combinações específicas, que estão associadas apenas a uma pessoa.

Os sistemas mais avançados em matéria de segurança utilizam a criptografia, que permite também uma autenticação que usa mais do que uma credencial e permite uma autenticação dinâmica. No primeiro caso, além da existência de uma chave privada, ela está gravada num suporte material, por exemplo um cartão e o acesso a ela só é possível mediante um palavra-passe que a confirme. A criptografia permite ainda uma autenticação dinâmica, em que os dados que são utilizados para autenticação são específicos e mudam em cada vez que se invoca uma identidade, por cada transação que se efetua.

Outro modo de identificação são os biométricos, que usam credenciais físicas das pessoas que com eles se identificam.

Os sistemas de identificação e de autenticação mais seguros não têm que ser necessariamente utilizados em todas as transações, dado que em muitos casos são mais onerosos e de utilização menos simples e expedita.

Esta multiplicidade atual de sistemas de identificação é uma realidade a que o direito não pode deixar de conferir relevância, embora fosse desejável uma maior uniformização, se possível num nível elevado de segurança jurídica.

É por essa razão, e também pelas necessidades de criação de um regime jurídico europeu da identificação eletrónica, que o regulamento reconhece a relevância jurídica desses sistemas e procede à sistematização da sua eficácia jurídica em função do critério da segurança jurídica que conferem.

Essa sistematização abrange a definição do papel dos sujeitos intervenientes no processo de identificação eletrónica, as fases desse processo e os níveis de garantia se segurança jurídica dos meios de identificação eletrónica.

2. – Sujeitos

A produção de um meio de identificação eletrónica pode ser feita pelos próprios agentes económicos ou pelas entidades administrativas, sempre que disponibilizam a prestação de serviços por meios eletrónicos, através da Internet ou das chamadas redes sociais. Ao procederem dessa forma, essas entidades cumprem o duplo papel de serem produtores desses meios e seus utilizadores, sempre que as pessoas que identificam os utilizam para beneficiarem desses serviços.

Os meios de identificação eletrónica podem ser produzidos por entidades especializadas nessa função, por exemplo, prestadores de serviços de certificação, que garantem um mais elevado níveis de segurança, dadas as suas competências e eventualmente o seu reconhecimento. Podemos, assim, separar, tal como o fizemos quanto às assinaturas, os seguintes tipos de sujeitos:

1. – O titular do meio de identificação eletrónica, que o Regulamento EIDAS designa de "*utilizador*",[601] mas que também podemos designar como a pessoa

[601] N.º 5 do artigo 3.º.

que se identifica ou como a entidade ("*entity*") que invoca a sua identidade ("*identity*") através do meio de identificação;[602]

2. – O prestador de serviços de identidade eletrónica. Pode tratar-se de uma entidade especializada, por exemplo um prestador de serviços de certificação, mas pode tratar-se também de um agente económico que para proporcionar os serviços que presta por via eletrónica, exige aos interessados que lhe forneçam um conjunto de elementos de identificação para depois emitir um meio de identificação eletrónica que passam a utilizar nas transações que efetuarem. A função dos prestadores de serviços é produzirem meios de identificação, que designamos de credenciais, que depois os titulares respetivos passam a utilizar para se identificarem. Essas credenciais ou meios de identificação eletrónicos podem ser palavras-chave, chaves privadas criptográficas, bem como as peças de suporte correspondentes, como por exemplo os cartões onde são guardadas, e ainda os dados biométricos. Os prestadores de serviços podem ser apoiados por entidades de registo cuja função é apenas receberem os pedidos de emissão de meios de identificação eletrónica, identificarem e autenticarem o requerente;
3. – A parte que confia, que é aquela perante quem o titular se identifica, e que normalmente é um agente económico ou uma entidade pública que prestam serviços eletrónicos. No passado era comum cada uma destas entidades possuir o seu próprio sistema de identificação eletrónica, mas isso é insustentável, porque inseguro, oneroso e um fator de dificuldade para o comércio eletrónico. Por essa razão é do interesse da segurança e da fluidez das relações jurídicas estabelecidas por meios eletrónicos que estas entidades aceitem, cada vez mais, utilizar sistemas de identificação eletrónica comuns ou de outras entidades, passando elas a ser apenas entidades que confiam nos meios e nos sistemas produzidos por aquelas, por nelas confiarem. A parte que confia exige os procedimentos de identificação para prestar os serviços que os titulares dos meios de identificação lhe solicitam, e efetuam os procedimentos de autenticação. Estas partes que confiam podem também entregar a terceiros a verificação da identidade e a autenticação daquelas pessoas.
4. – Fonte qualificada – Uma entidade que seja competente e reconhecida como fiável, que identifique de forma exata uma pessoa, singular ou coletiva e emita

[602] Utilizamos os conceitos "*entity*" e "*identity*" que são utilizados pela norma internacional de segurança jurídica relativa à identificação eletrónica, Norma ISO/IEC DIS 29115.

informações ou elementos de prova que a comprovem. São entidades qualificadas, as entidades públicas competentes para a identificação civil e comercial. O papel destas entidades é relevante para simplificar o procedimento de criação dos meios de identificação eletrónica, dado que os procedimentos que estas entidades já efetuaram, de identificação e de autenticação, não necessitam de ser repetidos, dado que os documentos por elas emitidos são um sucedâneo desses procedimentos, suficientes para representarem a identidade. Uma fonte qualificada pode também ser um objeto, desde que tenha sido produzido por uma das entidades antes referida e comprove, com segurança, a identidade de uma pessoa.[603]

3. – Fases da identificação eletrónica

Embora o procedimento de identificação de uma pessoa perante outra pareça simples e intuitivo nas relações presenciais, não o é nas relações estabelecidas por meios eletrónicos, pelo que a sua regulação e a criação de normas legais que garantam a segurança jurídica pressupõem a sua prévia enunciação. Tanto o Regulamento EIDAS como o Regulamento de Execução, inspirados na Norma ISO/IEC DIS 29115 identificam 3 fases desse procedimento, que são as seguintes:

1. - A fase designada de inscrição e da identificação das pessoas, que inclui o pedido do requerente, a identidade que invoca e o procedimento da entidade que vai gerar o meio de identificação eletrónica verifica a identidade de quem o requereu e a comprova com os elementos de prova correspondentes.[604] Esta fase inclui, por sua vez, dois procedimentos distintos:
    1.1. - Aquele que se refere ao pedido de emissão de um meio identificação por uma pessoa, singular ou coletiva, e onde a entidade emitente deverá ter o cuidado de documentar esse pedido,

[603] O ponto 1 do n.º 1 do Regulamento de Execução 2015/1502, definem entidade qualificada nos seguintes termos: "*Qualquer fonte, independentemente da sua forma, que pode ser considerada fiável para fornecer dados exatos, informações e/ou elementos de prova que podem ser utilizados para comprovar a identidade*".

[604] Trata-se do procedimento que o Regulamento EIDAS designa de prova e de verificação, na alínea a) do n.º 3 do artigo 8.º do Regulamento EIDAS, e o Regulamento de Execução (EU) 2015/1502, de 5/9/2015, designa de inscrição, na alínea a) do n.º 2 do artigo 1.º.

registá-lo e recolher dois tipos de elementos necessários – elementos informativos, declarados pelo requerente e elementos documentais de prova, que deverão ser também arquivados;[605]

1.2. Aquele que se refere à comprovação, pela entidade requerida, dos elementos probatórios e da identidade do requerente. Esta comprovação deve ser suficiente para se confirmar que a identidade invocada é efetiva e verdadeira. E essa confirmação é o resultado de outras cinco – i) que a identidade invocada existe, ou seja, que não é fictícia; ii) que ela pertence àquela pessoa em concreto, e não se trata de uma tentativa de roubo de identidade de outra pessoa; iii) que essa pessoa apresenta elementos de prova da sua identidade; iv) que esses elementos são genuínos e válidos, e v) que esses elementos foram emitidos por uma fonte qualificada.[606] Esse procedimento pode incluir a verificação física dos documentos e a presença física dos requerentes. No caso em que a entidade que requer a emissão do meio de identificação é uma pessoa coletiva, aos procedimentos antes referidos haverá que acrescer os que se relacionam com a confirmação da legitimidade da pessoa singular que a requer e a representa.[607]

2. - A fase da gestão dos meios de identificação eletrónica, que inclui a sua criação, a entrega ao requerente, a sua utilização por este, a sua suspensão, revogação ou reativação e se desdobra em três domínios fundamentais:[608]

2.1. – A qualidade da produção e da geração do meio de identificação eletrónica, bem como a sua caraterização e configuração. No primeiro caso, são relevantes os procedimentos seguidos pela entidade que o produziu para garantir que só é utilizado pela pessoa

[605] Esta fase está regulada no ponto 2.1.1 do anexo ao Regulamento de Execução (EU) 2015/1502, de 5/9/2015.

[606] O n.º 1 do ponto 1 do anexo ao Regulamento de Execução define fonte qualificada como uma entidade "*fiável para fornecer dados exatos, informações e/ou elementos de prova que podem ser utilizados para comprovar a identidade*". Trata-se, normalmente, das entidades oficiais competentes para a identificação civil, no caso português.

[607] Tópicos 2.1.2, 2.1.3 e 2.1.4. do Anexo ao Regulamento de Execução que vimos citando.

[608] Alíneas b) e f) do n.º 3 do artigo 8.º do Regulamento EIDAS e alínea b) do n.º 2 do artigo 2.º do Regulamento de Execução (EU) 2015/1502, de 5/9/2015.

que identifica, ou sob o seu controlo, de modo a prevenir ou evitar a sua utilização indevida por terceiros. Esses procedimentos, que devem ser auditáveis, devem garantir a confidencialidade dos dados, bem como a impossibilidade de a partir deles outras pessoas podere duplicar ou apropriar-se dos meios de identificação que foram produzidos. No segundo caso importa saber se esse meio contém apenas um ou mais fatores de autenticação, sendo certo que quantos mais forem esses fatores maior é a segurança;

2.2. – A emissão e entrega do meio de identificação eletrónica, no que respeita às garantias de que foi efetivamente entregue ao respetivo requerente e titular, e ficou apenas na sua posse. A geração do meio de identificação deve garantir que não será conhecido pela entidade que o produziu ou por outrem a partir. Do mesmo modo a sua entrega ao titular que o requereu deve ser segura, e não ocorrer, por exemplo por via telefónica, nem mediante um mecanismo de transmissão ou de transporte que não dê garantias de chegar apenas ao titular;

2.3. – Os procedimentos estabelecidos de suspensão, revogação, reativação, renovação e substituição dos meios de identificação eletrónica, em especial as garantias de que não deverão ser utilizados enquanto suspensos ou revogados;

3. – A fase da autenticação, que corresponde a cada momento que, em concreto, cada utilizador invoca a sua identidade e utiliza as suas credenciais mediante o meio de identificação, para a demonstrar. Corresponde também, do lado da entidade perante quem a identidade é invocada, aos procedimentos que esta utiliza para a comprovar e se certificar dela. A autenticação desenvolve-se em 3 domínios fundamentais:

3.1. - Antes de mais, pela verificação de que o meio de identificação é válido;

3.2. - A segurança de que os dados de identificação pessoal que constam do meio de identificação (por exemplo o cartão de onde consta a chave privada) estão seguros e protegidos contra perdas, fuga ou acesso indevido;

3.3. – O meio de identificação está protegido contra o acesso indevido às credenciais, nomeadamente através de escutas (por exemplo nos casos de palavras-chave comunicadas por telefone), adivinhação ou reprodução.

4. – Gestão e organização. Tanto os sujeitos envolvidos no sistema de identificação eletrónica como os produtos e as fases do procedimento de identificação estão subordinados a um conjunto de obrigações e procedimentos de segurança, de avaliação de risco e de controlo, nomeadamente nos seguintes domínios:

4.1. – Os prestadores de serviços de identificação eletrónica são sempre entidades públicas ou entidades privadas reconhecida com competência pelo direito nacional, com capacidade para assumirem riscos e suportarem os encargos financeiros correspondentes à responsabilidade em que incorrem, incluindo nos casos em que subcontratem os serviços da sua competência;

4.2. – Os prestadores de serviços fornecem aos utilizadores a informação relativa aos termos e condições de prestação desses serviços, incluindo as taxas cobradas e a política de proteção da privacidade;

4.3. – Gestão da segurança da informação. Os prestadores de serviços devem possuir protocolos que prevejam o modo de proteção da informação e dos dados de suporte à produção dos meios de identificação eletrónica, bem como planos de contingência previstos para os casos em que ocorrer a sua vulneração. Esses planos incluem a informação de registo e a proteção dos dados pessoais, bem como o arquivo dos dados e a sua conservação, incluindo para fins de auditoria

4.4. – Existem controlos técnicos destinados a garantir a confidencialidade, a integridade e a disponibilidade da informação, incluindo os canais de comunicação utilizados para a comunicação de dados pessoais, bem como a segurança do material criptográfico utilizado;

4.5. – Os prestadores de serviços devem ser sujeitos a auditorias, tendo em vista o controlo e a verificação dos procedimentos estabelecidos.

4. – Níveis de garantia dos meios de identificação eletrónica

A tipificação de níveis de garantia dos meios de identificação eletrónica avalia a sua resistência aos riscos de utilização indevida, nomeadamente com a criação de identidades fictícias, falsas ou contra o designado roubo de identidade. Estes riscos, que são sempre comuns a todos os tipos de identificação eletrónica, devem ser sempre avaliados em conjugação com os prejuízos que podem ser causados em função da sua utilização em concreto. Assim, quando se trate do fornecimento do mero acesso a uma publicação periódica de caráter público, por exemplo um jornal eletrónico de acesso pago, os riscos envolvidos são sempre reduzidos, quando comparados com o acesso, proporcionado por uma entidade bancária, à movimentação de fundos numa conta bancária, ou ainda, pelo acesso, proporcionada por uma entidade, aos rendimentos e às despesas (por exemplo de saúde) declarados para efeitos fiscais por um sujeito passivo de imposto.

Ao mesmo tempo, esta tipificação servirá para aumentar a confiança no ambiente eletrónico como base para o estabelecimento de relações jurídicas, permitindo ainda aos prestadores de serviços, públicos e privados, determinar os níveis de segurança em que devem postular as suas exigências de identificação aos sujeitos das relações jurídicas que estabelecem.

Finalmente a tipificação proporciona as condições para que os órgãos das administrações públicas aceitem que os cidadãos que as demandam eletronicamente utilizem meios de informação eletrónica gerados noutros Estados Membros, desde que o seu nível de garantia seja igual ou superior àquele que é por eles exigido. Essa aceitação é estabelecida imperativamente pelo Regulamento EIDAS, como mais adiante veremos.

NA tipificação dos níveis de garantia, o Regulamento inspirou-se na Norma ISO/IEC DIS 29115, embora não a siga na sua totalidade, dado que esta prevê a existência de 4 níveis e o Regulamento só consagra os seguintes três:[609]

[609] A Norma ISO/IEC DIS 29115 prevê a existência dos níveis de garantia ("*levels of assurance*") de 1 a 4, sendo o primeiro aquele em que o nível de garantia da identidade declarada é mínimo (*"little or no*

1. – Nível de garantia reduzido – corresponde genericamente aos dois níveis mais baixos daquela Norma, sendo o nível de confiança no meio de identificação eletrónica, limitado e a sua finalidade de apenas reduzir o risco de utilização ou alteração indevida.[610] [611]

   1.1. - Relativamente à fase de inscrição e da identificação, para a prova da identidade basta, as exigências estão ao nível a aparência, sem confirmação, bastando que se possa considerar que o utilizador está na posse dos elementos de prova, sem se exigir a sua verificação nem se estabeleçam condições acerca da natureza dos elementos probatórios;

   1.2.– Relativamente fase da gestão dos meios de identificação eletrónica, exige-se apenas que esses meios possuam um fator de autenticação, que as caraterísticas desses meios permitem aos utilizadores tomar as medidas razoáveis para só serem utilizados por eles ou sob o seu controlo, e que depois de produzidos foram entregues por meio que permite apenas "*presumir*" que chegaram à pessoa a quem se destinam, ou seja o seu titular e não outra pessoa;

   1.3.– No que respeita à autenticação, exige-se que além dos requisitos aplicáveis ao nível reduzido, o mecanismo de autenticação efetue uma verificação fiável da existência e da validade do meio de identificação utilizado e que execute os procedimentos de segurança que garanta ser "*altamente improvável*" a sua vulnerabilidade à descoberta das credenciais mediante a adivinhação, escutas não autorizadas, reprodução ou manipulação por intrusão "*com capacidade de ataque básica-reforçada*".

---

confidence"); o segundo aquele em que existe uma certa confiança acerca da autenticidade (*some confidence*); no nível 3 existe uma grande confiança (*high confidence*) e no nível quatro essa confiança é muito elevada (*very high confidence*). (Ponto 6).

[610] Alínea a) do n.º 2 do artigo 8.º do Regulamento EIDAS.

[611] Utilizamos como base, além das normas citadas do EIDAS, o anexo do Regulamento de Execução (EU) 2015/1502, de 5/9/2015. Este regulamento inspira-se na Recomendação da UIT ITU. (2012). Entity authentication assurance framework; Recommendation ITU-T X.1254, International Telecommunication Union; SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY. Cyberspace security – Identity management. Consulta a 26/11/2015. Em: file:///C:/Users/jp01918/Downloads/T-REC-X.1254-201209-I!!PDF-E.pdf.

2. – Nível de garantia substancial – O nível de confiança é classificado de substancial e a sua finalidade é reduzir substancialmente aquele risco.[612] Essa qualificação resulta dos seguintes fatores:

2.1. - Relativamente à fase de inscrição e da identificação, para a prova da identidade, as exigências estão ao nível da confirmação mediante elementos de prova. Exige-se, em primeiro lugar, que se "*verifique*" que o requerente "*está na posse dos elementos de prova reconhecidos pelo Estado Membro*". Para isso é necessário que se esses elementos sejam efetivamente apresentados, por exemplo, um documento de identificação emitido por uma entidade qualificada que se constate a sua existência, validade e genuinidade.[613] Em segundo lugar, é necessária a constatação de que esses elementos "*representam a identidade declarada*";

2.2. – Relativamente fase da gestão dos meios de identificação eletrónica exige-se apenas que esses meios possuam pelo menos dois fatores de autenticação, que esses meios de autenticação sejam concebidos de forma que permita "*presumir*" que só são utilizados pela pessoa a quem pertencem ou sob o seu controlo, e que depois de produzidos foram entregues por meio que permite não apenas "presumir" que chegaram, mas também que "ficaram na posse" da pessoa a quem se destinam;

2.3. – No que respeita à autenticação, exige-se que além dos requisitos do nível reduzido, a verificação da existência e da validade do meio de identificação utilizado seja efetuada mediante uma autenticação

[612] Alínea b) do n.º 2 do artigo 8.º do Regulamento EIDAS.

[613] Normalmente estes procedimentos de identificação do requerente exigem a presença física do requerente perante a entidade de registo ou o prestador de serviços de certificação, bem como a verificação efetiva dos elementos de prova da identidade, mas pode não ser necessariamente assim. O Regulamento de Execução permite que estas entidades aceitem, para a criação de meios de identificação eletrónica, como sucedâneo dessa forma mais efetiva de identificação, documentos emitidos por entidades que já tenham adotado esses procedimentos. Essa possibilidade é admitida tanto nos casos em que esses procedimentos foram efetuados para os fins de emissão de meios de identificação eletrónica como para outros fins de identificação, por exemplo, para a identificação civil e comercial. (ponto2.1.2 do anexo ao Regulamento). Dispensa-se, assim, a repetição sucessiva dos procedimentos de comprovação da identidade do requerente, beneficiando-se de procedimentos já anteriormente efetuados por fontes qualificadas ou por entidades certificadas, com a condição de terem sido adotados procedimentos considerados com níveis de garantia substancial ou elevado. Exige-se, porém, uma certificação de que o procedimento de comprovação efetuado é equivalente, efetuada por um organismo de avaliação da conformidade. Essa certificação não é necessária quando a comprovação da identidade seja de carácter eletrónico e tenha sido efetuada para a produção de meios de identificação eletrónica que tenham sido notificados nos termos do regulamento EIDAS.

dinâmica, normalmente com utilização de meios criptográficos e que execute os procedimentos de segurança que garanta ser "*altamente improvável*" a sua vulnerabilidade à descoberta das credenciais mediante a adivinhação, escutas não autorizadas, reprodução ou manipulação por intrusão "*com capacidade de ataque moderada*".

3. Nível de garantia elevado - O nível de confiança é muito elevado e a finalidade é evitar a utilização ou alteração indevida da identidade.[614] Essa qualificação resulta dos seguintes fatores:

   3.1. - Relativamente à fase de inscrição e da identificação, para a prova da identidade, as exigências estão ao nível da comprovação especificada, mediante elementos de prova qualificados. Exige-se que essa comprovação seja efetuada fisicamente e conduza à conclusão de que o requerente está na posse efetiva dos seguintes elementos de identificação:

      3.1.1. – Com fotografia ou dados biométricos;

      3.1.2. – Que tratando-se de dados biométricos, sejam reconhecidos pelo Estado Membro onde se efetua o pedido;

      3.1.3. – Que os elementos de prova representem a identidade declarada;

      3.1.4. – Que se efetue uma confirmação da validade dos elementos de prova de identidade apresentados, ou seja, que não estão caducos, suspensos ou revogados;

      3.1.5. – Que essa confirmação seja efetuada mediante fonte qualificada, ou seja, uma entidade com competência e fiabilidade para fornecer dados exatos de identificação e para comprovar a identidade;

      3.1.6. - Que a identidade invocada pelo requerente foi confirmada mediante confrontação das suas caraterísticas físicas com uma fonte qualificada, ou seja, com dados

[614] Alínea c) do n.º 2 do artigo 8.º do Regulamento EIDAS.

exatos de identificação produzidos por uma entidade competente para ela.[615]

3.2. – Relativamente fase da gestão dos meios de identificação eletrónica exige-se que, além dos requisitos aplicáveis para os níveis reduzido e substancial, o meio de identificação eletrónica "*protege contra a duplicação e a manipulação, bem como contra ataques de elevado potencial*". Mais se exige que protejam contra a utilização por terceiros, e a segurança de que depois de produzidos foram efetivamente entregues e ficaram na posse da pessoa a quem se destinam;

3.3. – No que respeita à autenticação, exige-se que além dos requisitos do nível substancial, o mecanismo de autenticação efetue uma verificação da existência e da validade do meio de identificação utilizado e que execute os procedimentos de segurança que garanta ser "*altamente improvável*" a sua vulnerabilidade à descoberta das credenciais mediante a adivinhação, escutas não autorizadas, reprodução ou manipulação por intrusão "*com capacidade de ataque elevada*".

5. – Requisitos do reconhecimento mútuo pelos Estados Membros

A utilização, pelos cidadãos ou pelas empresas, da sua identificação eletrónica, para a realização de transações eletrónicas em Estados Membros diferentes daquele onde foram produzidos os respetivos meios de identificação eletrónica, depende de um ato de reconhecimento expresso, por este último Estado (que designamos Estado Reconhecedor), da validade daqueles meios de identificação eletrónica produzidos noutros Estados Membros (que designamos Estado Produtor).

[615] Estes procedimentos não necessitam de ser repetidos para os fins de emissão de meios de identificação eletrónica, nos casos em que tenham sido efetuados por uma entidade com competência para a identificação, mas esse requisito tem que ser confirmado por um organismo de avaliação da conformidade e foram dotadas medidas para demonstrar que esses procedimentos continuam válidos. Do mesmo modo, se esses procedimentos foram seguidos anteriormente na produção de outros meios de identificação eletrónicos, não necessitam de ser repetidos na criação de outros meios desse tipo, nos casos, em que tenham sido notificados ou que, não o tendo sido, se efetue aquela avaliação por um organismo de avaliação de conformidade. (Ponto 2.1.2 do Regulamento de Execução 2015/1502).

Este ato ocorre no final de um procedimento composto por várias diligências, que sistematizamos do seguinte modo:

1. – A disponibilização, pelo Estado Produtor aos restantes Estados, de uma descrição do sistema de identificação eletrónica que se propõe disponibilizar para ser utilizado noutros Estados Membros. Esta disponibilização serve para que as entidades públicas dos futuros Estados Reconhecedores conheçam as caraterísticas técnicas do sistema e o seu grau de interoperabilidade com os seus próprios sistemas, bem como as garantias de segurança que oferece. Este conhecimento é importante para essas entidades efetuarem os ajustamentos aos seus sistemas informáticos que venham a permitir que ambos os sistemas interajam de forma eletrónica e automática;[616]
2. - A notificação, pelo Estado Produtor, do sistema de identificação eletrónica à Comissão Europeia, nos termos do artigo 9.º. A notificação é uma faculdade que os Estados Membros são livres de adotar ou não, porque o Regulamento não obriga os Estados a fazê-la. Porém, essa notificação será sempre vantajosa para os Estados Membros, que assim prestam um melhor serviço aos seus cidadãos. Na verdade, para os Estados Membros, é sempre melhor que os seus cidadãos utilizem os sistemas neles produzidos para se identificarem e autenticarem tanto internamente como nos restantes Estados Membros. Para os cidadãos é vantajoso que possam utilizar em todo o espaço europeu os meios de identificação que já possuem. Do mesmo modo, existindo mais do que um sistema de identificação eletrónica, a escolha daqueles que são notificados é também uma faculdade dos Estados, mas será sempre do interesse dos Estados Membros notificar todos os sistemas, pelo menos aqueles que gerem meios de identificação substanciais ou qualificados. O Regulamento só aceita que sejam notificados sistemas de identificação eletrónica que cumpram um conjunto de requisitos, que são essenciais à sua operacionalidade e segurança jurídica, e que são os seguintes:
    2.1. - Que os meios de identificação eletrónica sejam produzidos por entidades públicas ou reconhecidas pelo estado membro notificante

[616] Esta disponibilização está prevista na alínea g) do artigo 7.º do Regulamento EIDAS e deve ocorrer no mínimo seis meses antes da notificação do sistema à Comissão Europeia, prevista no artigo 9.º.

(alínea a) do artigo 7.º). Esta exigência cumpre o propósito do Regulamento, de colocar os Estados a liderar o esforço de criação de um sistema europeu de autenticação. Admite-se, porém, que estes sistemas venham a ser utilizados de forma transfronteiriça pelas empresas privadas, como estabelece a segunda parte da alínea f) do artigo 7.º);

2.2. - Os sistemas de identificação que produzem os meios de identificação cumpram um nível de garantia elevado, substancial ou reduzido, tal como são definidos pelo artigo 8.º do Regulamento e que o Estado notificante, bem como a entidade que os produziu, garantem que os dados de identificação eletrónica são atribuídos de acordo com esses níveis (alíneas c), d) e e) do atrigo 7.º);[617]

2.3. Que o Estado notificante garanta a possibilidade de autenticação em linha. Esta garantia é muito importante, porque quando um cidadão se identificar perante um serviço em linha de outro Estado Membro, o respetivo sistema informático terá que interagir com aquele que gerou o meio de identificação, para que seja efetuada a autenticação (alínea f) do artigo 7.º).

3. – A publicação, pela Comissão Europeia, da lista dos sistemas notificados, que deverá ocorrer no prazo de dois meses após a notificação;[618]

4. – O reconhecimento, pelo Estado Reconhecedor do sistema publicado nos termos antes referido. Este reconhecimento deve ocorrer no prazo máximo de 12 meses após a publicação da lista da Comissão antes referida.[619]

O Regulamento EIDAS estabelece dois tipos de reconhecimento, sendo um deles obrigatório e o outro facultativo, como analisamos de seguida.

5.1. – Reconhecimento facultativo

[617] As especificações que devem respeitar estes meios foram definidas pelo Regulamento de Execução (EU) 2015/1502, de 5/9/2015.
[618] A primeira publicação dos sistemas foi já efetuada, após a publicação do Regulamento de Execução 2015/1502, como estabelece o n.º 2 do artigo 9.º do Regulamento EIDAS, devendo as futuras publicações de novos sistemas notificados ser efetuadas nos termos do n.º 3 do mesmo artigo.
[619] Parte final do n.º 1 do artigo 6.º do Regulamento EIDAS.

O reconhecimento é facultativo relativamente aos meios de identificação cujo nível de garantia seja reduzido. A utilização transfronteiriça desses meios de identificação não é prioritária para a construção do mercado digital europeu, dado que cumprem os respetivos requisitos a generalidade dos sistemas de identificação eletrónica, e as dificuldades resultantes da fragmentação ocorrem nos casos em que os Estados Membros impõem restrições, mediante a imposição de exigências técnicas adicionais, à utilização de sistemas de outros países. A tipificação dos níveis de garantia tem por objetivo impedir essa prática, sendo que o Regulamento impede os Estados Membros de imporem requisitos técnicos desproporcionados que dificultem a interoperabilidade, na parte final da alínea f) do artigo 7.º do Regulamento EIDAS.

O reconhecimento facultativo que se aplica aos meios de identificação com nível de garantia reduzido não depende dos Estados Membros, mas dos órgãos da administração pública que prestam os serviços eletrónicos demandados pelos cidadãos.

5.2. – Reconhecimento obrigatório

O reconhecimento obrigatório, pelos Estados Membros, é o mais importante efeito do Regulamento EIDAS no que respeita à identidade eletrónica, porque é dele que resulta a criação do quadro jurídico que funda o direito dos cidadãos a utilizarem, no limite, um único meio de identificação eletrónica para acederem a todos os serviços prestados em linha pelas administrações públicas dos Estados Membros.

O Regulamento centra os seus efeitos imperativos nos meios de identificação com nível elevado e substancial, porque são eles que poderiam criar entraves à eficácia do direito à utilização transfronteiriça e também porque são eles que garantem um mais elevado nível de confiança dos agentes, dada a sua mais elevada segurança contra os riscos de utilização indevida.

O reconhecimento obrigatório tem um âmbito objetivo e um âmbito subjetivo. Relativamente ao âmbito objetivo, a obrigatoriedade abrange os meios de identificação que cumpram cumulativamente todos as seguintes condições:

i) Tenham sido previamente notificados pelos Estados Membros à Comissão Europeia e por esta publicitados (alínea a) do n.º 1 do artigo 6.º)[620];

ii) Sejam utilizados num serviço público do Estado notificante (n.º 1 do artigo 6.º), sendo essa uma consequência do facto de o Regulamento EIDAS seguir uma estratégia de criar um sistema europeu de interoperabilidade a partir dos serviços das administrações públicas, tendo em vista o seu posterior alargamento aos mercados eletrónicos transnacionais, para assim se alcançar um mercado único eletrónico europeu. Porém, esse alargamento será sempre voluntário, dependendo do interesse das empresas em utilizar meios de identificação notificados. É também uma regra de prudência, porque os sistemas de identificação eletrónica dependem sempre dos sistemas de identificação civil e comercial, de natureza pública;

iii) Tenham um nível de garantia substancial ou elevado (Alíneas b) e c) do n.º 1 do artigo 6.º);[621]

Relativamente ao âmbito subjetivo, estão obrigados ao reconhecimento todos os Estados Membros que possuam órgãos da administração pública que prestem serviços em linha que utilizem meios de identificação eletrónica que exijam níveis de garantia substancial ou elevado. Esta obrigatoriedade subjetiva destina-se a evitar que os

[620] O carácter voluntário da notificação está expresso nos considerandos do Regulamento EIDAS, em cujo ponto 13 se menciona que "*Os Estados-Membros não deverão ser obrigados a notificar os seus sistemas de identificação eletrónica à Comissão*". E mais adiante, no ponto 17: "*Os Estados-Membros deverão incentivar o setor privado a utilizar voluntariamente meios de identificação eletrónica que integrem um sistema notificado para fins de identificação*". Porém, essa notificação é vantajosa, como anteriormente referimos, tanto para os Estados Produtores como para os cidadãos que já utilizam internamente esses sistemas

[621] Estes níveis de garantia reportam-se à segurança com que os meios de identificação eletrónica identificam de novo unívoco o respetivo titular. Esses níveis de segurança reportam-se sempre ao risco de utilização indevida dos meios de identificação eletrónica, nomeadamente o risco de um terceiro os utilizar, fazendo-se passar por outra pessoa e com isso conseguindo aceder a serviços a que só teria direito o seu legítimo titular e praticar eventualmente atos com relevância jurídica em seu nome. Esse risco existe sempre, particularmente nos suportes eletrónicos. A tipificação dos níveis de segurança corresponde aos graus de intensidade com que esses riscos são diminuídos. Os níveis de garantia são especificados no artigo 8.º do Regulamento e no Regulamento de Execução (EU) 2015/1502, de 5/9/2015, que os segmenta em 3 categorias, correspondendo o primeiro ao nível de garantia reduzido, o segundo substancial e o terceiro elevado. No primeiro caso estão os meios em que esses riscos são reduzidos, no segundo aqueles em que são substancialmente reduzidos e, no terceiro, aqueles que são adequados a evitar esses riscos. O Regulamento de Execução enuncia as especificações técnicas que, para alcançarem esses níveis, devem ser observadas nas diversas fases do procedimento de identificação, desde os procedimentos de produção dos meios de identificação (inscrição, recolha, verificação e registo dos elementos de identificação, procedimentos de geração e ativação dos meios de identificação), aos de verificação e prova da identificação, aos mecanismos de autenticação e às garantias de segurança oferecidas pelas próprias entidades que produzem os meios de identificação.

Estados Membros recorram à exigência de níveis de garantia substancial ou elevado como instrumento para evitar o reconhecimento e a interoperabilidade.[622] O reconhecimento obrigatório habilita imediatamente os cidadãos que possuam meios de identificação com níveis de garantia igual ou superior, mesmo que gerados noutros Estados Membros, a utilizá-los para se identificarem eletronicamente, perante os serviços eletrónicos disponibilizados pelo Estado Reconhecedor.

O ato de reconhecimento terá que se praticado no prazo máximo de 12 meses depois da publicação, pela Comissão, do sistema notificado (parte final do n.º 1 do artigo 6.º). Embora o Regulamento não estabeleça qualquer sanção para os Estados que não cumpram esta obrigatoriedade ou violem o prazo de reconhecimento, trata-se de uma norma imperativa, a que os Estados estão obrigados, cabendo à comissão velar pelo seu cumprimento efetivo.

Esta obrigatoriedade revela a vontade do legislador europeu de promover, mediante uma liderança dos poderes públicos, a criação do chamado mercado digital europeu. Alcança-se, desta forma, o objetivo de eliminar a segmentação dos mercados, provocadas pela imposição de exigências técnicas pelos órgãos da administração pública a fim de evitarem a utilização de meios de identificação eletrónica geridos por terceiros.

O Regulamento protege ainda os cidadãos contra eventuais tentativas dos Estados Membros de dificultarem a utilização de meios de identificação gerados noutros Estados, proibindo expressamente a imposição de requisitos técnicos desproporcionados que dificultem ou impeçam, quer a utilização transfronteiriça daqueles meios, quer a interoperabilidade dos respetivos sistemas (parte final da alínea f) do artigo 7.º).

5.3. – Interoperabilidade

O regime de identificação eletrónica no espaço da União Europeia assenta nos sistemas de identificação de cada Estado Membro. É sobre eles que opera o princípio do reconhecimento mútuo que é a base jurídica fundamental do Regulamento. Mas a operacionalidade do sistema depende da capacidade de os sistemas informáticos se conexionarem e interagirem de forma automatizada, em especial os sistemas autenticadores e os sistemas produtores de meios de identificação eletrónica.

[622] Esta obrigatoriedade consta da alínea c) do n.º 1 do artigo 6.º do Regulamento EIDAS.

Em termos práticos, a operação de comprovação da identificação de uma pessoa (autenticação) que se apresenta perante um sistema informático para receber a prestação de um serviço, é efetuada em dois passos seguidos:

i) Primeiro a pessoa invoca a que identidade perante o sistema. Essa invocação é feita mediante a introdução de um nome (*user*), um número por que é conhecido, um endereço eletrónico, etç. Esse nome ou número de identificação está associado, no sistema informático respetivo, a um conjunto mais amplo de elementos de identificação;

ii) De seguida o sistema informático necessita de confirmar que se trata da pessoa cuja identidade é invocada, e para exige a introdução de uma credencial, normalmente uma palavra-chave, um cartão, uma chave privada, um elemento biométrico, ou seja, algo que só aquela pessoa possui ou sabe. Se essa credencial estiver correta, então está estabelecida a conexão entre o nome (user) e a confirmação da identidade da pessoa.

Esta operação é relativamente simples e imediata, mas apenas nos casos em que o sistema perante o qual a pessoa está a operar é o mesmo que produziu o meio de identificação eletrónica. Nesses casos, por ocasião da emissão desse meio, a pessoa interessada foi previamente identificada, tendo sido recolhidos elementos da sua identidade suficientes para a confirmar, por exemplo, o seu nome, número de identificação civil, fotografia, impressão digital, presença física, etç. Depois de esses elementos terem sido recolhidos e armazenados, o sistema emite o meio de identificação eletrónica, que nos casos mais comuns é composto por um nome (*user*) e uma palavra-chave. Quando essa pessoa se identifica perante esse mesmo sistema informático para efetuar uma transação, insere primeiro o seu nome (ou *user*), que o sistema já conhece, e depois a palavra-chave. Com base nos dados que possui armazenados, confirma que se trata da pessoa cuja identidade foi invocada e considera-se consumada a autenticação.

Nos casos em que o instrumento de identificação utiliza criptografia assimétrica, depois de inserir o nome (user), o utilizador aplica a chave privada sobre um suporte de dados, encriptando-o. Se o sistema o conseguir desencriptar com a chave pública que lhe está associada, confirma então que se trata efetivamente da pessoa que invoca ser, correspondendo aquela a que está associado o *user* e os restantes casos de identificação.

Os procedimentos são mais difíceis nos casos em que essa mesma pessoa se pretende identificar para efetuar transações com relevância jurídica em sistemas eletrónicos que não aquele que produziu o meio de identificação que pretende utilizar. É que, nesses casos, esse sistema não reconhece quaisquer dados que o interessado lhe apresenta, simplesmente porque não os conhece, o que torna a autenticação impossível. Era isso que ocorria no espaço europeu, nos casos em que não eram usadas assinaturas eletrónicas avançadas ou qualificadas. Na verdade, o processo de autenticação consiste em comparar dados constantes do meio de identificação eletrónica com outros dados que o sistema informático autenticador (que designamos de sistema prestador, por facilidade de expressão, por ser aquele que é demandado pelo utilizador para obter a prestação de serviços que pretende adquirir) possui nas bases de dados internas da respetiva entidade a que acede quando elas estão disponíveis noutros sistemas. E, não havendo acesso a eles, a autenticação não é possível. É esse problema que o Regulamento EIDAS pretende ultrapassar. E para isso é necessário, além da construção do instituto jurídico do reconhecimento mútuo, a criação de uma obrigação jurídica de interoperabilidade dos sistemas informáticos.

O quadro de interoperabilidade permite ultrapassar a separação entre o sistema autenticador e o sistema que produziu o meio de identificação eletrónica (que designamos, por facilidade, de sistema produtor - do meio de identificação).

Garantindo-se a interoperabilidade entre os dois sistemas, quando um utilizador demanda um sistema prestador, e esse sistema não produziu o meio de identificação eletrónica que pretende utilizar, identifica, perante ele, qual o sistema produtor, que tem que ser um dos que consta da lista publicitada pela Comissão Europeia. De seguida, o sistema prestador (autenticador) abre o sistema de identificação eletrónica do sistema produtor, para que o utilizador insira nele os elementos de identificação eletrónica. Esse sistema efetua a autenticação dos elementos desses elementos e, se a autenticação tiver sucesso, comunica ao sistema prestador a identidade do utilizador. Com base nessa informação, o sistema prestador passa a conhecer com segurança quem é a pessoa com quem está a interagir.

Para que este quadro de interoperabilidade funcione é necessário que os órgãos das administrações públicas dos Estados Membros, que prestam serviços eletrónicos, efetuem previamente a conexão eletrónica entre os seus sistemas informáticos e os sistemas informáticos das entidades que produziram meios de identificação eletrónicos. Esses trabalhos devem, tendencialmente, abranger todos os sistemas notificados e

publicitados e, sendo trabalhos complexos e morosos, devem ser efetuados antes daquela publicitação, dado que eles são indispensáveis para a interoperabilidade. É por essa razão que o Regulamento estabelece a obrigatoriedade de os Estados Membros, disponibilizarem informação relativa aos sistemas de identificação eletrónica que pretendem notificar, pelo menos seis meses antes da notificação, aos restantes Estados Membros. Essa disponibilização é um pressuposto essencial para que, na data da notificação, o Estado Membro do sistema produtor, possa garantir essa operacionalidade, que é um pressuposto essencial da notificação, como estabelece a alínea h) do artigo 7.º do Regulamento.

Este quadro de interoperabilidade entre sistemas informáticos é estabelecido no art.º 12.º do Regulamento, e constitui um quadro de obrigações de todos os Estados Membros, que evitará que constrangimentos de caráter técnico ou logístico retirem efeito útil ao princípio do reconhecimento mútuo.[623]

Este quadro de interoperabilidade que se impõe aos Estados Membros, desde logo nos sistemas de prestação de serviços eletrónicos por organismos públicos, pode também alargar-se, embora de forma voluntária, às entidades privadas.[624] Esta possibilidade destina-se a promover o mercado digital europeu e é tributária de um princípio da UE, segundo o qual devem ser a administração pública e os Estados a liderar a expansão da utilização dos meios eletrónicos nas atividades comerciais e institucionais.[625]

---

[623] Já em 2012 se anunciava a instituição de um sistema destinado a *"garantir a interoperabilidade técnica dos sistemas de identificação eletrónica notificados* COM(2012) 238 final, pág. 14.

[624] A extensão do programa às entidades privadas é admitida e desejada pela proposta, nos seguintes termos: *"The concept of notified eID is not limited to public-sector issued eIDs: Member States could also notify eIDs issued by the private sector that they recognise for use in their own public-sector services. This approach is necessary since not all Member States authorities issue eIDs The cross-sector approach of the legislation would allow the private sector to integrate the use of notified eIDs in e-services when secure e-identification is needed"*..SWD(2012) 136 final, pág. 6.

[625] No desenvolvimento dessa estratégia de liderança pública, a UE tem lançado várias iniciativas, de que são exemplo o caso da Diretiva 2011/24/EU, de 9/3, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços e a iniciativa doa Balcões Únicos, destinada a permitir aos cidadãos a utilização de pontos de contacto e interação eletrónica, únicos, com várias administrações públicas, por exemplo para o início de uma atividade comercial (artigo 8.º da Diretiva 2006/123/CE, de 12/12/2006. Releva especialmente neste domínio a Agenda Digital para a Europa, pelo seu carácter transversal, que tem como ambição a generalização no espaço da UE, da utilização dos meios eletrónicos (COM(2010)245 final). Do mesmo modo o projeto de programa dos dados abertos, que pretende colocar à disposição da comunidade, nomeadamente científica, académica e empresarial, os dados das administrações públicas que não estejam sujeitos a qualquer reserva ou sigilo ("COM(2011) 882 final"), e ainda a iniciativa para o reforço da confiança no mercado único digital do comércio em linha e dos serviços em linha ("COM(2011) 942 final"). Releva também como iniciativa no domínio do sector público, a estratégia para a contratação eletrónica constante do documento COM(2012) 179 final. É

O regime da interoperabilidade foi ainda especificado no Regulamento de Execução (UE) 2015/1501, da Comissão, de 8 de setembro de 2015. Essa especificação destina-se a tipificar o modo como os sistemas de identificação e de autenticação dos diferentes Estados Membros se devem conectar e interagir. O Regulamento estabelece o princípio de que o Estado notificante, além de disponibilizar o sistema de autenticação notificado, deve ainda disponibilizar os procedimentos técnicos que permitam aos restantes agentes dos outros Estados Membros ligarem os seus sistemas a esse, sem custos relevantes. Para isso são parametrizadas os modos de ligação entre os sistemas, assentes em nós, que são os locais eletrónicos com endereços eletrónicos definidos onde os sistemas se ligam. São também parametrizadas as mensagens, que correspondem aos dados que os sistemas devem trocar para que se consume a identificação e a autenticação.

Estes nós de interoperabilidade dispensam a existência de conexões individuais e substituem-nas por plataformas comuns, onde vários sistemas se podem ligar. Prevê-se a possibilidade de essas plataformas serem geridas por operadores autónomos, que prestam esses serviços de interconexão, e também pela própria Comissão, estabelecendo o Regulamento de Execução, no artigo 9.º, que esses operadores não podem guardar registo dos dados que através deles são trocados entre os sistemas.

A interoperabilidade é também protegida pelo legislador do Regulamento contra entraves financeiros. Além do princípio da proibição de imposição de custos desproporcionados no estabelecimento das infraestruturas de conexão entre os sistemas informáticos, estabelece-se, também de forma imperativa, o princípio da gratuitidade na concreta prestação de serviços de autenticação de cada um dos utilizadores, sempre que estes pretendam aceder aos serviços eletrónicos de outras entidades.

Os Estados não podem tornar onerosos os serviços que os sistemas de identificação eletrónica que produziram meios de identificação eletrónica, de autenticação de pessoas singulares ou coletivas que os invoquem perante sistemas de identificação eletrónica de outros Estados Membros. Esse princípio está consagrado na segunda parte da alínea f) do artigo 7.º do Regulamento EIDAS e aplica-se apenas nos casos em que a o serviço de identificação e autenticação é prestado entre órgãos da administração pública. Nos casos em que o serviço seja prestado a uma entidade privada, o regulamento não impede que esse serviço seja oneroso.

---

também relevante a Resolução do Parlamento Europeu, de 20/4/2012 (2013/C 258 E/09). JOCE, 7.9.2013, C 258 E/65.

Assim, além dos constrangimentos técnicos e logísticos que o regime da interoperabilidade elimina, são também eliminados constrangimentos financeiros à utilização transfronteiriça dos meios de identificação eletrónica.

O quadro de interoperabilidade corresponde à tradução operacional e tecnológica do princípio jurídico do reconhecimento mútuo, garantindo com ele o legislador, a efetividade daquele princípio, regulando-o expressamente.

5.4. – Efeitos

Os meios de identificação eletrónica com níveis de garantia substancial e elevado adquirem, deste modo, validade e eficácia em todo o espaço da União Europeia. Em consequência, tendencialmente, os cidadãos dos Estados Membros que possuam um desses meios passarão a poder utilizá-lo para acederem a todos os serviços prestados em linha por órgãos da administração pública em qualquer outro Estado. Aqueles que possuam um meio de identificação com nível de garantia substancial poderão utilizá-lo para aceder a serviços eletrónicos que exijam o correspondente nível de garantia, mas já não o poderão utilizar naqueles que exijam nível elevado. Esta universalidade é o mais importante resultado do Regulamento EIDAS e um verdadeiro direito dos cidadãos europeus à identificação eletrónica única.

Estabelece-se assim um direito dos cidadãos da União Europeia à utilização transfronteiriça dos meios de identificação eletrónica, que se constitui logo que exista notificação, publicitação pela Comissão e reconhecimento pelos Estados Membros respetivos. Esse direito é o principal efeito do Regulamento, no que respeita à identificação eletrónica.

Por outro lado, é gratuita a utilização dos elementos necessários à autenticação eletrónica, pelas entidades que deles necessitem. Quando alguém invoca a sua identidade porque pretende a ceder a um serviço eletrónico noutro Estado Membro, pessoa singular ou coletiva perante quem essa invocação é feita, necessita de utilizar os serviços eletrónicos da entidade que produziu o meio de identificação eletrónica que é utilizado, para que assim possa certificar-se, mediante a autenticação, de que se trata efetivamente da pessoa que diz ser. Esta autenticação é efetuada com recurso à entidade que gerou o meio de identificação utilizado, pelo que, no final de contas, é essa entidade que efetua a confirmação da identidade invocada, prestando assim um serviço à

entidade de destino. Ora, a segunda parte da alínea f) do artigo 7.º do Regulamento, estabelece a gratuitidade desse serviço quando se trate de entidades públicas, admitindo apenas a possibilidade de ser oneroso nos casos em que o serviço seja prestado a entidades privadas.

Este regime permite uma maior eficiência, rapidez, facilidade e economia na utilização dos serviços eletrónicos disponibilizados pelas administrações públicas, podendo também alargar-se às empresas, o que será muito importante para o crescimento do comércio eletrónico e a promoção do objetivo da construção do mercado único digital que o Regulamente anuncia.

Estabelece-se ainda um quadro de interoperabilidade, no art.º 12.º do Regulamento, que permitirá a conexão entre os sistemas das administrações públicas, na parte relativa à identificação e autenticação dos cidadãos e empresas e uma maior automatização e rapidez da sua operacionalidade.

O sistema de identificação de um órgão da administração pública de um estado membro, que possua os dados de identificação de um determinado cidadão, pode ser por este invocado nas transações eletrónicas que pretenda efetuar perante órgãos da administração pública de outros Estados Membros, para se identificar e autenticar perante este. Nesse caso, este último órgão utilizará o sistema do primeiro, para confirmar a identidade do cidadão ou da empresa que com ele pretende interagir.

Institui-se um sistema destinado a *"garantir a interoperabilidade técnica dos sistemas de identificação eletrónica notificados"*.[626]

O regulamento centra este quadro de interoperabilidade nos serviços das administrações públicas, mas não exclui a sua utilização por entidades privadas.[627] Esta opção é tributária de um princípio da UE, segundo o qual devem ser a administração pública e os Estados a liderar a expansão da utilização dos meios eletrónicos nas atividades comerciais e institucionais.[628]

---

[626] COM(2012) 238 final, pág. 14.

[627] A extensão do programa às entidades privadas é admitida e desejada pela proposta, nos seguintes termos: *"The concept of notified eID is not limited to public-sector issued eIDs: Member States could also notify eIDs issued by the private sector that they recognise for use in their own public-sector services. This approach is necessary since not all Member States authorities issue eIDs The cross-sector approach of the legislation would allow the private sector to integrate the use of notified eIDs in e-services when secure e-identification is needed"*..SWD(2012) 136 final, pág. 6.

[628] No desenvolvimento dessa estratégia de liderança pública, a UE tem lançado várias iniciativas, de que são exemplo o caso da Diretiva 2011/24/EU, de 9/3, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços e a iniciativa doa Balcões Únicos, destinada a permitir aos cidadãos a utilização de pontos de contacto e interação eletrónica, únicos, com várias administrações públicas, por exemplo para o início de uma atividade comercial (artigo 8.º da Diretiva 2006/123/CE, de

O regulamento não obriga que todos os serviços eletrónicos prestados por entidades públicas possuam sistemas de identificação eletrónica que cumpram os requisitos correspondentes aos níveis de garantia nele tipificados. Apesar disso, a sua sistematização constitui um marco jurídico que deve servir de parâmetro para que cada órgão da administração pública adeque os serviços que presta por via eletrónica aos níveis de garantia estabelecidos no Regulamento. E embora não exista uma obrigação explícita nesse sentido, os serviços das administrações públicas devem adequar os seus sistemas a esses níveis de garantia, para que possam corresponder às exigências dos cidadãos em ambos os sentidos. Na verdade, os cidadãos portugueses que sejam titulares de meios de identificação eletrónica gerados por órgãos das administrações públicas portuguesas necessitarão de os utilizar para se identificarem perante serviços eletrónicos noutros Estados Membros. Por outro lado, os órgãos das administrações públicas portuguesas necessitam de adequar os sistemas mediante os quais prestam serviços eletrónicos, à sua utilização por cidadãos de outros Estados Membros que se pretendam identificar perante eles com meios de identificação eletrónica produzidos nesses Estados.

12/12/2006. Releva especialmente neste domínio a Agenda Digital para a Europa, pelo seu carácter transversal, que tem como ambição a generalização no espaço da UE, da utilização dos meios eletrónicos (COM(2010)245 final). Do mesmo modo o projeto de programa dos dados abertos, que pretende colocar à disposição da comunidade, nomeadamente científica, académica e empresarial, os dados das administrações públicas que não estejam sujeitos a qualquer reserva ou sigilo ("COM(2011) 882 final"), e ainda a iniciativa para o reforço da confiança no mercado único digital do comércio em linha e dos serviços em linha ("COM(2011) 942 final"). Releva também como iniciativa no domínio do sector público, a estratégia para a contratação eletrónica constante do documento COM(2012) 179 final. É também relevante a Resolução do Parlamento Europeu, de 20/4/2012 (2013/C 258 E/09). JOCE, 7.9.2013, C 258 E/65.

Capítulo VI – A Assinatura eletrónica e os restantes serviços de confiança

Uma das principais inovações do Regulamento EIDAS é o da estruturação do direito da confiança jurídica na utilização dos meios eletrónicos em torno de dois regimes fundamentais. Por um lado a identificação eletrónica, que se autonomiza do regime das assinaturas eletrónicas. Por outro lado o regime dos serviços de confiança eletrónica, onde se integram as assinaturas eletrónicas.

A assinatura eletrónica ocupa no seio do conjunto dos serviços de confiança, função igual à da assinatura nas relações não eletrónicas, ou seja a de instrumento de autenticação de documentos. O Regulamento EIDAS assenta, nesta matéria, no pressuposto de base de que nas relações estabelecidas por meios eletrónicos, tal como nas restantes, a maioria se opera sem qualquer documentação, por desnecessária. Desta forma, limita-se a necessidade de utilização das assinaturas eletrónicas a um escasso segmento de relações jurídicas em que essa documentação é necessária.

Desta limitação resulta uma outra. Se a função da assinatura é assinar documentos, o conceito limita-se ao do papel, porque o Regulamento importa para o seu

seio o conceito jurídico de "*assinar*", que não é específico dos suportes eletrónicos, mas é o mesmo que se aplica às relações estabelecidas por meios não eletrónicos.

O que acabamos de dizer não exclui, porém a possibilidade de as assinaturas eletrónicas serem utilizadas para assinar conjuntos de dados eletrónicos, em transações que não seriam normalmente suportadas em documentos nos casos em que se tratasse de transações não eletrónicas.

As transações eletrónicas são ainda um meio novo de tráfego jurídico e isso pode conduzir a que as partes pretendam conferir-lhe uma maior segurança. Por outro lado trata-se de transações que deixam sempre rasto e existe sempre registo delas. Ao contrário das transações efetuadas presencialmente e em ambiente não eletrónico, não existem transações meramente verbais, em que o registo das declarações negociais se esvai com a volatilização das ondas sonoras respetivas. Por essa razão é sempre possível que os dados dessas transações possam ser submetidos a assinatura eletrónica, ainda que não constituam formalmente um documento. Assim, as assinaturas eletrónicas podem autenticar dados, quando as partes assim o entendam, ainda que esses dados não constituam um documento eletrónico.

A assinatura nos suportes não eletrónicos é um instrumento de vinculação de pessoas singulares, não sendo um conceito aplicável à vinculação de pessoas coletivas. Por essa razão, o Regulamento limita a utilização das assinaturas eletrónicas às pessoas singulares, definindo-as como "*os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar*" (n.º 10 do artigo 3.º). Mas antes, define-se signatário como "*a pessoa singular que cria uma assinatura eletrónica*" (n.º 9 do artigo 3.º). Desta forma, e na configuração do Regulamento, só as pessoas singulares podem ser signatários e titulares de assinaturas eletrónicas.

Além das assinaturas eletrónicas, são também tipificados como serviços de confiança no Regulamento EIDAS os seguintes:

1. - Os selos eletrónicos, que passam a ser o instrumento de autenticação, pelas pessoas coletivas, dos documentos eletrónicos que emitem. O efeito jurídico da utilização dos selos eletrónico é idêntico ao da assinatura eletrónica, embora, naturalmente, o Regulamento não o defina como instrumento para o signatário assinar, mas como instrumento para o criador do selo (as pessoas coletivas, como refere o n.º 24 do artigo 3.º, garantirem "*a origem e a integridade*" de dados em formato

eletrónico).[629] O regime dos selos eletrónicos é praticamente o mesmo do regime das assinaturas eletrónicas, mas o conceito de selo eletrónico é mais abrangente que o de assinatura, porque engloba a autenticação e a garantia de integridade de quaisquer dados, e isso inclui os dados que formam um documento eletrónico, bem como todos os tipos de dados.[630] Incluem-se, nestes casos, os selos que autenticam servidores, para as transações com relevância jurídica efetuada entre máquinas. O selo eletrónico autentica todos os dados emitidos por uma máquina de uma pessoa coletiva, como sendo emitidos pela própria pessoa coletiva, vinculando-a. Do mesmo modo, podem os selos eletrónicos identificar um programa informático como sendo da pessoa coletiva correspondente. A diferença aqui é que no caso dos servidores, trata-se da autenticação de máquinas como sendo de determinadas pessoas coletivas, e no caso do software, trata-se da autenticação de sistemas informáticos. Os artigos 35.º a 40.º do Regulamento replicam para os selos eletrónicos o mesmo regime das assinaturas eletrónicas. Para os selos eletrónicos qualificados é estabelecida uma presunção legal de integridade dos dados por eles autenticados, bem como de correção da sua origem, tal como nas assinaturas eletrónicas;

2. Os Certificados qualificados de autenticação de *sítios web*. Estes certificados conferem a certeza da autenticidade desses sítios. Nestes casos a autenticidade corresponde à determinação da origem desses sítios, ou seja, à identificação dos sujeitos de direito que são seus titulares, normalmente agentes económicos ou organismos públicos. Este tipo de certificados dá a conhecer a todos os interessados a identidade do titular respetivo, nomeadamente o nome, a sua natureza de pessoa singular ou coletiva, o endereço físico da sua localização, "*incluindo, pelo menos a cidade e o Estado*". O conteúdo dos certificados está previsto no Anexo IV do Regulamento e no artigo 45.º, e esse conteúdo é

[629] Como se refere no par. 59 dos Considerandos do Regulamento, os selos eletrónicos servem: *"de prova da emissão de um documento eletrónico por determinada pessoa coletiva, certificando a origem e a integridade do documento"*.

[630] Esta conclusão é confirmada pelo par. 65 dos Considerandos do Regulamento, segundo o qual os selos eletrónicos servem para autenticar qualquer bem em formato eletrónico das pessoas coletivas: "*os selos eletrónicos podem ser utilizados para autenticar qualquer bem digital da pessoa coletiva, como um código de software ou um servidor"*

idêntico aos dos certificados qualificados de assinatura eletrónica e dos selos eletrónicos. Esta identificação dos titulares dos sítios *web* é um importante instrumento de segurança para que os interessados que pretendam estabelecer relações jurídicas com as respetivas pessoas singulares ou coletivas, tenham a certeza de que as estão a estabelecer mediante a utilização desses sítios. Dessa forma, as interações com esses sítios, consideram-se estabelecidas com os titulares que constam dos respetivos certificados.[631] Embora a Comissão não tenha ainda publicado os atos de execução que regulem este serviço de confiança, trata-se de um instrumento de identificação de um agente económico que é titular de um serviço eletrónico mediante o qual exerce uma atividade económica ou de outra natureza, permitindo aos interessados conhecerem a identificação da parte com quem estabelecem relações jurídicas através desses sítios. Estes certificados são apenas instrumentos de autenticação da identidade dos sítios *web*, limitando-se a sua função à identificação do sujeito das relações jurídicas que é deles titular.[632] A sua função não abrange, por essa razão, a autenticação das comunicações e das trocas de dados que se efetuam nas operações que se estabelecem através desses sítios;[633]

3. Os selos temporais são instrumentos jurídicos eletrónicos de vinculação de um conjunto de dados a uma determinada data e hora.[634] Além dessa

[631] A certificação de sítios web é uma importante inovação do Regulamento EIDAS,. Na economia atual os sítios *web* (*sites* ou páginas eletrónicas na Internet, como são comummente designados) são verdadeiras personificações eletrónicas de empresas, através das quais qualquer interessado pode efetuar transações com relevância jurídica imediata. Atualmente muitos desses sítios *web* desempenham verdadeiras funções idênticas às dos estabelecimentos comerciais Por essa razão, a segurança acerca da autenticidade dos sítios *web* releva de elevada importância para a confiança jurídica dos agentes. O Regulamento especifica no anexo IV os requisitos de segurança e estabelece no artigo 45.º a possibilidade de a Comissão regulamentar a sua autenticação. Esta autenticação pode consistir na emissão de uma chave privada por um prestador de serviços de certificação e uma chave pública, que é utilizada para encriptar a informação recebida dos utilizadores desse *site*. Para certificar a sua autenticidade, deve o *site* disponibilizar o certificado de assinatura emitido pela entidade que gerou o par de chaves. Esse certificado garante a autenticidade do site.

[632] A definição de certificado de autenticação de sítio web consta do n.º 38.º do artigo 3.º do Regulamento, como *"um atestado que torne possível autenticar um sítio web e associe o sítio web à pessoa singular ou coletiva à qual o certificado tenha sido emitido"*.

[633] O par. 67 do preâmbulo do regulamento refere que *"Os serviços de autenticação de sítios web fornecem meios que dão aos visitantes de um sítio web a garantia de que existe uma entidade genuína e legítima responsável pelo sítio"*.

[634] O n.º 33 do artigo 3.º do Regulamento define os selos temporais do seguinte modo: *"«Selos temporais»: os dados em formato eletrónico que vinculam outros dados em formato eletrónico a uma hora específica, criando uma prova de que esses outros dados existiam nesse momento"*.

vinculação temporal, os selos temporais asseguram a integridade dessa vinculação, o que inclui os dados do documento ou da operação efetuada e do próprio selo. O n.º 2 do art.º 41.º do Regulamento estabelece uma presunção de exatidão e de vinculação. A certificação temporal estava já prevista no Decreto-Lei n.º 290-D/99, de 2/8, mas a falta de especificação normativa do seu regime não permitiu o seu desenvolvimento. Este serviço de confiança é muito importante nos casos de atos que são praticados por meios eletrónicos, nomeadamente nos casos em que têm que ser praticados em prazos determinados, bem como naqueles casos em que a prática de um ato abre ou encerra um determinado prazo. Do mesmo modo, os selos temporais asseguram que a transação efetuada ocorreu durante o período de validade do certificado de assinatura eletrónica. Relevam, particularmente nesta matéria, os atos praticados na ação administrativa, incluindo a receção de documentos entregues pelos cidadãos no âmbito de procedimentos administrativos. Quando os selos temporais são emitidos por prestadores qualificados de serviços de confiança e cumprem os restantes requisitos estabelecidos no artigo 42.º do Regulamento, adquirem a classificação de selos temporais qualificados, produzindo o efeito de se presumir a exatidão da data e hora que certificam e da integridade dos dados a que se aplicam n.º 2 do artigo 41.º). Do mesmo modo, esses selos temporais são obrigatoriamente reconhecidos em todos os Estados Membros da UE, como estabelece o n.º 3 do artigo 41.º. Relativamente aos selos temporais não qualificados, são também reconhecidos efeitos jurídicos de certificação da data e hora da produção dos factos jurídicos a que se aplicam, embora sem a presunção legal de conformidade e prova (n.º 1 do artigo 41.º);

4. Os serviços de envio registado eletrónico asseguram a certificação do envio e da receção das comunicações eletrónicas, bem como a integridade dos dados enviados e recebidos.[635] Essa certificação é efetuada por uma entidade terceira que presta serviços de confiança,

[635] O n.º 36 do artigo 3.º do Regulamente define da seguinte forma os serviços de envio registado eletrónico. *"«Serviço de envio registado eletrónico»: um serviço que torne possível a transmissão de dados entre terceiros por meios eletrónicos e forneça prova do tratamento dos dados transmitidos, nomeadamente a prova do envio e da receção dos mesmos, e que proteja os dados transferidos contra o risco de perda, roubo, dano ou alteração não autorizada"*.

cujas declarações neste domínio fazem prova. A função deste serviço é garantir que os dados foram enviados de um remetente identificado para um destinatário, também identificado. Essa garantia é assegurada por um prestador de serviços de confiança, que pode ser qualificado. Quando assim for, pode o serviço de envio registado eletrónico adquirir a natureza de qualificado, desde que se cumpram também os requisitos de identificação segura do remetente e do destinatário, os dados enviados devem ser assinados com assinatura eletrónica ou com selo eletrónico, quando se trate de uma pessoa coletiva, bem como com um selo temporal que certifique a data e hora de envio e de receção dos dados (artigo 44.º do Regulamento). Nesses casos, a lei estabelece a presunção da integridade dos dados que foram remetidos, bem como da sua receção pelo destinatário. Do mesmo modo se presume real a data da remessa e da entrega (n.º 2 do artigo 43.º do Regulamento). O serviço é prestado por um ou mais prestadores de serviços, devendo eles serem qualificados para que o serviço seja também classificado como qualificado e beneficie da presunção antes referida. Nada impede, porém que o serviço seja prestado por prestadores não qualificados, mas o Regulamento afasta a possibilidade de este serviço ser prestado pelas próprias partes, dado que, nos termos da própria definição, deve ser presado por entidades terceiras. Faz sentido que assim seja, porque a intervenção de uma entidade terceira confere maior segurança jurídica, em especial em caso de litígio entre as partes. Este serviço de confiança é também uma importante inovação do Regulamento, em especial para a matéria das notificações efetuadas no âmbito dos procedimentos administrativos, como analisaremos no capítulo V da Parte III do nosso trabalho;

Além dos serviços de confiança que acabamos de enunciar, que o Regulamento EIDAS tipifica, outros existem que podem ser praticados, que embora não estejam ainda regulados especificamente, tenderão a automatizar-se, nomeadamente os seguintes:

i) Os serviços de validação de assinaturas eletrónicas qualificadas. Trata-se de um serviço mediante o qual um prestador de serviços de confiança efetua a verificação da assinatura ou do selo eletrónico de um determinado documento eletrónico e atesta a sua validade jurídica. Essa

verificação e atestação, por uma entidade terceira e especializada destina-se a garantir, para eventual utilização futura, a confirmação da integridade do documento e a sua autenticação no momento e que foi recebido ou emitido por uma das partes, ou então em determinado momento do tempo.[636] Este serviço de validação só está previsto para os casos e que a assinatura eletrónica que é validada é qualificada (artigo 32.º). A validação permite ultrapassar os problemas de suspensão, cancelamento ou revogação dos certificados de assinatura ou de selos eletrónicos, em data posterior à da assinatura de determinados documentos. O serviço de validação permite atestar que em determinado momento, em especial o da assinatura dos documentos, o certificado era válido e vinculava juridicamente o autor da assinatura ou o titular do selo eletrónico. Quando este serviço é prestado por prestadores qualificados de serviços de confiança, adquire a natureza de serviço qualificado de validação, desde que o resultado dessa validação possa ser recebido de modo automático pelo utilizador e inclua a assinatura eletrónica ou o selo eletrónico avançado do prestador (artigo 33.º). Nesses casos presume-se a conformidade dos atos verificados de assinatura. Este serviço aplica-se também à validação dos selos eletrónicos qualificados (artigo 40.º);

ii) O serviço qualificado de preservação de assinaturas eletrónicas qualificadas. Trata-se de um serviço destinado a fazer perdurar no tempo os efeitos das assinaturas eletrónicas, quando qualificadas, em especial nos casos em que a tecnologia que foi utilizada na sua criação ficou ultrapassada e deixou de ser utilizada. Trata-se de um problema que releva em especial no domínio dos arquivos dos documentos eletrónicos. A evolução tecnológica conduz ao abandono de tecnologias que são ultrapassadas pela inovação, sendo substituídas por outras mais eficientes. Esse processo pode conduzir a que, em determinado momento deixe de ser possível a verificação das assinaturas de determinados documentos, em especial os mais antigos, para cuja análise já não estejam as tecnologias correspondentes àquelas com que

[636] O n.º 41.º do artigo 3.º do Regulamento define validação como o "processo pelo qual é verificada e confirmada a validade de uma assinatura ou selo eletrónico".

foram criadas. É para evitar esse efeito que estes serviços permitem a preservação das assinaturas eletrónicas qualificadas. Trata-se de um tipo de serviço que só pode ser prestado por prestadores qualificados (artigo 34.º). Este serviço pode também ser prestado relativamente aos selos eletrónicos (artigo 40º).

iii) Serviços de geração ou gestão, em nome do signatário, dos dados necessários para a criação de assinaturas eletrónicas ou de selos eletrónicos. Embora não se trate de um serviço de confiança autonomamente regulado no Regulamento EIDAS, o n.º 3 do Anexo II prevê a possibilidade de entidades terceiras gerarem, em nome e por conta do signatário ou do titular dos selos eletrónicos, os dados necessários à criação de assinaturas eletrónicas ou de selos eletrónicos. Permite-se, em primeiro lugar, a possibilidade de o signatário confiar a um terceiro o dispositivo de assinatura eletrónica, desde que se trate de um prestador de serviços que, nos casos em que o certificado seja qualificado, seja também ele qualificado. É necessário, além disso, para que se mantenha o caráter qualificado da assinatura eletrónica, que se garanta a adoção dos procedimentos de segurança adequados para que o signatário mantenha o controlo dos procedimentos de criação da assinatura, já não a exclusividade do acesso, mas o controlo exclusivo da utilização dos dados de criação da assinatura. Para isso é necessário que o canal utilizado seja seguro e que o sistema de aplicação da assinatura seja controlado pelo signatário.[637] Do mesmo modo se permite a criação de assinaturas eletrónicas à distância, mediante canais seguros que garantam o mesmo tipo de controlo pelo signatário.[638] A criação de assinaturas à distância é possível desde que se cumpram os seguintes requisitos:[639]

   i) O ambiente em que são criadas seja gerido por um prestador de serviços de confiança em nome do signatário;

[637] Como se refere no considerando 51 do Regulamento EIDAS; "*Os dispositivos qualificados de criação de assinaturas eletrónicas deverão poder ser confiados a terceiros pelo signatário*".
[638] Este serviço é enunciado nos termos seguintes pelo Considerando n.º 52 do Regulamento EIDAS: "*A criação de assinaturas eletrónicas à distância, sendo o ambiente em que são criadas gerido por um prestador de serviços de confiança em nome do signatário*".
[639] N.º 52 dos Considerandos do Regulamento e n.º 3 do Anexo II.

ii) Que utilizem canais de comunicação eletrónica seguros;

iii) Os prestadores de serviço de confiança que as criam garantam a fiabilidade do ambiente de criação das assinaturas;

iv) Se garanta que esse ambiente é utilizado sob a supervisão exclusiva do signatário;

v) Sendo assinaturas qualificadas, aplicam-se os mesmos requisitos dos prestadores qualificados de serviço, devendo o prestador de serviços ser também ele qualificado.

Ambos os tipos de serviços, que podem ser complementares, só podem ser prestados por prestadores qualificados de serviços de confiança, quando se trate de assinaturas eletrónicas qualificadas. Ambos os tipos de serviços podem também ser utilizados na aplicação de selos eletrónicos (n.º 1 do artigo 39.º). Estes serviços são utilizados especialmente nos casos em que se procede à criação, em massa de assinaturas eletrónicas. Nesses casos não e possível que a ordem de criação da assinatura seja dada de forma manual e individual pelo signatário, necessitando-se da criação de um mecanismo automático que efetue essa criação. Nessas situações poderia ficar em causa a proteção dos dados de criação da assinatura contra a utilização abusiva por terceiros e o princípio da utilização exclusiva pelo signatário. A fim de compatibilizar os dois interesses da produção em massa e de forma automatizada, e da proteção contra a utilização por terceiros, permite-se que o serviço de geração das assinaturas eletrónicas de forma massiva e automatizada possa ser prestado por terceiro, desde que este garanta aquela proteção. E para isso o Regulamento reserva a prestação deste tipo de serviços apenas para os prestadores de serviços de confiança, que terão que ter o estatuto de qualificados nos casos em que se trate de assinaturas ou de selos qualificados. A fim de viabilizar a prestação deste tipo de serviços, o n.º 4 do Anexo II do Regulamento prevê a possibilidade de serem duplicados os dados de criação das assinaturas eletrónicas, desde que se destinem apenas a servir de cópias de

segurança, que o nível de segurança seja igual e a cópia se destine apenas a garantir a continuidade do serviço. Apesar do caráter inovador deste tipo de serviço de confiança, o Regulamento não especifica os termos da sua prestação, o que levanta algumas questões, nomeadamente a de que não basta apenas a regra de segurança de que sejam apenas prestadores qualificados a prestá-lo. Compreende-se que assim seja, dado o caráter crítico que resulta de este serviço ser de natureza excecional, porque se está a permitir a criação de assinaturas por terceiros, o que é sempre problemático. E não basta, como regra de segurança, que se estabeleça que só o prestador qualificado tenha acesso aos meios de criação de assinatura. É também necessário que a lei estabeleça que a determinação dos documentos aos quais se permite a colocação da assinatura por esses prestadores seja controlada, de forma rigorosa pelo signatário. Na verdade, de pouco serve a exclusividade de acesso à chave privada pelo prestador de serviços, se não existir um controlo rigoroso e delimitado dos tipos, conteúdo e das quantidades de documentos submetidos a assinatura. É ainda necessário prever que todos os procedimentos utilizados sejam auditados e deixem, para isso os necessários registos. Embora o Regulamento não seja expresso nessa matéria, parece-nos que esse tipo de controlos está subjacente aos seus princípios.

O universo de serviços de confiança que o Regulamento estabelece expressamente como tal, não é fechado, como acabamos de ver e como a inovação tecnológica e a criatividade empresarial recomenda, sendo que o Regulamento admite que, apesar de o seu quadro normativo ser harmonizado, possam os Estados Membros criar internamente novos serviços de confiança.[640]

[640] Como aliás se expressa no considerando n.º 25 do Regulamento, nos seguintes termos "*Os Estados-Membros deverão continuar a ser livres de definir outros tipos de serviços de confiança para além dos que constam da lista exaustiva de serviços de confiança prevista no presente regulamento, tendo em vista o seu reconhecimento a nível nacional como serviços de confiança qualificados*".

Parte III.

Construção jurídica da assinatura eletrónica

Capítulo I – Os princípios jurídicos da assinatura eletrónica

O corpo conceptual do direito das assinaturas eletrónicas, bem como os regimes normativos adotados, assentaram num conjunto de princípios fundamentais, que analisamos de seguida.

1. O princípio da inalterabilidade do direito subjacente

A disciplina da assinatura eletrónica tem por objeto meios eletrónicos que documentam relações jurídicas e não o conteúdo destas. Trata-se de um regime jurídico de documentos e não do regime jurídico das relações que do seu conteúdo emerge.

A utilização dos meios eletrónicos tem impacto sobre o modo do exercício dos direitos, mais do que sobre estes, pelo que as normas que regulam a sua utilização não interferem com o direito subjacente.

O princípio da inalteração do direito reflete a preocupação de as normas que regulam a relevância jurídica dos suportes eletrónicos não interferirem com os direitos

que o seu conteúdo incorpora.[641] A eletrónica é apenas um suporte instrumental para o exercício dos direitos, como o é o papel.[642] Trata-se de uma disciplina de meios, mais que de conteúdos.[643]

Embora não tenham sido consagrados explicitamente na LMCE, os pressupostos daquilo que viria a ser este princípio vêm já nela mencionados, nomeadamente no n.º 7 do art.º 10.º que estabelece que as normas que regulam o momento e o lugar de emissão e de receção das comunicações eletrónicas não podem contender com os efeitos jurídicos do conteúdo dessas comunicações.[644]

Este princípio está expresso na Diretiva 1999/93/CE, que na parte final do art.º 1.º exclui a aplicação das respetivas normas às relações jurídicas subjacentes aos documentos em forma eletrónica.[645] O mesmo princípio se consagra também no n.º 3 do artigo 2.º do Regulamento EIDAS.

2. O princípio da equivalência funcional

[641] Segundo Mariliana Carrillo, *"La firma electrónica no es sino un nuevo suporte de las obligaciones y contratos que no afecta las reglas de Derecho preexistentes y no implica su modificación"*. Carrillo, Mariliana Rico; op. cit., pag. 143.

[642] Essa separação da relevância jurídica das comunicações eletrónicas e do seu conteúdo ou efeitos jurídicos que dele relevam, manifesta-se nos primeiros trabalhos da LMCE: *"Article 13 is not intended to interfere with law on the formation of contracts but rather to promote international trade by providing increased legal certainty as to the conclusion of contracts by electronic means. It deals not only with the issue of contract formation but also with the form in which an offer and an acceptance may be expressed"*. "A/CN.9/WG.IV/WP.64", par. 97.

[643] Tal como afirma Rivero, citando Illescas Ortiz, a disciplina jurídica da assinatura eletrónica *"no implica "una modificación sustancial del Derecho existente de obligaciones y contratos "nacional e internacional" en el momento en que la articulación jurídica de la electrónica como instrumento de transacciones comerciales tiene lugar"*. Ortiz, R.I., (2000). *Derecho de la Contratación Electrónica. Civitas Ediciones*. Madrid., pag. 84.

[644] O artigo 14.º da LMCE estabelece o regime aplicável ao momento em que se consideram emitidas e recebidas as mensagens eletrónicas, bem como ao respetivo local, nos casos em que o respetivo emitente solicita conformação da sua receção ao respetivo destinatário. "Guide to Enactment LMCE (1996)", pág. 10. Do mesmo modo, como refere o Guia para a Transposição da LMCE, *"It should be noted that, under the Model Law, the mere signing of a data message by means of a functional equivalent of a handwritten signature is not intended, in and of itself, to confer legal validity on the data message. Whether a data message that fulfilled the requirement of a signature has legal validity is to be settled under the law applicable outside the Model Law"*. "Guide to Enactment LMCE (1996)", par. 61.

[645] É a seguinte a redação da parte final do preceito: *"A presente directiva não cobre aspectos relacionados com a celebração e a validade de contratos ou a constituição de outras obrigações legais para os quais a legislação nacional ou comunitária preveja determinados requisitos em matéria de forma, nem afecta as normas e as restrições constantes da legislação, nacional ou comunitária, que regem a utilização de documentos"*.

O princípio da equivalência funcional consiste na assunção de que os suportes eletrónicos podem e devem cumprir as mesmas funções que os suportes em papel.[646]

Este princípio desempenhou um papel importante na primeira legislação produzida para a juridificação dos suportes eletrónicos. Face á ausência de tecnologia capaz de garantir a autenticação segura dos documentos eletrónicos, eles apresentavam-se menos idóneos que o papel para cumprir a função de documentação dos atos jurídicos. Essa idoneidade só poderia ser adquirida pela via jurídica, tendo este princípio constituído o instrumento jurídico fundamental para suprir essa lacuna. Os primeiros instrumentos jurídicos, nomeadamente a LMCE, não utilizam ainda o conceito de assinatura eletrónica e são normas que instituem a equivalência funcional dos documentos eletrónicos aos documentos em papel, em determinadas condições. O princípio da equivalência funcional foi a base da metodologia jurídica da formação do direito da assinatura eletrónica na sua fase inicial.

Havia entendimentos no sentido de que a emergência dos documentos eletrónicos obrigaria a construir novos conceitos jurídicos, nomeadamente de assinatura, documento, escrita, original, comunicação, identificação, autenticação e outros. Por exemplo, os conceitos de escrita e de original, formados no contexto físico do papel, poderiam não ser simplesmente aplicáveis aos suportes eletrónicos, pelo que seria necessário criar novos conceitos próprios dos documentos eletrónicos. Não foi, porém, esse o caminho seguido pelos legisladores.

A metodologia seguida assenta no pressuposto de que mais do que os suportes dos documentos, importa analisar as funções que servem em termos jurídicos e diagnosticar as condições que terão que se considerar reunidas, de forma objetiva, para que um suporte eletrónico cumpra o requisito de ser um documento escrito ou um original.[647]

Esta abordagem metodológica aproveita toda a disciplina jurídica já consolidada dos documentos e aplica-a aos documentos eletrónicos, em função da verificação, por estes, de um conjunto de requisitos de equivalência. Parte-se do

---

[646] Rivero define este princípio do seguinte modo: *"La equivalência funcional es la capacidade de un instrumento electrónico de satisfacer la misma necessidade que un instrumento tradicional".* Rivero, D.C. (Mayo 2005); op. cit., pag. 9.

[647] Essa metodologia foi adotada nos trabalhos preparatórios da LMCE: *"Functional-equivalent approach", is based on an analysis of the purposes and functions of the traditional paper-based requirement, with a view to determining how those purposes or functions could be fulfilled through EDI techniques"*. "A/CN.9/WG.IV/WP.69", par. 49.

pressuposto de que se trata apenas de dois suportes diferentes, e não de realidades novas que tornem inaplicável o direito pré-existente.[648]

Uma vez efetuada a identificação dessas funcionalidades, nomeadamente de registo, conservação, autenticação, prova, título de propriedade, bem como os instrumentos jurídicos correspondentes, de escrita, assinatura, legibilidade, originalidade, não alteração, estudaram-se as possibilidades de os suportes eletrónicos desempenharem as mesmas funções e as necessidades de adequação para que juridicamente essas funções fossem asseguradas nesses suportes, de forma equivalente ao papel.[649] O objetivo fundamental era o de o suporte eletrónico ser capaz de desempenhar as mesmas funções que o papel, como suporte dos documentos e das comunicações com relevo jurídico.[650]

Este princípio começa por fundar, na sua essência, uma equivalência funcional dos documentos, mais do que das assinaturas. É o suporte eletrónico que ele pretende erigir em alternativa ao papel, conferindo-lhe as mesmas funções logo que estejam reunidos um conjunto de pressupostos.

Mas se é verdade que o regime jurídico dos documentos eletrónicos não interfere com os efeitos das relações jurídicas que através deles se estabelecem, também é verdade que o regime jurídico dos documentos eletrónicos não pode consistir apenas numa transposição linear do regime jurídico aplicável aos documentos em papel e às comunicações tradicionais.[651]

---

[648] Como defende Rivero, trata-se de utilizar a analogia como metodologia de construção do conceito e do regime jurídico da assinatura eletrónica, partindo das funções das assinaturas em papel. *"El concepto de firma electrónica se basa en realidad en una analogía entre la relación de la firma manuscrita con el documento en soporte papel y la relación de la firma electrónica con el mensaje electrónico"*. Rivero, D.C. (Mayo 2005); op. cit., pag. 11.

[649] Como se refere nos documentos que reportam os trabalhos preparatórios da LMCE, *"The "functional equivalent approach", which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through EDI techniques. For example, among the functions served by a paper document are the following: to provide that a document would be legible by all; to provide that a document would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts"*. "A/CN.9/426", par. 31.

[650] Essa preocupação com a necessidade de os documentos eletrónicos proporcionarem um nível de segurança jurídica pelo menos tão eficaz como o papel é constante nos trabalhos da LMCE: *"For example, with respect to the functions of paper in general, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met"*. "A/CN.9/WG.IV/WP.69", par. 49.

[651] Não existe correspondência completa entre os suportes em papel e os eletrónicos, dado que a sua natureza é diferente, embora as funcionalidades que proporcionam possam ser equiparadas na lei. *"An electronic communication, in and of itself, cannot be regarded as an equivalent of a paper document*

A transformação proporcionada pelas novas tecnologias, não veio substituir nem o direito nem os sujeitos dos direitos. Proporcionou apenas novas técnicas de expressão e de comunicação da informação e do conhecimento, bem como da organização das atividades empresariais, das administrações públicas e dos cidadãos. Trata-se de uma transformação operada apenas nos meios.

A informática e a eletrónica são apenas meios técnicos, instrumentos da inteligência e do conhecimento humano, que tornam a sua expressão e execução mais rápida, eficiente e eficaz, tal como a descoberta de outras técnicas a tornou no passado. A técnica é inerente à ação humana e a descoberta de novos instrumentos e a sua exploração tem acompanhado ancestralmente o Homem como complemento da sua inteligência e da sua perícia.

E tal como aconteceu com outras técnicas quando foram descobertas, por exemplo a imprensa e o papel como suporte da escrita, elas necessitam do necessário enquadramento do direito. Não há uma revolução no direito, provocada pela chamada revolução digital, e talvez não exista mesmo revolução digital, mas apenas um conjunto de novas técnicas que produzem novas formas de expressão e de transmissão de informação com valor jurídico, que necessitam de ser reconhecidas pelo direito. E isso acontece com as tecnologias eletrónicas da mesma forma que acontece com qualquer nova técnica que produza efeitos jurídicos ou um impacto nas relações jurídicas.

Mas se este nosso entendimento nos parece adequado, também é verdade que não podemos afirmar que a emergência dos documentos eletrónicos não tem impacto no mundo jurídico. A emergência deste novo suporte levanta questões jurídicas, algumas das quais ainda não estão resolvidas.

Compreende-se que tenha sido estabelecido como pilar fundamental da juridificação dos documentos e das comunicações eletrónicas, a identificação das questões jurídicas que o fenómeno da revolução eletrónica coloca, e a conceção de postulados normativos cuja verificação conduzirá à transposição para os documentos e as comunicações eletrónicas, do regime jurídico aplicável ao suporte papel.[652]

---

because it is of a different nature and does not necessarily perform all conceivable functions of a paper document". A/CN.9/608/Add.1, par. 7.

[652] Essa opção de equiparar as funções e não os suportes ou os meios, nem de criar conceitos novos está expressa de forma muito clara num dos documentos de trabalho da UNCUECIC: *"The Convention does not attempt to define a computer-based equivalent to any particular kind of paper document. Instead, it singles out basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by data messages, enable such data messages to enjoy the same level of legal recognition as corresponding paper documents performing the same function"*. "A/CN.9/608/Add.1", par. 8.

O princípio da equivalência funcional desdobra-se em duas vertentes fundamentais:

i) O princípio da não discriminação dos documentos e das comunicações só pelo facto de se apresentarem em suporte eletrónico. É um princípio abrangente e universal, que tem como objeto o próprio suporte, mais do que a informação que dele consta e que os direitos e obrigações que nele se fundam. Ele estabelece a idoneidade do suporte eletrónico para ser portador de informação com relevância jurídica, em condições de igualdade com o papel. Este princípio responde à preocupação fundamental de eliminar os impedimentos legais à utilização dos meios eletrónicos no comércio jurídico e desdobra-se em dois domínios:[653]

   a. Impede que simplesmente se recusem efeitos jurídicos a um documento só pelo facto de ele constar em suporte eletrónico;

   b. Impede que sejam estabelecidas exigências de validade e de eficácia superiores aos documentos em suporte eletrónico, relativamente às que são aplicáveis aos documentos em papel.[654] O princípio consta do art.º 5.º da LMCE, estabelecendo que não se negarão efeitos jurídicos, tanto no que respeita à sua validade como à sua eficácia, aos documentos, comunicações, mensagens e qualquer tipo de informação consignada, só pelo facto de o seu suporte ser o eletrónico.[655] Este princípio também está subjacente à LMAE,[656] e

[653] Essa preocupação é reconhecida de forma reiterada, nomeadamente pela UNCITRAL, em vários documentos, nomeadamente o seguinte: *"The Model Law is based on the recognition that legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern means of communication"*. "A/CN.9/426", par. 30.

[654] Como se referia nos trabalhos preparatórios da LMCE, *"The adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the costs associated with them) than in a paper-based environment"*. "A/CN.9/608/Add.2", par. 6.

[655] O artigo 5.º da LMCE, sob o título *"Legal recognition of data messages"*, tem a seguinte redação: "*Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message"*. Este princípio está também expresso noutras normas da LMCE, por exemplo na parte final do n,º 1 do artigo 11.º, no que respeita à formação e validade dos contratos ("*Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose*") e no n.º 1 do artigo 12.º no que respeita às declarações negociais constantes de um suporte eletrónico *("As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message"*). "Guide to Enactment LMCE (1996)"; pág. 5 e 8, respetivamente.

[656] Este princípio está subjacente às respetivas opções, como se reconhece no Guia de Transposição correspondente: *"Approach under which functional equivalents of traditional paper-based concepts and practices should not be discriminated against"*. "UNCITRAL Model Law ... 2001", par. 67.

foi também traduzido no art.º 9.º da UNCUECIC, que estabelece a equivalência funcional entre os conceitos de escrita, assinatura e de original, nos suportes eletrónicos e de papel.[657] Com a evolução da legislação e da doutrina, o princípio da equivalência funcional deixou de ter como objeto as mensagens e os documentos eletrónicos para se passar a centrar no objeto da sua autenticação, que são as assinaturas eletrónicas, dado que essas eram entendidas como o modo geral de autenticação eletrónica. É assim que a diretiva 1999/93/CE, de 13/12/1999 postula o princípio, no n.º 2 do artigo 5.º, centrando-o na assinatura e reflexamente nos dados ou documentos que lhe subjazem. Com a cisão operada pelo Regulamento EIDAS, entre os serviços de confiança eletrónica e a identificação eletrónica e, no seio destes entre a assinatura eletrónica e os restantes, o Regulamento assegura a dupla aplicabilidade do princípio tanto às assinaturas eletrónicas como aos documentos eletrónicos (respetivamente artigos 25.º e 46.º);

ii) O princípio da equivalência, segundo o qual, cumpridos que sejam determinados requisitos, aplica-se aos documentos eletrónicos o mesmo regime que a lei estabelece para o suporte papel. Trata-se de um princípio que é simultaneamente mais abrangente e mais restrito que o anterior. É mais abrangente porque estabelece uma equivalência efetiva dos documentos eletrónicos aos documentos em papel sempre que se cumpram os requisitos legais de equivalência, que podem abranger também os documentos formais, em que a lei exija para os documentos em papel o cumprimento de um conjunto de requisitos formais específicos, nomeadamente o de assinatura.[658] Ao contrário do princípio anterior, este não é de aplicação universal, mas limitado aos

[657] Nos trabalhos da UNCUECIC considerou-se serem as seguintes as funções do papel nos documentos: assegurar a sua legibilidade, evitar que sofra alterações, ou seja, assegurar a sua integridade, permitir a sua reprodução, proporcionar meios para aa sua autenticação mediante uma assinatura e servir de meios de prova perante os tribunais e administrações públicas. São essas funções que o princípio da equivalência assegura aos documentos eletrónicos. *"The functional-equivalent approach has been taken in article 9 of the Convention with respect to the concepts of "writing", "signature" and "original""*. "A/CN.9/608/Add.2", par. 7.

[658] *"This principle of functional equivalence goes beyond the concept of non-discrimination and requires that paper-based and electronic documents should be treated equally by the law so long as the electronic document satisfies the requirements for equivalence specified in the law"*. A/CN.9/WG.IV/WP.115, par. 32.

documentos que cumpram os requisitos legais estabelecidos. Assim é o caso, como vimos, anteriormente, no que respeita aos requisitos de escrita, de assinatura e de original, quando a lei os exige com exigência formal, nomeadamente de reconhecimento, para os documentos em papel. Para estes casos são estabelecidos os requisitos e as condições necessárias para que um documento eletrónico possua os requisitos correspondentes estabelecidos para o papel. Trata-se, na verdade, de uma presunção de fiabilidade, que inverte o ónus da prova. Mas este princípio opera sobre os atributos e não sobre o suporte.[659] Não se estabelece um equivalente funcional eletrónico ao papel, como um documento, mas apenas para os atributos e funções específicos que os documentos em papel cumprem, nomeadamente os de assinatura, escrita, originalidade e autenticidade. São as funções que são objeto de equivalência funcional e não os próprios documentos em geral.[660] Essa equivalência é restrita a cada uma das funções específicas. Por exemplo, os requisitos aplicáveis ao arquivo dos documentos eletrónicos, não possuem qualquer equivalência funcional com os documentos em papel, sendo requisitos aplicáveis apenas aos primeiros. Do mesmo modo os requisitos de verificação e evidência de data e lugar em que se consideram expedidos e recebidas as comunicações eletrónicas constantes da LMCE.[661] Esta exclusão da equivalência no que respeita às regras de arquivo manteve-se na UNCUECIC, tal como na LMCE considerando-se que se trata de regimes específicos que devem ser objeto de regulação na legislação nacional.[662] Estas questões

[659] Como se refere nos documentos preparatórios da UNCUECIC, *"This approach does not attempt to define a computer-based equivalent to any particular kind of paper document. Instead, it singles out the basic functions of the primary paper-based form requirements, and sets out criteria that, if satisfied, enable electronic records to enjoy the same level of legal recognition as corresponding paper documents"*. A/CN.9/WG.IV/WP.115, par. 31.

[660] Assim se enuncia nos trabalhos preparatórios da LMCE: *"The Model Law does not attempt to define a computer-based equivalent to any kind of paper document. Instead, it singles out basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by data messages, enable such data messages to enjoy the same level of legal recognition as corresponding paper documents performing the same function"*. "A/CN.9/426", par. 33.

[661] *"The functional-equivalent approach has been taken (...)with respect to the concepts of "writing", "signature" and "original" but not with respect to other legal concepts dealt with in the Model Law"*. "Guide to Enactment LMCE (1996)"; par. 18.

[662] Foi desta forma que nos trabalhos preparatórios da UNCUECIC se considerou a exclusão dessa equivalência. *"In view of the public policy considerations related to those objectives, and the varying*

só mais tarde viriam a ser resolvidas, com a configuração legal de novos serviços de confiança nos suportes eletrónicos, como são os selos temporais, os serviços de envio registado eletrónico e os serviços de preservação de assinaturas eletrónicas a que nos referimos no Capítulo VI da Parte II. A equivalência aos documentos formais, que na verdade é uma presunção de fiabilidade, de integridade e de autenticidade, era reservada para as assinaturas eletrónicas qualificadas, no n.º 1 do artigo 5.º da Diretiva da UE e no n.º 2 do artigo 25.º do Regulamento EIDAS. Em ambos os casos se trata de presunções sobre as assinaturas, mas como elas são instrumentos de autenticação e de identificação, essa presunção projeta-se sobre os próprios documentos, operando sobre a base da equivalência funcional dos próprios documentos que é consagrada no artigo 46.º. Ficam, assim, deste modo cobertos sob o princípio da equivalência todos os tipos de documentos eletrónicos, a todos os tipos de documentos em papel, incluindo aqueles em que as garantias de autenticidade sejam as mais altas.

O princípio da equivalência funcional tem ainda uma vertente negativa destinada a garantir que a utilização de meios eletrónicos não produza o efeito contrário de obrigar as contrapartes a fazerem uso deles. Uma parte que receba uma proposta contratual por via eletrónica não fica vinculada à utilização dessa via para remeter a sua resposta, podendo utilizar outra via que entenda mais adequada. Esse princípio ganhou expressão na UNCUECIC, em especial no n.º 2 do seu art.º 8.º.[663]

As partes ficavam livres de adotar os meios de comunicação que entendessem, sem que qualquer deles adquirisse uma qualquer prevalência. O princípio da equivalência funcional converte-se também num princípio de igualdade de meios utilizáveis nas comunicações eletrónicas.[664]

---

degree of technological development in different countries, it was felt that record storage should be left outside the scope of the Convention". "A/CN.9/608/Add.2", par. 7.

[663] A redação desta norma é a seguinte:*"Nothing in this Convention requires a party to use or accept electronic communications, but a party's agreement to do so may be inferred from the party's conduct"*. "UNCUECIC". United Nations Commission on International Trade Law; United Nations, New York, 2007, pág. 5.

[664] Esse princípio foi expresso nos trabalhos preparatórios da UNCUECIC, do seguinte modo:*"Where the law did not provide a form requirement, it was conceivable that an oral reply to a written offer might constitute a valid reply, in much the same way as a data message would under the draft article. Where a form requirement existed, the draft article was expressing a legislative policy choice to ensure the equivalence between data messages and paper-based writings"*. A/CN.9/546, par. 43.

Só mais tarde os pressupostos de equivalência dos documentos eletrónicos passaram a transportar-se para pressupostos das assinaturas e a equivalência se centrou nestas, com a consagração do conceito de assinatura eletrónica que a tecnologia digital proporcionou.

Apesar de as funções essenciais da assinatura eletrónica serem as mesmas da assinatura manuscrita, os suportes sobre que assentam são diferentes. O conceito tradicional de assinatura é próprio para os documentos em papel, que não é transponível linearmente para os documentos eletrónicos. Todas as normas legais anteriores à emergência dos mecanismos eletrónicos de criação e de comunicação de documentos que preveem a assinatura referem-se, naturalmente, à assinatura de documentos em suporte de papel, tendo sempre como referência fundamental a assinatura manual autógrafa.[665]

A aplicação do conceito de assinatura aos documentos eletrónicos não é linear, em razão da diferença estrutural dos suportes sobre que se aplica, e não podemos dizer que nesta matéria a diferença entre uma assinatura de um documento em papel e de um documento eletrónico existe apenas uma diferença do suporte utilizado. Utilizar o conceito de assinatura aplicando-o a um documento eletrónico é não é um procedimento linear, uma vez que uma assinatura é um ato físico de colocação de uma marca visível e indelével num objeto material que é o papel. Isso não é possível nos documentos eletrónicos. Por essa razão podemos dizer que não existem assinaturas eletrónicas, quando utilizamos o conceito de assinatura na sua essencialidade tradicional.

Podem existir instrumentos eletrónicos suscetíveis de produzir os mesmos efeitos nos documentos eletrónicos que os de uma assinatura nos documentos em papel, mas esse facto não lhes confere a natureza de assinaturas nessa aceção tradicional.

A assinatura eletrónica é uma convenção que é estabelecida para que, uma vez verificados os requisitos estabelecidos, se apliquem ao documento eletrónico correspondente os mesmos efeitos que a lei prevê para os documentos escritos assinados em papel. A assinatura eletrónica não é ontologicamente uma assinatura, igual, na sua essencialidade, à assinatura manual e autógrafa. Trata-se antes de um conjunto de procedimentos eletrónicos e humanos que produzem os mesmos resultados de uma

[665] Como se refere no Guia de Aplicação da LMCE, o conceito de assinatura formou-se, sedimentou-se e está claramente associado à utilização do papel como suporte documental. *"The notion of signature is intimately linked to the use of paper"*. "Guide to Enactment LMCE (1996)", par. 55.

assinatura manuscrita e autógrafa, mas não se trata da mesma entidade.[666] Mas as necessidades de autenticação são maiores nos suportes eletrónicos do que no papel, pelo que a vontade das partes pode conduzir a que o recurso à documentação dos atos seja mais frequente nesses casos e, em consequência se aplique com maior frequência a assinatura eletrónica. Por outro lado, nas transações não eletrónicas as declarações negociais, expressas quase sempre de forma verbal, volatilizam-se com a sua manifestação e desaparecem. Mas isso não acontece nas transações eletrónicas que operam sempre com dados que são registados, sendo que esses dados quando formam conjuntos com conteúdo e significado jurídico são documentos eletrónico.

Mesmo nos casos em que se tarte materialmente de documentos eletrónicos, mas apenas de conjunto s de dados aos quais se aplica uma assinatura eletrónica, em termos legais, esses procedimentos são designados de assinatura, para que a sua equivalência à assinatura manual e autógrafa seja plena, desde logo no próprio nome.

Essa equivalência faz subingressar o documento a que foram aplicados os procedimentos que a lei estabelece, na mesma posição jurídica em que se encontram os documentos em papel assinados, aplicando-se-lhe, a partir daí, os efeitos jurídicos que a ordem jurídica prevê para os documentos assinados. Mas as exigências legais de vinculação do instrumento em que se materializa a assinatura ao documento assinado e ao signatário terão que ser adequadas ao suporte utilizado, que no papel é um objeto e nos suportes eletrónicos é um conjunto de procedimentos automatizados.

3. O princípio da neutralidade tecnológica

Existem vários tipos de assinatura eletrónica, desde os mais antigos e rudimentares, como eram as assinaturas digitalizadas e as palavras-chave, até às assinaturas digitais e aos métodos biométricos. Existem também vários tipos de tecnologias disponíveis nos mercados, para a criação de instrumentos de assinatura eletrónica. O princípio da neutralidade tecnológica impede a lei de adotar alguma dessas tecnologias em detrimento de outras, deixando à liberdade das partes essa opção, em função das suas necessidades de segurança jurídica. Os efeitos consignados na lei para a

[666] Como afrma Rivero, *"cuando se habla de la firma electrónica debe tenerse en cuenta que, en realidad, no es una firma, sino un procedimiento electrónico que cumple una función equivalente a la firma"*. Rivero, D.C. (Mayo 2005); op. cit., pag. 11.

utilização, pelas partes, de qualquer um destes tipos de assinatura, devem ser equivalentes, independentemente da tecnologia utilizada.[667]

Este princípio é importante, face à preponderância que a assinatura digital adquiriu no contexto das assinaturas eletrónicas.[668] A assinatura digital congrega a mais avançada tecnologia e conhecimento na utilização da criptografia, para dar resposta aos desafios das comunicações e das redes eletrónicas, sendo atualmente a mais completa tecnologia de assinatura eletrónica. A emergência desta tecnologia, nos últimos anos de século XX, conduziu alguns países a aprovar e fazer entrar em vigor leis de assinatura eletrónica, seguindo exclusivamente o modelo da assinatura digital, confundindo a assinatura digital com a assinatura eletrónica.[669]

Por essa razão, já depois da publicação dos primeiros diplomas normativos sobre assinatura eletrónica, a LMAE veio consagrar o princípio da neutralidade tecnológica, deixando à liberdade das pessoas a possibilidade de optarem por qualquer modalidade de assinatura para se vincularem nos suportes eletrónicos.[670]

A LMAE consagra este princípio no art.º 5.º.[671] Dele não resulta que todos os tipos de assinatura possuam a mesma eficácia no que respeita à segurança das partes na sua vinculação aos documentos assinados e aos seus efeitos jurídicos.[672] Qualquer

---

[667] A adoção deste princípio foi assumida como uma necessidade, desde logo para evitar que cada país adotasse um método específico de técnica de assinatura, o que poderia conduzir a uma segmentação internacional e à impossibilidade prática do comércio eletrónico internacional. É nesse sentido que o Global Action Plan for Electronic Commerce da OCDE, de 1998, o defende de forma expressive. *"Standards for electronic signatures that are used or recognised by governments should be technology neutral, not endorse". or favour any particular solution and should allow for technological innovation"*. Disponível em http://www.witsa.org/papers/globecom.htm, pág.s 15 e 16 (última consulta em 2/5/2016).

[668] Esse peso da assinatura digital era sensível nos trabalhos preparatórios da LMAE e logo de início esteve presente o cuidado de não privilegiar essa tecnologia relativamente às demais. *"The Working Group might appropriately focus its attention on the issues of digital signatures in view of the apparently predominant role played by public-key cryptography in the emerging"*. A/CN.9/WG.IV/WP.73, par. 4.

[669] Era o caso, por exemplo, da Lei da Assinatura Eletrónica do Estado do Utah, o primeiro diploma legal de assinatura eletrónica, que só admitia como assinaturas as que utilizassem a tecnologia das assinaturas digitais. *"In that connection, it was pointed out that neutrality should be ensured also as to the way in which a particular technology was being implemented (e.g., a digital signature with or without a certificate)"*. "A/CN.9/446", par. 54.

[670] O princípio da neutralidade tecnológica inclui a possibilidade de as partes num negócio utilizarem uma tecnologia determinada apenas parcialmente. É o caso, por exemplo, das situações em que as partes num negócio utilizam pares de chaves assimétricas para se autenticarem, sem recorrer a serviços prestados por terceiros, nomeadamente a entidades certificadoras. *Ibidem*.

[671] Que, subordinado ao título *"Equal treatment of signature technologies"*, tem a seguinte redação: *"Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6, paragraph 1, or otherwise meets the requirements of applicable law"*. "UNCITRAL Model Law ... 2001", pág. 2.

[672] Essa ressalva é importante e consta do próprio Guia para a transposição da LMAE: *"However, article 3 should not be misinterpreted as establishing the legal validity of any given signature technique or of any electronically signed information"*. "UNCITRAL Model Law ... 2001", par. 107.

tecnologia pode possuir graus diversos de eficácia no que respeita àquela segurança de vinculação, e o reconhecimento de que cada um desses graus pode possuir diferentes efeitos jurídicos, não colide com o princípio da neutralidade tecnológica.[673] Porém, a eficácia vinculativa e os efeitos legais, não dependem necessariamente da tecnologia, mas antes das funções que cada um dos tipos de assinatura e cada um dos tipos de tecnologia proporcionam.

O efeito deste princípio traduz-se numa garantia de não discriminação em função da tecnologia utilizada, e na garantia de que nenhuma assinatura eletrónica ficará excluída de relevância jurídica em face da tecnologia em que assenta.[674]Mas uma coisa é a tecnologia utilizada para assinar e coisa diferente é o grau de fiabilidade dos procedimentos que em concreto são utilizados na criação das assinaturas em concreto, bem como os respetivos efeitos jurídicos. Esse grau de fiabilidade pode variar em todos os tipos de assinaturas, e não é ele que as distingue. É possível, por exemplo que uma assinatura que utiliza a tecnologia das chaves assimétricas seja pouco fiável, porque não foram adotados os procedimentos de segurança na identificação do titular ou de salvaguarda na exclusividade do acesso ao dispositivo do qual consta o instrumento de criação da assinatura. A fiabilidade não depende da tecnologia que é utilizada, mas dos procedimentos e dos métodos estabelecidos. Este princípio não se relaciona com os níveis de fiabilidade das assinaturas em concreto, mas apenas com as tecnologias de assinatura que são utilizadas.

Os efeitos jurídicos que a LMAE consagra, bem como os respetivos pressupostos, são de natureza substancial e formal, e podem ser preenchidos por qualquer tipo de meios tecnológicos que as partes entendam utilizar.[675] As leis de

---

[673] Como se refere nos documentos dos trabalhos preparatórios da LMAE, o princípio da neutralidade tecnológica respeita à não discriminação quanto aos meios técnicos utilizados e já não quanto aos graus de eficácia que cada um desses meios técnicos pode proporcionar relativamente à segurança jurídica quanto à vinculação das partes. *"The principle of media-neutrality"*. "A/CN.9/WG.IV/WP.82", par. 15.

[674] Essa preocupação foi claramente manifestada nos trabalhos preparatórios: *"The purpose of the draft article is to ensure the media-neutrality of the Uniform Rules, to make it clear that the use of low-security authentication techniques is not prohibited"*. "A/CN.9/WG.IV/WP.76", par. 21.

[675] A materialização deste princípio efetua-se mediante a neutralidade das normas legais, não devendo, em caso algum, a satisfação dos pressupostos legais depender da utilização em concreto de uma tecnologia específica. *""Neutral" rules; that is, they do not depend on or presuppose the use of particular types of technology and could be applied to communication and storage of all types of information"*. "A/CN.9/608/Add.1", par. 4.

assinatura eletrónica devem ser adequadas para que os seus pressupostos se possam alcançar independentemente dos meios tecnológicos utilizados.[676]

A consagração deste princípio é também uma necessidade de permitir que se desenvolvam novas tecnologias de autenticação eletrónica, para além das que já estão disponíveis nos mercados, bem como para que estas se aperfeiçoem.[677] O direito da autenticação eletrónica, como todos os ramos do direito, utiliza as técnicas disponíveis que são utilizadas nas relações jurídicas, mas as tecnologias de assinatura eletrónica são relativamente recentes e estão em desenvolvimento, pelo que a legislação que as regula deve possuir a abertura suficiente para não ser, ela mesma, um fator que impeça o seu aperfeiçoamento e inovação.[678] [679]

4. O princípio da liberdade contratual

As assinaturas eletrónicas, tal como as assinaturas manuscritas, proporcionam graus diferenciados de autenticação, correspondentes a gradações diversas de segurança na vinculação dos documentos.

Quando se trate de negócios privados, entre duas partes que se conhecem e que utilizam um canal privado de comunicação é natural que a necessidade de recurso a assinaturas eletrónicas que proporcionem um nível mais elevado de segurança não seja

---

[676] A neutralidade tecnológica é, antes de mais, a neutralidade de meios. *"Technological neutrality encompasses also "media neutrality""*. "A/CN.9/608/Add.1", par. 5.

[677] O princípio da neutralidade tecnológica desempenha um importante papel na abertura da LMAE à inovação tecnológica. Essa capacidade de ajustamento da lei à inovação é importante para que ela não fique obsoleta e caia em desuso em razão de uma evolução tecnológica que é expectável que venha a ocorrer. *"Technological neutrality is particularly important in view of the speed of technological innovation and development, and helps ensure that the law is able to accommodate future developments and does not quickly become dated"*. "A/CN.9/608/Add.1", par. 5.

[678] Esta preocupação foi defendida pela delegação dos EUA nos trabalhos preparatórios da LMAE, com a proposta de uma resolução nos seguintes termos: *"Technology Neutrality - Any rules should neither require nor hinder the use or development of authentication technologies. States should anticipate that authentication methods will change over time and avoid legislation that might preclude innovation or new applications. States should avoid laws that intentionally or unintentionally drive the private sector to adopt only one particular technology for electronic authentication to the exclusion of other viable authentication methods"*. A/CN.9/WG.IV/WP.77, pág. 3.

[679] Como refere o Guia para a Transposição da LMAE, *"No method of electronic signature should be discriminated against, that is, that all technologies would be given the same opportunity to satisfy the requirements of article 6. As a result, there should be no disparity of treatment between electronically signed messages and paper documents bearing handwritten signatures or between various types of electronically signed messages, provided that they meet the basic requirements set forth in article 6, paragraph 1, of the Model Law or any other requirement set forth in applicable law"*. E mais adiante, "*Article 3 merely indicates that the form in which a certain electronic signature is applied cannot be used as the only reason for which that signature would be denied legal effectiveness"*. "UNCITRAL Model Law, 2001", par. 107.

tão intensa como quando as partes não se conhecem e utilizam redes abertas de comunicação. É possível que as assinaturas que conferem níveis mais elevados de segurança sejam mais dispendiosas em termos financeiros e também em termos procedimentais da sua utilização.

Quando as partes se conhecem e confiam entre si, podem estabelecer métodos de autenticação criados por elas próprias, sem necessidade de intervenção de terceiras entidades, sendo possível a uma dela emitir um par de chaves que utiliza exclusivamente para se autenticar perante a outra, incluindo nos casos em que são utilizadas chaves assimétricas.

O respeito pela validade deste tipo de convenções de autenticação é um dos fundamentos do direito da assinatura eletrónica e esteve na base do reconhecimento da relevância jurídica de todas as formas de autenticação eletrónica convencionadas entre as partes, mesmo quando não sejam de um dos tipos previstos na lei, e desde que, naturalmente, não a violem.[680] Aliás, foi no seio das relações comerciais, que normalmente se estabelecem entre empresas que se conhecem e praticam operações repetidas entre si, em redes fechadas que nasceu o direito da assinatura eletrónica.[681] As necessidades de segurança no que respeita à identificação e à vinculação das partes são diferenciadas, em conformidade com o contexto das relações que entre elas se estabelecem e o seu objeto e finalidade, relevando, em especial o grau de risco que cada transação envolve e a necessidade de o diminuir, que resulta da avaliação que as partes efetuam.[682] Por essa razão, são as partes que intervêm nas comunicações eletrónicas que melhor conhecem as necessidades de segurança que são adequadas e que devem ser satisfeitas em ordem a que os negócios por elas celebrados possam ser válidos e eficazes.[683]

---

[680] Mariliana Carrillo entende que este princípio é apenas um corolário do princípio da não alteração do direito pre-existente, porque o concebe como respeitando à relação jurídica subjacente. Porém este princípio vai mais longe e abrange a própria autonomia contratual no que respeita à determinação do modo de identificação e de autenticação dos documentos eletrónicos que as partes troquem entre si. Carrillo, Mariliana Rico; op. cit., pag. 144.

[681] A assinatura eletrónica nasceu no seio das comunicações eletrónicas efetuadas através de redes fechadas. *"With respect to electronic signatures, the practical importance of "closed" networks makes it necessary to provide wide recognition of party autonomy"*. A/CN.9/WG.IV/WP.73, par. 14.

[682] A liberdade das partes quanto aos métodos de autenticação foi consensual na conceção da LMAE. *"The purpose of the draft article is to ensure the media-neutrality of the Uniform Rules, to make it clear that the use of low-security authentication techniques is not prohibited, and to provide appropriate recognition of party autonomy, without allowing parties to derogate from mandatory rules of law relating to signatures"*. "A/CN.9/WG.IV/WP.76", par. 21.

[683] A salvaguarda do princípio da autonomia foi repetida pela delegação dos EUA nos trabalhos da LMAE: *"Party Autonomy - Parties to a transaction should be permitted, to the maximum extent possible, to determine by contract the appropriate technological and business methods of authentication with the*

A LMAE consagra a prevalência das formas de autenticação mediante acordo entre as partes, desde que esse acordo seja válido e que não viole as normas da LMAE.[684] Essa prevalência ocorre mesmo nos casos em que se trate de formas de autenticação que a lei não prevê ou que as partes ajustem os modos de autenticação legalmente previstos.[685]

Os limites estabelecidos na LMAE para a vontade das partes na convenção de modelos de autenticação são os limites gerais da proibição de acordos que violem normas imperativas, que normalmente se destinam a proteger o interesse de terceiros ou o interesse público.[686]

A eficácia deste princípio é também alargada pela LMAE aos casos em que se considera a assinatura eletrónica equivalente às assinaturas eletrónicas reconhecidas. Esse regime de equivalência consta dos art.ºs 6.º e 7.º da LMAE, sendo que ela poderá resultar de um acordo entre as partes, desde que, no contexto desse acordo, se verifique o pressuposto da fiabilidade do método de autenticação convencionado e utilizado pelas partes.[687]

A prevalência do princípio da autonomia contratual das partes é também reconhecida no que respeita ao reconhecimento internacional das assinaturas eletrónicas, sendo estabelecida pela LMAE no n.º 5 do art.º 12.º. Nos seus termos, e sem prejuízos da proibição da violação de normas imperativas, uma assinatura eletrónica criada no estrangeiro, seja por uma entidade certificadora ou não, será sempre

---

assurance that those means will be recognized as legally binding, whether or not those technological and business means are specifically addressed by legislation or regulation". "A/CN.9/WG.IV/WP.77, pág. 2.

[684] O artigo 5.º da LMAE, sob o título "*Variation by agreement*", tem a seguinte redação: *"The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law"*. "UNCITRAL Model Law ... 2001", pág. 2. Como se refere no Guia da Transposição da LMAE, esta disposição legal manifesta um princípio de ampla confiança do legislador na autonomia de vontade das partes e da sua liberdade de vinculação. *"Extensive reliance on party autonomy"*. *Ibidem*, párágrafo 67.

[685] *"… Freedom of the parties to agree among themselves that they could derogate from or vary the provisions of these Rules, for the purposes only of transactions between the agreeing parties"*. "A/CN.9/WG.IV/WP.82", par. 36. Essa liberdade de as partes definirem entre si as formas de autenticação que adotam está também expressa no seguinte trecho: *"… Ability of the parties to agree on how to conduct their transactions between themselves and, in particular, on what might constitute a signature"*. "A/CN.9/465", par. 45.

[686] *"Article 5 should not be misinterpreted as allowing the parties to derogate from mandatory rules, e.g., rules adopted for reasons of public policy"*. A/CN.9/WG.IV/WP.86/Add.1, 16 August 2000, par. 11.

[687] *"Paragraph 4 (a) is intended to provide a legal basis for the commercial practice under which many commercial parties would regulate by contract their relationships regarding the use of electronic signatures"*. "UNCITRAL Model Law ... 2001", par. 128.

reconhecida como válida e eficaz, se tiver sido livremente convencionada como instrumento de autenticação pelas partes.[688]

Do mesmo modo o Regulamento EIDAS deixa à liberdade de escolha das partes a opção por qualquer tipo de assinatura eletrónica, assegurando no n.º 1 do artigo 25.º a relevância jurídica de todas, sem prejuízo da maior eficácia probatória das assinaturas eletrónicas qualificadas que é consignada no n.º 2.

[688] *"Paragraph 5 provides for the recognition of agreements between interested parties regarding the use of certain types of electronic signatures or certificates as sufficient grounds for cross-border recognition (as between those parties) of such agreed signatures or certificates".* "UNCITRAL Model Law ... 2001", par. 160.

Capítulo II – Os sujeitos da assinatura eletrónica

Para assinar um documento em papel, basta ao signatário possuir uma caneta que escreva. São esses dois instrumentos simples – caneta e tinta – os únicos que são indispensáveis para executar o ato da assinatura sobre um documento em papel.

Uma assinatura eletrónica não tem a mesma simplicidade naturalística. O autor da assinatura deve possuir, além de um instrumento para criar a assinatura eletrónica que contenha, por exemplo, uma chave privada, os instrumentos necessários para que o sistema informático efetue os processamentos matemáticos de aplicação do algoritmo aos dados de base do documento, gerando assim a sequência de dados em que consiste a assinatura.

Para obter esses elementos, o autor da assinatura necessita de os adquirir a um prestador de serviços de confiança. Essa entidade procede à geração de um par de chaves matematicamente relacionadas. Esta é uma das mais importantes funções das entidades terceiras que prestam serviços de confiança.

A outra função destas entidades é a de certificarem a identidade do titular de uma determinada chave pública. Esse serviço depende de outros dois serviços que lhe

estão subjacentes, que são o procedimento de identificação do titular da assinatura e a credibilidade que o prestador de serviços oferece. Para isso, estas entidades devem possuir essa credibilidade, para gerar a confiança necessária, que garantam a todos os interessados que a pessoa que diz ser o titular de uma chave pública corresponde efetivamente a essa pessoa.

Nas assinaturas eletrónicas uma chave privada é apenas um conjunto de algarismos e o algoritmo que efetua a encriptação é apenas uma fórmula matemática. E assim é, também, com o conjunto de dados que resultam da aplicação de um algoritmo a um documento. Trata-se apenas de uma sequência numérica ininteligível, mesmo quando resumida previamente pelo *hash*.

Para que um destinatário que recebe um documento assinado por uma assinatura eletrónica fique a saber quem é o assinante, necessita de saber que a chave privada que deu origem à sequência de dados que constituem a assinatura eletrónica que o acompanha, pertence a uma determinada pessoa. [689] [690] É que o sistema criptográfico de chaves assimétricas é um mecanismo puramente objetivo e matemático, nada tem de pessoal ou de subjetivo. Como se pode então ligar esse sistema a uma pessoa em concreto, ou seja, como podemos subjetivizar esse sistema?

Essa função é própria dos chamados Prestadores de Serviços de Confiança.[691] São eles que, cumprindo um conjunto de requisitos legalmente tipificados, asseguram que determinado par de chaves corresponde a uma pessoa em concreto.[692] Estas entidades desempenham um importante papel de serem terceiros de confiança,[693] a quem a ordem jurídica reconhece credibilidade que é fonte de confiança para todos os interessados, sendo que ela advém do cumprimento, por estas entidades, de um conjunto de obrigações legais que a legitimam, bem como de um controlo mais rigoroso da sua

[689] Como se refere em "A/CN.9/WG.IV/WP.88", par. 45, *"However, a public and private key pair has no intrinsic association with any person; it is simply a pair of numbers"*.
[690] No mesmo sentido Ortega Diaz: *"O receptor de uma mensagem assinada digitalmente está seguro apenas de que a chave privada com a qual a mensagem foi assinada, corresponde a uma chave pública. Não obstante, não pode ter a certeza de que de que o titular daquela chave é quem diz ser"*. Díaz, J.J.O., Op. Cit., pág. 53.
[691] A lei portuguesa (DL n.º 290-D/99, de 3/8), designa estas entidades de "*entidades certificadoras*" (artigo 9.º e seguintes), mas o Regulamento EIDAS designa-as de prestadores de serviços de confiança (em especial artigo 19.º).
[692] Como afirmam Velásquez, Rubio e Sau, "*a identificação do assinante realiza-se mediante a chave pública que evidencia a posse, por ele, da chave privada*". Velásquez, R.R., Sau, C.R. e Muñoz, R.M. (2004). Op. cit., pág. 193.
[693] Díaz, J.J.O., Op. Cit., pág. 53.

atividade. Uma das mais importantes funções destas entidades é declararem exatamente que determinada chave pública está vinculada a determinada pessoa.[694]

O funcionamento eficiente dos sistemas de assinatura eletrónica depende, assim, de três sujeitos:

i) O titular da assinatura eletrónica, que o Regulamento EIDAS designa de signatário, que voluntariamente se vincula a documentos, comunicações ou transações, mediante a utilização de um dispositivo de assinatura;

ii) As entidades que prestam serviços de confiança neste domínio, nomeadamente os serviços de certificação, que o Regulamento EIDAS designa de prestadores de serviços de confiança e;[695]

iii) Todas as pessoas que recebem documentos ou interações eletrónicas assinados e que, com recurso aos elementos disponibilizados pelos seus autores e fundamentalmente pelas entidades certificadoras, verificam a autenticidade desses documentos ou transações.

Essas três entidades têm papéis distintos num sistema de assinatura eletrónica. Os primeiros, que são os titulares da assinatura, que a utilizam, cumprem a função de assinar os documentos, os segundos a função de certificação da assinatura e os terceiros a função de confiar na assinatura.[696] Por essa razão, a estes também chamamos de entidades que confiam nas assinaturas.[697]

São as funções destas três entidades que vamos analisar de seguida.[698]

---

694 Citando, *"An additional mechanism is necessary to associate reliably a particular person or entity to the key pair"*. "A/CN.9/WG.IV/WP.88", par. 45.

695 A origem da função das entidades terceiras que prestam serviços de confiança advém também da função desempenhada pelas entidades de registo nas operações de documentação eletrónica das transações de mercadorias em circulação nos mercados internacionais. A passagem, para os suportes eletrónicos, dos chamados conhecimentos de embarque, que eram títulos em papel, cuja posse era prova da titularidade das mercadorias, foi viabilizada pela criação de entidades de registo. Essas entidades emitiam chaves privadas a cada um dos sucessivos titulares de mercadorias, servindo essas

696 *"Three functions (or roles) with respect to key pairs, namely, the key issuer (or subscriber) function, the certification function and the relying function"*. "A/CN.9/457", par. 68.

697 *"The signatory function, the certification function, and the relying function"*. "A/CN.9/493", par. 32.

698 *"Setting up a public key infrastructure (PKI) is a way to provide confidence that: (1) a user's public key has not been tampered with and in fact corresponds to that user's private key; (2) the encryption techniques being used are sound; (3) the entities that issue the cryptographic keys can be trusted to retain or recreate the public and private keys that may be used for confidentiality encryption where the use of such a technique is authorized; (4) different encryption systems are inter-operable"*. "A/CN.9/WG.IV/WP.71", par. 33.

1. Os prestadores de serviços de confiança[699]

A função destas entidades consiste, essencialmente, em proporcionar às partes um bem jurídico essencial à atividade económica. Esse bem jurídico é a confiança, neste caso na utilização dos suportes eletrónicos nas suas relações jurídicas.

A confiança é um bem jurídico essencial também no paradigma do papel, sendo entidades terceiras que a garantem, como é o caso das que são competentes para a identificação civil e os notários. Em última instância é a informação gerada por elas que nos confere confiança. Mesmo quando não recorremos a ela é apenas porque eventualmente já o havíamos feito alguma vez no passado. A necessidade de fazer intervir essas entidades depende da tipologia das relações que se estabelecem.

No paradigma eletrónico, a participação das entidades que prestam serviços de confiança no fornecimento desse bem jurídico é ainda mais importante, em especial nas redes abertas, em que é necessário estabelecer relações jurídicas com pessoas desconhecidas, à distância, e sempre através da mediação e interação de máquinas e sistemas informáticos,[700]

Os prestadores de serviços de confiança cumprem, no domínio eletrónico, funções relativamente próximas das que desempenham as entidades com competência de identificação das pessoas e relativamente aos notários, embora não venham substituir nem umas nem outras. Aliás a função destas entidades releva também para os suportes eletrónicos.

Nas comunicações eletrónicas é essencial conhecer a identidade das partes e, como elas não são presenciais, é necessário garantir que a segurança que é oferecida pelas entidades com competência na identificação civil se estende através das máquinas que operam as comunicações eletrónicas. Essa extensão é uma das funções dos prestadores de serviços de confiança.

Em segundo lugar, o facto de uma assinatura eletrónica ser um conjunto de dados produzido por um sistema informático que opera numa máquina e de esses dados

---

[699] Utilizamos o conceito que foi adotado pelo Regulamento EIDAS, mas a LMAE designa-as de Prestadores de Serviços de Certificação, depois de várias designações possíveis: *"As a matter of drafting, it was generally agreed that the term "certification service provider (CSP)" was commonly used in practice and should be preferred to "information certifier", "supplier of certification services" or "certification authority"*. "A/CN.9/483", par. 66.

[700] Como se refere na primeira proposta de Diretiva da UE sobre Assinaturas Eletrónicas, de 1998, *"A verificação da autenticidade e da integridade dos dados não prova necessariamente a identidade do signatário que cria as assinaturas eletrónicas"*. ("COM(1998) 297 final").

dependerem de outros dados que são externos aos documentos, exige que seja estabelecida entre o autor da assinatura e o instrumento de geração dos dados que compõem a sua assinatura, um vínculo inquestionável, e a construção desse vínculo não pode depender daquelas entidades.

Em terceiro lugar, essa garantia de vinculação não é um ato instantâneo, mas uma atividade que se prolonga no tempo. E o tempo tem uma relevância jurídica nas assinaturas eletrónicas diferente daquela que tem nas assinaturas manuscritas. A assinatura eletrónica é um instrumento tecnológico que se adquire nos mercados, e não uma caraterística intrínseca do seu autor como é a assinatura manuscrita. Esta última é uma caraterística própria da pessoa, que a acompanha a vida toda. O estilo com que o autor desenha a sua assinatura no papel faz parte da sua própria essência e forma de expressão, é um estilo que é inato àquela pessoa e depende apenas dela.

Pelo contrário, uma assinatura eletrónica é produzida por uma infraestrutura lógica que se adquire e que em condições normais é produzida por terceiros. E sendo algo que é externo à pessoa que a utiliza, pode ser também apropriado por terceiros, incluindo para fins ilícitos, pelo que, por razões de segurança, esse instrumento deve ter um período de validade limitado, a fim de se renovar periodicamente a garantia da sua vinculação ao seu legitimo titular. Por outro lado, o instrumento da assinatura pode, ao longo do seu período de validade, ser exposto à possibilidade de ser utilizado por terceiros, pode o seu titular perder a sua posse, etc. Nesses casos terá que existir um regime de suspensão e de cancelamento, a fim de se garantir a segurança e a confiança nesse instrumento.

A gestão do ciclo de vida dos instrumentos de assinatura eletrónica é uma das mais importantes funções das entidades certificadoras.

Em correspondência, estas entidades prestam o serviço de disponibilizar informação acerca da validade e da vigência das assinaturas eletrónicas, tanto no momento em que os documentos assinados são recebidos pelos interessados, como na data em que eles foram efetivamente assinados pelo seu autor.

Finalmente, como entidades que geram confiança, estas entidades devem ser elas próprias credíveis, devendo essa sua credibilidade ser universal e inquestionável, dado que o âmbito das pessoas que necessitam de confiar nelas é potencialmente universal.

A LMAE define prestador de serviços de certificação como a entidade que emite certificados de assinatura eletrónica e que pode prestar outros serviços

relacionados com as assinaturas eletrónicas.[701] Ao longo dos trabalhos preparatórios foi eliminado o requisito de que essa fosse a atividade principal da entidade, para que o âmbito da LMAE abrangesse todas as entidades que emitem certificados, mesmo nos casos em que a sua atividade principal é outra. Podem existir situações em que uma entidade que exerce outra qualquer atividade emita certificados para se relacionar com outras entidades com as quais possui convenção de autenticação, ou então situações em que uma empresa emite certificados para que os seus trabalhadores se possam relacionar com ela ou com terceiros por via eletrónica.[702]

O Regulamento EIDAS define como prestador de serviços de confiança qualquer *"pessoa singular ou coletiva que preste um ou mais serviços de confiança"*, incluindo os serviços de criação e de gestão de dispositivos de assinatura eletrónica ou de outro qualquer serviço de confiança previsto no Regulamento.[703] Incluem-se na definição, quer os prestadores qualificados quer os não qualificados, sendo que ambos estão submetidos aos poderes de controlo das entidades de supervisão, apesar de esse controlo ser mais intenso para os primeiros. O Regulamento EIDAS veio, pela primeira vez, criar o estatuto de prestador qualificado, sujeitando-o a reconhecimento prévio para concessão do respetivo estatuto (n.º 20 do artigo 3.º) .

A regulação da atividade dessas entidades consta de todos os instrumentos legislativos relativos à assinatura eletrónica e à confiança jurídica eletrónica, como veremos de seguida.

1.1. Natureza das funções de confiança

As funções das entidades certificadoras desdobram-se em duas vertentes, conforme os destinatários dos serviços que prestam: [704]

[701] Essa definição consta da alínea e) do artigo 2.º e tem a seguinte redação: *""Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures".* "A/CN.9/WG.IV/WP.88", pág. 8.

[702] Esse entendimento foi definido de forma consensual nos trabalhos preparatórios. "*In the deliberations, it was decided that the definition of "certification service provider" should emphasize that, in all cases, the certification service provider as defined would have to provide certification services, possibly together with other services".* "A/CN.9/483", par. 100. Do mesmo modo, *"The definition covers all entities that provide certification services within the scope of the Model Law, i.e., "in the context of commercial activities""*. "A/CN.9/WG.IV/WP.88", par. 104

[703] N.º 19 do artigo 3.º.

[704] As funções destas entidades foram elencadas pela primeira vez em 1996, nos seguintes termos: *"(1) managing cryptographic keys used for digital signatures; (2) certifying that a public key corresponds to a private key; (3) providing keys to end users; (4) deciding which users will have which privileges on the*

i) Aos titulares de uma assinatura eletrónica, fornecem-lhes os instrumentos necessários para a possuírem, sendo esses instrumentos o par de chaves e o suporte magnético de onde ele consta (um cartão magnético que pode ser lido por um computador, um CD, uma *pen-drive*).[705] Trata-se dos instrumentos de criação de assinaturas eletrónicas ou, como o Regulamento EIDAS os designa, de dispositivos de criação de assinaturas eletrónicas (n.º 22 do artigo 3.º). Prestam-lhes ainda um conjunto de serviços destinados a garantir a fiabilidade desse instrumento de assinatura ao longo do tempo, como veremos já de seguida;

ii) Aos destinatários dos documentos e das comunicações eletrónicas dão a conhecer a identidade das partes de quem recebem informação autenticada, garantindo a segurança e a fiabilidade dessa autenticação e a sua vinculação ao autor da assinatura. Esses serviços incluem a disponibilização da sua chave pública, para com ela poderem verificar as respetivas assinaturas. Num paradigma de redes abertas em que virtualmente é possível o estabelecimento de comunicações com relevância jurídica com um universo de pessoas desconhecidas, este papel é muito importante.[706]

Os prestadores de serviços de confiança podem prestar um conjunto vasto de serviços, nomeadamente os seguintes:[707],[708]

---

system; (5) publishing a secure directory of public keys or certificates; (6) managing personal tokens (e.g., smart cards) that can identify the user with unique personal identification information or can generate and store an individual's private keys; (7) checking the identification of end users, and providing them with services; (8) providing non-repudiation services; (9) providing timestamping services; (10) managing encryption keys used for confidentiality encryption where the use of such a technique is authorized". "A/CN.9/WG.IV/WP.71", par. 33.

[705] A previsão da possibilidade de fornecimento destes serviços está prevista e perpassa toda a LMAE, em especial o n.º 1 do artigo 9.º.

[706] Essa função era enfatizada pela UNCITRAL do seguinte modo: *"An additional mechanism is necessary to associate reliably a particular person or entity to the key pair. If public key encryption is to serve itsintended purposes, it needs to provide a way to send keys to a wide variety of persons, many of whom are not known to the sender, where no relationship of trust has developed between the parties. To that effect, the parties involved must have a high degree of confidence in the public and private keys being issued"*. "A/CN.9/WG.IV/WP.88", par. 45.

[707] Seguimos parcialmente, para o que releva da nossa investigação, a enunciação dos serviços prestados no âmbito de uma PKI, constante do documento "A/CN.9/WG.IV/WP.88", par. 50.

[708] No Regulamento EIDAS, estes serviços são designados de serviços de confiança eletrónica e estão enunciados genericamente no n.º 16 do artigo 3.º, bem como nos artigos 19.º e 24.º.

1 – A comprovação da identificação dos utilizadores finais que solicitem a emissão de pares de chaves de assinatura eletrónica, antes de a fornecerem;[709]

2 - A gestão dos pares de chaves de assinaturas eletrónicas. A necessidade desta gestão deve-se ao facto de o dispositivo que serve para assinar um documento eletrónico, ser um objeto e, como tal, suscetível de posse e de apropriação, quer pelo seu legítimo titular quer por terceiros. Ao contrário das assinaturas manuais, as assinaturas eletrónicas dependem de um dispositivo suscetível de posse, não pessoal nem inato, pelo que, por razões de segurança, deve possuir um período de validade limitado e deve ser suscetível de ser cancelado ou suspenso. Pela mesma razão, os terceiros que confiam devem poder conhecer esses períodos de suspensão e de cancelamento, bem como confirmar que a sua validade. Esses serviços são prestados pelos prestadores de serviços de confiança;[710]

3 – A certificação de que uma chave pública está matematicamente relacionada com uma chave privada determinada. Este serviço desdobra-se na informação geral acerca da vinculação das chaves pública e privada, da informação acerca da identidade do respetivo titular, mas também da própria integridade da assinatura eletrónica que foi colocada num determinado documento em concreto, detetando, nomeadamente nos casos de utilização ilícita com a cópia de uma assinatura legítima, de um documento assinado pelo seu titular, para um outro documento que não foi por ele assinado. A entidade certificadora pode atestar essa utilização ilícita e a violação da integridade da assinatura;[711]

4 – A publicação de guia seguro de emissão de pares de chaves. Trata-se de um requisito de transparência destinado a que todos os eventuais

[709] As obrigações das entidades certificadoras, correspondentes a estes serviços estão especificadas, em especial, na subalínea i) da alínea c) do n.º 1 do artigo 9.º da LMAE. No Regulamento UE n.º 910/2014, de 23/7, estão enunciadas, em especial para os prestadores qualificados, no n.º 1 do artigo 24.º.

[710] As obrigações das entidades certificadoras, correspondentes a estes serviços estão especificadas, em especial, nas subalíneas da alínea d) do n.º 1 do artigo 9.º da LMAE. No Regulamento UE n.º 910/2014, de 23/7, estão enunciadas, em especial para os prestadores qualificados, nos n.ºs 2 e 3 do artigo 24.º.

[711] As obrigações das entidades certificadoras, correspondentes a estes serviços estão especificadas, em especial, nas subalíneas da alínea c) do n.º 1 do artigo 9.º da LMAE e no artigo 24.º do Regulamento UE n.º 910/2014, de 23/7, para os prestadores qualificados.

interessados possam conhecer os métodos de segurança e de qualidade que fundamentam a confiança que se deposita nestas entidades;[712]

5 – A administração de senhas de acesso pessoais que possam servir para os utilizadores protegerem o acesso à sua chave privada, que consta sempre de um ficheiro informático que está gravado num suporte magnético de acesso exclusivo, sendo que esta exclusividade é protegida, normalmente, por uma palavra-passe. Essa palavra-passe é gerada, em primeiro lugar, pela entidade certificadora;[713]

6 – A prestação de serviços de repúdio negativo. A segurança jurídica na utilização da assinatura eletrónica inclui também a certeza de que em caso de alguém se fazer passar por outra pessoa ilicitamente, isso possa ser detetado e corrigido. Estas entidades possuem também essa obrigação de atestar que determinada chave pública não pertence a uma pessoa, nos casos em que alguém a pretende utilizar ilicitamente. Do mesmo modo, nos casos em que alguém, de forma ilícita, nega que tenha assinado determinado documento, alegando que determinada chave pública não lhe pertence, caberá às entidades certificadoras informar da verdade acerca do efetivo titular de determinada chave pública;[714]

7 – A prestação de outros serviços de confiança eletrónica, nomeadamente, de marcação cronológica. A utilização da tecnologia das assinaturas eletrónicas possibilita que fique registada a data e a hora em que uma chave privada foi aplicada a determinado documento, podendo assim o destinatário e qualquer pessoa que pretenda verificar essa assinatura, constatar essas circunstâncias de tempo. Essa possibilidade é um serviço que vai para além das funções essenciais de assinatura eletrónica, pelo que a sua prestação dependerá

[712] A obrigação dos prestadores de serviços nesta matéria está especificada, em especial, na alínea a) do n.º 1 do artigo 9.º da LMAE, que tem a seguinte redação: *"(a) act in accordance with representations made by it with respect to its policies and practices"*.

[713] A obrigação das entidades certificadoras, correspondente a este serviço está especificada, em especial, na subalínea ii) da alínea c) do n.º 1 do artigo 9.º da LMAE, que tem a seguinte redação: *"ii) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued"*. A/CN.9/WG.IV/WP.88", pág. 10.

[714] A prestação deste serviço pelas entidades certificadoras resulta das suas obrigações de gestão da validade dos certificados e da identificação dos titulares da assinatura, em especial constantes das alíneas b), c) e d) do n.º 1 do artigo 9.º da LMAE.

das condições contratuais estabelecidas entre o utilizador e a entidade certificadora.[715] O regulamento EIDAS veio acrescentar uma extensa lista de serviços que estas entidades prestam, que enunciámos no Capítulo VI da Parte II.

Analisamos de seguida, e em pormenor, os serviços fundamentais prestados por estas entidades, de emissão dos pares de chaves e de identificação dos titulares.[716]

1.1.1. A geração e fornecimento de pares de chaves de assinatura eletrónica

A geração deste instrumento é um procedimento com alguma criticidade, porque essa entidade está a gerar um instrumento de vinculação estritamente pessoal. Por essa razão, essa entidade necessita de possuir instrumentos e de adotar procedimentos de segurança para que mais ninguém possa aceder a esses elementos, nomeadamente à chave privada.

Para que essa entidade cumpra a sua função é necessário que assegure com rigor o cumprimento das seguintes obrigações:

i) A prévia identificação daquele titular, garantindo a certeza de que se trata da pessoa que constará do certificado;

ii) A entrega pessoal e exclusiva da chave privada a esse titular;

iii) Que mais ninguém receberá dessa entidade a mesma chave privada, que não pode ser gerada nova chave igual e que essa entidade também não a poderá utilizar.[717]

Estas garantias emergem da relação jurídica entre o prestador de serviços e o titular da assinatura, mas aquela entidade terá também que cumprir outras obrigações, de que são sujeitos ativos todas as pessoas que eventualmente venham a necessitar de verificar assinaturas privadas:

i) Que determinada chave pública pertence a determinada pessoa por ela identificada;

---

[715] A prestação deste tipo de serviços não consta das obrigações específicas das entidades certificadoras consignadas na LMAE, pelo facto de este não ser um serviço próprio das funções da assinatura eletrónica, mas um serviço que excede essas funções. Trata-se de uma função que é, porém, um instrumento importante de segurança jurídica que as tecnologias de assinatura eletrónica proporcionam.

[716] Outro tipo de serviço que as entidades certificadoras podem prestar é o de encriptação para fins de confidencialidade. Como estas entidades operam com tecnologia de encriptação, é natural que prestem serviços que lhe estão associados.

[717] A alínea g) do artigo 24.º do DL n.º 290-D/99, de 2/8, estabelece que a entidade certificadora deve garantir a *" sua confidencialidade [da chave privada] durante o processo da criação das chaves"*.

ii) Que essa chave pública corresponde à chave privada que está na posse exclusiva da pessoa que é o seu titular.

iii) Que a chave privada está vigente, é válida e íntegra;

iv) Que a chave pública é capaz de detetar eventuais utilizações abusivas da chave privada e de as assinalar aos interessados;

v) Que a chave pública é capaz de proporcionar os meios para detetar eventuais alterações ao documento assinado pela chave privada e de os assinalar.

A geração de pares de chaves assimétricas pode ser efetuada por qualquer pessoa que possua um sistema adequado, que pode adquirir nos mercados de produtos eletrónicos e podem ser usadas nas relações que se estabelecem entre elas, sem necessidade de intervenção de entidades terceiras. Essas chaves assim emitidas não cumprem os requisitos legais necessários para proporcionarem confiança a terceiros, dado que a entidade que as emitiu não é prestadora de serviços de confiança. É o cumprimento por estas de um conjunto de obrigações e de requisitos de segurança, sujeitos a auditoria e certificação, que é o fundamento da confiança dos agentes.[718] Com base no princípio da liberdade contratual entendia-se que as partes podiam, entre elas, estabelecer convenções de autenticação livremente. Mas o Regulamento EIDAS veio consagrar o princípio de que todas essas entidades, ainda que sejam partes em qualquer transação, e ainda que a sua atividade principal seja outra, são classificadas como prestadores de serviços de confiança, desde que prestem esse tipo de serviços, ficando sujeitas ao seu regime. O Regulamento EIDAS não se aplica apenas aos serviços de confiança utilizados "*exclusivamente dentro de sistemas fechados*" (n.º 2 do artigo 2.º), considerando-se, para esse efeito como tal os sistemas dentro dos quais são operadas

[718] A LMAE admite que a certificação possa ser feita por uma das partes, sem recurso a terceiros independentes, de acordo com o princípio de liberdade contratual, no art.º 5.º: *"The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law"*. O recurso a entidades independentes, especialmente os qualificados, é adequado nas situações em que as partes não se conheçam ou quando pretendem alcançar um nível de segurança mais elevado. Pode também uma parte estabelecer relações com uma entidade certificadora, e que essa entidade certificadora tenha sido a mesma que emitiu o seu próprio certificado. Nesse caso a entidade certificadora é ao mesmo tempo um terceiro que confia na assinatura eletrónica. *"The Model Law thus provides common grounds for PKI systems relying on independente certification authorities and electronic signature systems where no such independente third party is involved in the electronic signature process. In all cases, the new Model Law provides added certainty regarding the legal effectiveness of electronic signatures, without limiting the availability of the flexible criterion embodied in article 7 of the [LMCE]"*. "A/CN.9/WG.IV/WP.88", par. 28.

transações eletrónicas que não vinculam terceiros.[719] Ou seja, todos os serviços de confiança que sejam utilizados em transações que envolvam terceiros estão sujeitos ao regime do EIDAS.

1.1.2. A identificação dos titulares da assinatura eletrónica

A identificação dos titulares de assinaturas eletrónicas antes da emissão dos pares de chaves pelas entidades certificadoras é uma função essencial, da qual depende a vinculação do par de chaves ao respetivo titular. A confiança que é proporcionada pelos prestadores de serviços que emitem as chaves é a de assegurarem aos terceiros interessados que uma determinada chave pública está associada a uma pessoa determinada e identificada.

É dessa função que deriva a garantia universal, proporcionada pelos prestadores de serviços, da vinculação de uma determinada pessoa a um determinado par de chaves, e a confiança de todos os terceiros eventualmente interessados.

A identificação exigirá um conjunto rigoroso de procedimentos que têm que ser observados pelos prestadores de serviços, bem como de registos que sejam auditáveis por outras entidades e a certificação do cumprimento daqueles requisitos, sendo caso disso. A importância dos procedimentos de identificação é manifestada pelo cuidado do legislador, de a regular. Por exemplo a LMAE referencia duas vezes esse requisito no art.º 9.º.[720]

Quando se trata de assinaturas eletrónicas qualificadas, o Regulamento UE n.º 910/2014, de 23 de julho, estabelece requisitos mais rigorosos de identificação dos titulares dos pares de chaves, estabelecendo a presença física e pessoal como o meio normal de identificação, no n.º 1 do art.º 24.º. A identificação só pode ser efetuada à distância nos casos em que o meio de identificação que utilize tenha pressuposto, antes

[719] Como se refere no n.º 21 dos considerandos do Regulamento, "*Apenas os serviços de confiança prestados ao público com consequências para terceiros deverão cumprir os requisitos estabelecidos no presente Regulamento*". E no n.º 35, "*Todos os prestadores de serviços de confiança deverão ficar sujeitos aos requisitos do presente Regulamento"*.

[720] O artigo 9.º da LMAE estabelece as obrigações das entidades certificadoras, entre elas, a de proporcionarem meios para que os eventuais interessados possam verificar e avaliar qual o método que essas entidades utilizaram para identificar o titular da assinatura eletrónica. Entre os procedimentos estabelecidos pelo artigo 9.º, que as entidades certificadoras devem adotar, consta o de *"provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise: (i) the method used to identify the signatory;…"*. "A/CN.9/WG.IV/WP.88", página 10.

da sua emissão, a identificação mediante a presença física.[721] Uma das inovações deste regulamento é a densificação das normas relativas à segurança na identificação dos titulares das assinaturas, nomeadamente a especificação das formas dessa identificação, prevendo-se que seja feita por presença física do interessado ou à distância, mas utilizando assinatura eletrónica qualificada como meio de autenticação.

O Regulamento institui também deveres de prestação de informações das entidades que prestam serviços de certificação, às entidades de supervisão, bem como intensifica as garantias de confidencialidade e de proteção de dados.

As obrigações dos prestadores de serviços qualificados são elencadas no art.º 24.º do Regulamento e aplicam-se a todos os tipos de serviços que estas entidades prestam, uma vez que o Regulamento abrange um universo de serviços de confiança que vai além das assinaturas eletrónicas.

1.2. As Infraestruturas de chaves públicas (PKI)

O sistema de assinatura eletrónica é composto pelas relações e pela interação estabelecida entre os três sujeitos intervenientes no sistema de assinatura eletrónica. A articulação do funcionamento deste sistema designa-se de Infraestrutura de Chaves Públicas (ICP, ou PKI no acrónimo em língua inglesa).[722] [723]

As Infraestruturas de Chaves Públicas correspondem à forma como estão organizados, nos seus direitos e deveres e como se articulam nas suas funções, em cada ordem jurídica, o autor da assinatura, os prestadores de serviços de certificação e as partes que confiam.

---

[721] Esta previsão justifica-se, porque quando se utiliza um meio eletrónico de identificação mediante assinatura eletrónica qualificada, a identificação que foi utilizada para a emissão do respetivo certificado já possuía a segurança correspondente.

[722] Habitualmente este conceito é conhecido pelas iniciais em língua inglesa de PKI. *"Public key infrastructure (PKI)"*, no acrónimo inglês, usado a nível internacional. "A/CN.9/WG.IV/WP.71", par. 33.

[723] O conceito de PKI é definido desde os primeiros trabalhos preparatórios da LMAE, pela UNCITRAl, como um conceito relacional, de interoperabilidade entre todos os sujeitos do sistema de assinaturas eletrónicas. *"The interplay of relationships between three distinct types of parties (i.e., key holders, certification authorities and relying parties) corresponded to one possible PKI model, but that other models were conceivable, e.g., where no independent certification authority was involved"*. "A/CN.9/457", par. 68. Do mesmo modo, *"The interplay of relationships between three distinct types of parties (i.e., signatories, suppliers of certification services and relying parties) corresponds to one possible PKI model, but other models are already commonly used in the marketplace (e.g., where no independent certification service provider is involved)".* "A/CN.9/493", par. 32.

Os prestadores de serviços de confiança produzem esse bem essencial que é a confiança dos agentes na utilização dos suportes eletrónicos. Para isso devem ser entidades com credibilidade no mercado, sendo que essa credibilidade não se decreta e deve estar legitimada num conjunto de fatores.

Para garantir essa credibilidade, são estabelecidas hierarquias de confiança internacional, através das quais entidades certificadoras conhecidas e conceituadas no mercado emitem certificados de que outras entidades cumprem os requisitos técnicos necessários à prestação com segurança deste tipo de serviços.[724]

Os agentes que confiam nestas entidades são também titulares de um direito, que é o de poderem confiar nos serviços por elas prestados. A esse direito corresponde um dever de resultado das entidades certificadora, que é o dever de assegurarem que os certificados que emitem são seguros e fiáveis.

A credibilidade destas é conferida pela segurança que utilizam nos seus procedimentos conexos com os serviços que prestam. São eles que garantem o cumprimento do dever de resultado a que nos referimos anteriormente. Por outro lado, para que exista essa credibilidade, é necessário que exista também transparência e para isso deve haver conhecimento, pelo mercado, do cumprimento efetivo dessas regras por essas entidades. Esse conhecimento gera-se e divulga-se mediante a realização de auditorias por outras entidades, que certificam o cumprimento dos requisitos de segurança das entidades auditadas.[725]

Nos casos em que a necessidade de segurança seja ainda mais efetiva, essas auditorias podem consistir em avaliações prévias ao cumprimento dos procedimentos de segurança e de qualidade que são necessários à prestação de determinados serviços, como é o caso, por exemplo, da emissão de pares de chaves e de certificados de assinatura eletrónica qualificada. É o que acontece no regime do Regulamento UE n.º 910/2014, de 23 de julho, para os prestadores qualificados (art.º 17.º a 24.º).

---

[724] Em Portugal foi criada uma entidade pública de certificação, destinada a facilitar a utilização da assinatura digital na administração pública, Trata-se do DL n.º 116-A/2006, de 16/6, a Entidade de Certificação Digital do Estado – Infra-estrutura de Chaves Públicas. A função principal desta Entidade é certificar outras entidades, principalmente da administração pública, mas também entidades privadas que se queiram instituir como entidades certificadoras para emitirem certificados. Uma das entidades públicas que emite certificados é o CEGER, como resultou da alteração ao n.º 2 do artigo 1.º do DL n.º 184/98, de 6/7, introduzida pelo DL n.º 116-B/2006, de 16/6.

[725] Obrigação importante destas entidades é também a publicação dos resultados das normas técnicas relativas aos procedimentos de geração de dispositivos de assinatura utilizados. Nesse sentido, Ubao, L.G.E. (2003). La Firma Electrónica. Em: Ros, R.M. e Gallego, M.L.M., *Derecho de Internet - La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.* Thomson, Aranzadi, Navarra., pág. 637.

Falta-nos agora analisar por que razão esses destinatários deverão confiar nas declarações dessas entidades. A confiança é um bem jurídico que se forma a partir da convicção dos utilizadores mediante a constatação de um conjunto de factos e de comportamentos.[726] Ora, a questão que se coloca é a de saber como os utilizadores do sistema de assinaturas eletrónicas podem, eles próprios, formar e consolidar essa convicção de segurança.

É essa uma das mais importantes funções das PKI. As entidades que prestam serviços de confiança nas assinaturas eletrónicas estão organizadas por níveis hierárquicos de confiança que garantem a solidez do sistema. Além das entidades que prestam serviços de geração e fornecimento de dispositivos de assinatura eletrónica, existem também outras entidades que prestam serviços a estas, de auditoria e de certificação da qualidade das práticas e dos procedimentos que estas adotam nos serviços que prestam.

O destinatário de um documento eletrónico pode adquirir a confiança referida, verificando quem foi o prestador de serviços que emitiu o certificado de assinatura eletrónica que consta do documento que recebeu. Conhecedor da chave pública dessa entidade, pode verificar, por sua vez, quem foi a entidade de segundo nível que emitiu o certificado de assinatura eletrónica dessa entidade, e assim sucessivamente, adquirindo a confiança consolidada por uma cadeia de níveis de entidades certificadoras, cuja função é, como vimos referindo, gerar confiança.[727] É este o sistema de geração de confiança de uma PKI, garantindo a solidez do sistema de geração de confiança de todos os agentes que emitem ou recebem documentos eletrónicos assinados.

Em síntese, podemos concluir que a função das PKI é oferecer garantia de confiança nos três domínios principais, da credibilidade do prestador de serviços e da sua classificação, da segurança do procedimento de identificação do signatário ou titular da assinatura e da segurança de geração do instrumento de criação de assinaturas:[728]

---

[726] Como se refere na Resolução do Parlamento Europeu a confiança é um bem jurídico fundamental para o desenvolvimento do comércio eletrónico. *"para que o comércio electrónico continue a desenvolver-se, é necessário despertar a confiança cada vez maior entre os utilizadores e fixar normas no que respeita, nomeadamente, à fiabilidade jurídica da identificação, da validade dos contratos, da integridade e da comunicação"*. (COM(97)0503 C4-0648/97), par. 12.

[727] *"The issuing certification authority's digital signature on the certificate can be verified by using the public key of the certification authority listed in another certificate by another certification authority (which may but need not be on a higher level in a hierarchy), and that other certificate can in turn be authenticated by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness"*. "A/CN.9/WG.IV/WP.71", par. 37.

[728] Seguimos a enunciação constante do documento "A/CN.9/WG.IV/WP.88", par. 50.

As garantias de confiança anteriormente referidas resultam dos serviços prestados pelos prestadores de serviços de confiança, mas também das declarações de boas práticas dessas entidades e das suas obrigações de disponibilizarem a todos os interessados informação acerca do cumprimento das obrigações de transparência na prática desses serviços.

Essas garantias são também asseguradas pela cadeia de certificações a montante, em que entidades de segundo nível, ou mais elevado, prestam serviços de auditoria e de certificação da segurança dos procedimentos utilizados por outras entidades nos serviços que prestam.

A conformação de uma PKI resulta do regime jurídico estabelecido em cada legislação nacional, mas o que é mais comum é que exista uma hierarquia de certificação, em que umas entidades certificam a assinatura eletrónica de utilizadores finais, e num segundo nível existam outras entidades que certificam a qualidade e a segurança dos procedimentos que estas têm instituído.

Cada PKI pode ter várias entidades certificadoras e também várias entidades de segundo nível, de terceiro nível e assim sucessivamente, sendo que a lei definirá os privilégios que terão os diversos utilizadores de um sistema.[729]

1.2.1. Organização das PKI

Os vários prestadores de serviços de confiança existentes numa PKI podem estar organizados de forma horizontal ou vertical.

Sendo a organização vertical ou hierárquica, existem normalmente três níveis. No meio estão as entidades que melhor conhecemos, que são aquelas que emitem certificados e pares de chaves a utilizadores finais.[730]

---

[729] *"Which users will have which privileges on the system"*. "A/CN.9/WG.IV/WP.88", par. 50.

[730] A organização vertical de uma PKI é descrita pela UNCITRAL do seguinte modo: *"A public key infrastructure (PKI) is often based on various hierarchical levels of authority". "(1) a unique "root authority", which would certify the technology and practices of all parties authorized to issue cryptographic key pairs or certificates in connection with the use of such key pairs, and would register subordinate certification authorities; (2) various certification authorities, placed below the "root" authority, which would certify that a user's public key actually corresponds to that user's private key (i.e., has not been tampered with); and (3) various local registration authorities, placed below the certification authorities, and receiving requests from users for cryptographic key pairs or for certificates in connection with the use of such key pairs, requiring proof of identification and checking identities of potential users"*. "A/CN.9/WG.IV/WP.88", par. 51.

Acima destas estão entidades que certificam a segurança, o rigor e a qualidade dos serviços que aquelas prestam, bem como a qualidade e a sofisticação dos equipamentos que utilizam e dos recursos humanos que com elas trabalham. Podem existir entidades certificadoras que se dedicam exclusivamente a emitir certificados e pares de chaves a outros prestadores de serviços de confiança e outras que se dediquem exclusivamente a auditar e a certificar as práticas de segurança de outras entidades certificadoras. Neste caso poderemos considerar estas entidades como estando num nível hierárquico superior àquelas que emitem os certificados. Nos documentos iniciais da UNCITRAL estas entidades designavam-se autoridades de certificação, mas essa designação caiu em desuso para não inculcar a ideia de que se trataria de entidades públicas dotadas de poderes de autoridade, uma vez que o exercício das suas funções pode também ser desenvolvido por entidades privadas em regime de livre concorrência.

Por debaixo das entidades que prestam serviços de confiança a utilizadores finais podem existir as chamadas entidades de registo. Trata-se, então, de entidades de terceiro nível. Estas entidades exercem funções de proximidade com os titulares das assinaturas eletrónicas, nomeadamente recebendo deles os pedidos de emissão de pares de chaves que depois estas entidades encaminham para as entidades certificadoras que as irão emitir. Estas entidades procedem à identificação das pessoas que requerem a emissão de pares de chaves e entregam os dispositivos de assinatura depois de serem gerados pelas entidades certificadoras. A função das entidades de registo é, deste modo, auxiliar e dependente das entidades que emitem os certificados a utilizadores finais, justificando-se a sua existência pela maior proximidade com os titulares de assinaturas eletrónicas.

A organização hierárquica de uma PKI tem a vantagem de constituir um mecanismo conhecido e simples de consolidação de confiança, mas tem também a desvantagem de, em caso de rotura da confiança na entidade mais elevada da hierarquia, colocar em causa toda a cadeia de confiança das entidades que prestam serviços de certificação.[731]

A organização de uma PKI pode não ser hierarquizada, apesar de se poderem manter os procedimentos de segundo nível, consistentes na função de certificação dos procedimentos, dos equipamentos e dos recursos humanos das entidades que prestam

[731] *"However, hierarchical PKIs have drawbacks as well, mainly as a consequence of reliance on a single trust point. If the root authority is compromised, the entire PKI is compromised"*. "A/CN.9/630/Add.1", par. 16.

serviços a utilizadores finais. Nesse caso essas funções são desempenhadas de forma cruzada, entre entidades que se situam no mesmo plano e que são simultaneamente entidades que emitem pares de chaves de assinatura eletrónica e respetivos certificados, e também auditam e certificam os procedimentos de segurança e de qualidade de outras entidades.

Uma entidade certificadora pode emitir pares de chaves e certificados a outra entidade certificadora e simultaneamente a qualquer outra pessoa, bem como certificar os procedimentos daquelas.

A organização das PKI é uma opção de política legislativa, sendo que teoricamente é concebível que uma entidade emita os seus próprios certificados e pares de chaves, desde que cumpra os requisitos que a lei estabelecer. Do mesmo modo, nas relações contratuais entre empresas é admissível que sejam convencionados regimes específicos de autenticação, podendo uma das partes emitir certificados e pares de chaves que ambas usam nas comunicações que entre elas estabelecerem. É possível, também, que ambas procedam dessa forma e uma efetue a certificação dos procedimentos da outra.[732]

A conformação dos modelos de PKI a adotar depende das opções de política legislativa, nomeadamente a quantidade de níveis hierárquicos, a possibilidade de existir auto certificação e certificação cruzada, a possibilidade de existirem entidades que emitem certificados de assinatura eletrónica com mais elevado grau de segurança, nomeadamente os certificados de assinatura eletrónica qualificada, bem como a possibilidade de existir uma entidade de base, de natureza pública que efetue a certificação de outras entidades certificadoras, etc. Todas estas possibilidades ficaram em aberto e se enquadram na LMAE.[733]

1.2.2. PKI e Estado

A participação do Estado ou de outras entidades públicas nas PKI é um tema sempre presente, dado o relevo que o bem jurídico confiança tem para a atividade

[732] Esta possibilidade é reportada pela UNCITRAL:*"In digital signature practice, parties relied increasingly on self-certification (or mutual-certification) schemes, involving only the originators and addressees of digitally-signed messages. Accordingly, the definition of "certification authority" should be broadened to cover all types of practices"*. "A/CN.9/446", par. 108.

[733] *"The organization of a PKI may involve various technical issues, as well as issues of public policy that may better be left to each individual State at the current stage"*. "A/CN.9/WG.IV/WP.88", par. 52.

económica em geral, bem como para todos os cidadãos, ao ponto de se poder considerar esse como um bem de natureza pública. Esse interesse é de natureza geral e beneficia toda a economia e a sociedade. [734]

No paradigma do papel e das assinaturas manuais, o desempenho dessas funções é considerado de natureza pública, sendo que muitas vezes elas são inclusivamente desempenhadas diretamente por entidades públicas. É o caso das entidades que emitem os documentos de identificação, bem como dos notários.

Esta origem pública das funções de autenticação das assinaturas e da identidade, projetou-se também no domínio das assinaturas eletrónicas, e logo nos documentos de trabalho iniciais da UNCITRAL esteve presente a possibilidade de o Estado ou outras entidades de natureza pública pudessem participar nas PKI.

Essa participação foi inicialmente considerada um importante instrumento de conferir maiores garantias e níveis de confiança aos agentes económicos e aos cidadãos nos sistemas de assinatura eletrónica.[735] Pelo seu peso, pelo seu poder de autoridade e também pela sua solvabilidade, o Estado poderia, mesmo que em última instância, ser o garante do sistema em que assenta a confiança nas assinaturas eletrónicas e, por isso, no comércio eletrónico. É por essa razão que inicialmente se designavam de "autoridades" de certificação, àquelas entidades de segundo nível que emitiam certificados aos prestadores de serviços de confiança, que certificavam os seus programas e procedimentos e que os auditavam.

Esta tendência inicial de apelar à participação do Estado no funcionamento das PKI compreendia-se, também, em face do crescimento da utilização dos meios

---

[734] Para além das razões políticas e económicas, a não intervenção do Estado nas redes eletrónicas era também uma espécie de militância assumida pelos primeiros utilizadores, tendo ficado célebre o manifesto de John Perry Barlow, "Declaração de Independência do Ciberespaço", uma espécie de novo mundo virtual e alheio à soberania do Estado. Pelo contrário, defendendo a regulação jurídica da Internet, Goldsmith, J. (1997). *Against Cyberanarchy*. Acedido a 20 de maio de 2014 em: http://groups.csail.mit.edu/mac/classes/6.805/articles/goldsmith-against-cyberanarchy.html. Do mesmo modo, Mas o Estado, que esteve na génese da criação da Internet, haveria de regressar à rede nos mais variados domínios. Barlow, J.P. (1996, February 8). *A Declaration of the Independence of Cyberspace*. Acedido a 11 de maio 2016, em: https://www.eff.org/cyberspace-independence. Como afirmam Birnhack e Elkin-Koren, *"In recente years the State has become more active in the digital environment"*, e mais adiante, *"The State, now re-entering the digital field …"*. Birnhack, M.D. e Elkin-Koren, N. (Summer 2003). The Invisible Handshake: The Reemergence of the State in the Digital Environment. Virginia Journal of Law and Technology. University of Virginia. Acedido a 11/5/2016, em: http://www.vjolt.net/vol8/issue2/v8i2_a06-Birnhack-Elkin-Koren.pdf.par.s 35 e 115, respetivamente.

[735] *"In a number of countries, it is envisaged that, for public policy reasons, only Government entities should be authorized to operate as certification authorities. In other countries, it is considered that certification services should be open to competition from the private sector"*. "A/CN.9/WG.IV/WP.71", par. 41.

eletrónicos e da necessidade de conferir rapidamente segurança jurídica aos agentes económicos na utilização desses meios.

A questão da credenciação prévia, por órgãos da administração pública, do cumprimento pelas entidades certificadoras, dos requisitos de fiabilidade e de segurança na emissão de pares de chaves e de certificados de assinatura eletrónica, era defendida como particularmente importante no que respeita às assinaturas eletrónicas qualificadas. Defendia-se mesmo que a emissão desse tipo de certificados deveria depender de um licenciamento prévio por um órgão da administração pública, das entidades que estavam em condições de emitir esses tipos de certificados de assinatura eletrónica.[736]

Ao longo dos trabalhos de conceção da LMAE, ocorreu uma evolução no sentido de se considerar que a atividade de certificação, quer ela fosse de primeiro ou de segundo nível, deveria poder ser desenvolvida em regime de livre concorrência.[737] Considerou-se que a intervenção do Estado e de entidades públicas envolvia um risco de burocratização do sistema, com impacto negativo adicional no reconhecimento internacional das assinaturas eletrónicas.[738]

Especialmente em razão da tradição liberal anglo-saxónica defendia-se que o exercício das atividades de certificação, também por entidades privadas em regime de livre acesso e livre concorrência seria o que melhor garantiria a eficiência e a rápida expansão do exercício dessas atividades, bem como da utilização das assinaturas eletrónicas.

Por outro lado, a opção pela consagração da liberdade de exercício da atividade de certificação e pela desnecessidade da dependência de uma autoridade credenciadora central do Estado, resulta também das necessidades da atividade económica no plano internacional. A dimensão global das transações eletrónicas poderia ser dificultada se ocorresse uma segmentação dos sistemas de certificação em função da geografia dos

---

[736] Esta certificação prévia, por uma autoridade administrativa, das entidades certificadoras que podiam emitir pares de chaves e certificados de assinatura eletrónica qualificada, seria uma importante garantia de segurança do sistema e de confiança dos agentes económicos. *"In the case of governmentallyauthorized certification authorities, the fulfilment of the applicable operation criteria by a certification authority would constitute a prerequisite for the authorization of that certification"*. "A/CN.9/437", par. 48.

[737] Nos documentos que reportam os trabalhos preparatórios da LMAE, encontram-se várias referências a esta matéria, como por exemplo a seguinte: *"It was also stated that the establishment of a public law scheme under which certification authorities might be authorized to operate would not necessarily foster the trustworthiness of digital signatures, which might be better achieved through privately-appointed certification authorities, or other forms of market-driven mechanisms"*. "A/CN.9/437", par. 40.

[738] *"Doubts were expressed as to the role of the State in making the determinations referred to in paragraph (1). One view was that any organ or authority set up to assess technical reliability of signature techniques should be industry-based. Another view was that the draft article should not focus on the question of who or what might be authorised to make the determination, but rather on the matters to be considered if any determination was to be made"*. "A/CN.9/465", par. 94.

estados. Pelo contrário, a possibilidade de existirem PKI com entidades certificadoras de vários níveis que pudessem operar em vários países em simultâneo, seria sempre um fator que facilitaria o reconhecimento transnacional dos certificados e das assinaturas eletrónicas, bem como a circulação dos documentos e a segurança das transações internacionais. Essa possibilidade não era incompatível com a participação de entidades públicas nas PKI.[739] Do mesmo modo, estas possibilidades também não impediam que os estados pudessem formar uma PKI própria, que operasse em regime de concorrência com as privadas.[740] Foi esse o entendimento que prevaleceu na elaboração da LMAE e que está na base da redação do seu art.º 7.º.

A possibilidade de as entidades certificadoras de segundo nível serem privadas aplica-se também à certificação das assinaturas eletrónicas qualificadas, uma vez que se trata de certificar previamente o cumprimento de um conjunto mais específico de requisitos de fiabilidade e de segurança.[741] Foi essa também a opção que prevaleceu na redação final do art.º 7.º da LMAE.[742] Por essa razão a LMAE não utiliza o conceito de *"autoridade"* certificadora que vinha sendo utilizado nos trabalhos preparatórios, e que foi abandonado e substituído pelo de entidade certificadora, para evitar que viesse essa

---

[739] *"Certification authorities could be operated by Government authorities or by private sector service providers"*. "A/CN.9/WG.IV/WP.88", par. 58.

[740] Essa designação de "autoridades de certificação" foi abandonada nos trabalhos da LMAE, por se considerar que poderia não ser a mais rigorosa, dado que a atividade dessas entidades não tem que ser necessariamente de natureza pública, podendo também ser exercida por entidades privadas em regime de livre concorrência, sem prejuízo de o Estado possuir também a sua PKI. *"Certification authorities can conceivably be operated by Government authorities or by private sector service providers"*. "A/CN.9/WG.IV/WP.71", par. 41.

[741] Nas notas ao artigo 7.º da LMAE, reconhece-se o papel do Estado em definir um organismo público, ou então uma entidade privada reconhecida pelo Estado para certificar entidades que emitem certificados de assinatura eletrónica. *"The role played by the enacting State in establishing or recognizing any entity that might validate the use of electronic signatures or otherwise certify their quality"*. "A/CN.9/WG.IV/WP.88", par. 127.

[742] O artigo 7.º da LMAE admite, especificamente, no que respeita ao reconhecimento das entidades que emitem certificados de assinatura eletrónica qualificada, sejam entidades públicas ou privadas. Essa possibilidade é confirmada nos seguintes termos: *"Paragraph (1) makes it clear that any entity that might validate the use of electronic signatures or otherwise certify their quality would not always have to be established as a State authority"*. "A/CN.9/WG.IV/WP.88", par. 129. Essa conclusão resultou do consenso no sentido de a adoção da opção pela dupla via, de permitir que a certificação prévia de entidades que pudessem emitir pares de chaves e certificados de assinatura eletrónica qualificada, pudesse ser feita quer por entidades públicas, quer por entidades privadas. *"It was widely felt that, given the far-reaching potential of a predetermination of [enhanced] electronic signature status, any declaration made under paragraph (1) should only be made by an organ or authority which was clearly in a position or authorized to make such a declaration, whether it be a public authority or a publicly-appointed private authority"*. "A/CN.9/454", par. 69. Do mesmo modo, *"Any entity that might validate the use of electronic signatures or otherwise certify their quality would not always have to be established as a State authority"*. "A/CN.9/WG.IV/WP.86/Add.1", par. 31.

atividade a ser confundida com própria de um órgão da administração pública.[743] Essa alteração tem, porém, a desvantagem de poder gerar confusão, porque não distingue entre as entidades certificadoras de primeiro e de segundo nível.

A LMAE permite que exista certificação prévia das entidades que cumprem os requisitos para a emissão de certificados de assinaturas eletrónicas qualificadas, mas em simultâneo permite também duas outras opções:

i) Que essa certificação possa ser efetuada por entidades privadas;

ii) Que as empresas que prestam serviços de confiança eletrónica, que pretendam iniciar a sua atividade e que cumpram os requisitos legais para a emissão de certificados de assinatura eletrónica qualificada o possam fazer sem necessidade de licenciamento prévio, sendo que nesse caso, em caso de litígio, o cumprimento dos requisitos legais terá que ser avaliado especificamente pelo tribunal competente.

Nas legislações nacionais, muitas das quais subsequentes à LMAE, a organização das PKI, no que respeita à participação do Estado organiza-se segundo três modelos distintos:[744]

1. – O modelo da autorregulamentação, de livre concorrência, onde não existe certificação pelo Estado. A certificação de segundo nível cabe às entidades privadas que operam no mercado da certificação. Os sistemas de certificação de segundo nível dependem da adesão voluntária dos prestadores de serviços de certificação e são, em si mesmos, uma forma de prestação de serviços de confiança. Este modelo não impede, porém, que o Estado ou outras entidades públicas estabeleçam as suas próprias entidades com competências de prestação de serviços de certificação, que podem prestar serviços a outros organismos públicos;[745]

[743] Essa ideia foi sugerida nos trabalhos preparatórios da LMAE em 1997: *"The Working Group might give consideration to the possibility of replacing the notion of "certification authority" by that of "certification entity", to avoid the possible implication that functions of certification were necessarily performed by public authorities"*. "A/CN.9/437", par. 90. Do mesmo modo, foi retirado do projeto o conceito de entidades certificadoras licenciadas, para evitar a mesma associação dessa atividade a qualquer exercício de poder de autoridade de uma entidade administrativa, salvaguardando-se o princípio da liberdade do exercício de atividade. *"Any reference to "licensed certification authorities" in the Uniform Rules might be interpreted as encouraging enacting States to establish licensing schemes"*. "A/CN.9/446", par. 110.

[744] Por nos parecer adequado, seguimos aqui o esquema utilizado pela UNCITRAL. "A/CN.9/630/Add.2", par. 15.

[745] São citados como exemplo o modelo dos EUA. "A/CN.9/630/Add.2", nota de rodapé 18.

2. – O modelo da intervenção pública limitada, em que o Estado institui uma entidade certificadora de segundo nível, com a função de certificar os procedimentos e os sistemas de outros prestadores de serviços, públicos ou privados, nomeadamente nos casos em que estes pretendam emitir certificados de assinatura eletrónica qualificada. Não se trata, porém, de uma entidade com competência exclusiva em matéria de certificação de procedimentos, podendo essas funções ser também desenvolvidas por outras entidades;[746]
3. – O modelo de processo dirigido pelo Estado, em que é instituída uma autoridade central de certificação, com poderes exclusivos. Este modelo admite também que o Estado possa concessionar a terceiros o exercício dessas funções, mas trata-se sempre de uma função que é assumida como administrativa e assente na autoridade pública.[747]

Em Portugal, o Decreto-Lei n.º 290-D/99, de 2 de Agosto, estabeleceu um regime de livre acesso à atividade de prestação de serviços, associado a um regime voluntário de credenciação por essas entidades.[748] Essa credenciação, por sua vez, era de natureza pública, estabelecendo a lei que a designação da entidade credenciadora seria efetuada em diploma autónomo (art.º 40.º), o que viria a ocorrer logo no ano seguinte, com a designação do Instituto das Tecnologias de Informação da Justiça (ITIJ) como entidade credenciadora.[749] Apesar disso tratava-se de um regime de credenciação voluntária e facultativa, que não fazia depender de autorização prévia o exercício da atividade.[750]

[746] Cita-se como exemplo deste modelo a legislação de Singapura. "A/CN.9/630/Add.2", nota de rodapé 19.
[747] Exemplo deste modelo é a legislação da China e da Malásia. "A/CN.9/630/Add.2", nota de rodapé 20.
[748] Esse regime estava previsto no artigo 10.º do diploma, sob o título *"Livre escolha da entidade certificadora"*. O regime mantém-se ainda hoje em vigor, com as alterações introduzidas pelo DL n.º 88/2009, de 9/4.
[749] Alínea i) do n.º 3 do artigo 18.º do DL n.º 146/2000, de 18/7 (Lei Orgânica do Ministério da Justiça). A regulamentação da atividade de credenciação consta do Decreto regulamentar n.º 25/2004, de 15/7. A entidade credenciadora é, atualmente, é a Autoridade Nacional de Segurança (artigo 8.º do pelo DL n.º 88/2009, de 9/4).
[750] No mesmo sentido Pupo Correia, Correia, M. P. (1999). Assinatura Electrónica e Certificação Digital. http://www.apdi.pt/wp-content/uploads/2016/10/8-ARTIGO_ASSINATURA_ELETRONICA_CERTIFICACAO_DIGITAL.pdf, pag. 28.

Também a lei espanhola de 1999, estabelecia um regime de livre acesso à atividade de certificação, em simultâneo com um regime de credenciação voluntária. [751] Este regime manteve-se, na sua essência, no regime de 2003.

O modelo alemão, consignado na lei da assinatura eletrónica de 1997, anterior, portanto, à Diretiva 1999/93/CE e quase contemporâneo da LMAE, rompe com a doutrina dominante nos países ocidentais e adota o modelo do processo dirigido pelo Estado. Estabelece um regime público de controlo do sistema de segurança eletrónica, fazendo depender de uma entidade administrativa a concessão de licenças de autorização do exercício da atividade pelos prestadores de serviços de certificação (§ 3.º).[752]

A Diretiva 1999/93/CE reverteria aquele princípio da lei alemã e assenta também, no princípio da não intervenção do Estado nas atividades de prestação de serviços de certificação e num princípio de voluntariedade da acreditação dos prestadores de serviços.[753] A diretiva não prevê qualquer tipo de intervenção pública no funcionamento das PKI, apesar de também não impedir os Estados Membros de as constituírem, sendo certo que não se estabelece qualquer tipo de supervisão pública do sistema. No contexto em que foi elaborada a diretiva, teve preponderância a necessidade de se expandir o mercado e de facilitar o acesso à atividade como forma de o conseguir, dado o relevante papel que as entidades certificadoras têm na promoção da confiança nas assinaturas eletrónicas. Nesta fase, esta primeira diretiva adotou este princípio aberto.[754]

---

[751] O Real Decreto Ley 14/1999, de 17/9, estabelecia no artigo 4.º o princípio do livre acesso á atividade de certificação. O artigo 6.º previa, porém, que dentro desse princípio, o governo pudesse estabelecer regimes voluntários de credenciação. Este regime de livre acesso e de credenciação facultativa manteve-se na *"Ley 59/2003, de 19 de diciembre, de firma electrónica"*. Em simultâneo era estabelecido diretamente na lei, e sem dependência da iniciativa do governo, um regime de credenciação facultativa no artigo 26.º, cujo n.º 1 estabelecia que: *"La certificación de un prestador de servicios de certificación es el procedimiento voluntario por el que una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público"*.

[752] Essa entidade seria a *"regulatory authority for telecommunications and posts"*, dependente do governo federal (§ 66 da Telekommunikationsgesetz, TKG). Versão em inglês disponível em http://germanlawarchive.iuscomp.org/?s=telecommunications+act&submit=#66 (última consulta efetuada em 28/1/2016).

[753] Essa opção vem refletida no ponto 11 do preâmbulo da diretiva no seguinte trecho: *"os prestadores de serviços de certificação devem ter a liberdade de aderir a estes regimes de acreditação e deles beneficiar"*.

[754] Com se refere nas considerações prévias à Proposta de Diretiva das Assinaturas Eletrónicas, de 13.05.1998, *"... devem evitar-se regimes de autorização prévia. Para ganhar a confiança dos consumidores, consideram-se úteis os sistemas de acreditação facultativa que visam proporcionar níveis mais elevados de segurança"*. COM(1998) 297 final.

A Diretiva viria a consagrar esse regime de livre acesso, prevendo também a possibilidade de os prestadores de serviços recorrerem a *"sistemas voluntários de acreditação"* (n.º 2 do art.º 3.º), tendo em vista, dessa forma, incrementar a confiança dos agentes económicos nas assinaturas eletrónicas.

Mas a Diretiva 1999/93/CE deixa também em aberto a possibilidade de os Estados Membros adotarem sistemas de *"supervisão dos prestadores de serviços de certificação estabelecidos no seu território"* que emitam certificados reconhecidos (n.º 3 do art.º 3.º). Esta norma vai um pouco mais longe do que a mera previsão dessa possibilidade, uma vez que o que ela estabelece é que os Estados Membros assegurarão a instituição de mecanismos de controlo e de supervisão desses prestadores de serviços. Esta norma da diretiva foi além do projeto, que não previa a criação destes organismos, tendo sido sugerida a sua introdução pela Resolução do Parlamento Europeu, de 21/9/1998, com fundamento na necessidade de reforço da confiança dos agentes económicos nas transações eletrónicas.[755]

A diretiva estabelece também um regime de controlo, mediante organismos de acreditação que podem ser públicos ou privados, com a incumbência de controlo dos prestadores de serviços que emitem certificados qualificados de assinatura eletrónica (n.º 4 do art.º 3.º). Obriga também os estados a notificarem a Comissão da criação desses organismos e da sua identidade, bem como a identificação de todos os prestadores de serviços localizados no respetivo território (n.º 1 do art.º 11.º).[756] Ao mesmo tempo a diretiva criou o Comité da Assinatura Eletrónica, composto por representantes dos Estados Membros e presidido pelo representante da Comissão, com competências de controlo da emissão dos certificados seguros ou qualificados (art.ºs 9.º e 10.º).

1.2.3. A supervisão e acreditação públicas. O regime da União Europeia

[755] Na parte final do par. 18 da Resolução estabelecia-se que *"seria oportuno que, em cada Estado-Membro, haja, pelo menos, uma autoridade de certificação que controle de forma objectiva, não discriminatória e transparente o respeito dessas normas, dado que isso reforçaria a confiança no mercado e seria benéfico para a criação de um clima favorável de investimentos internacionais"*. (COM(97) 0503 C4-0648/97).

[756] As normas com as especificações técnicas para a notificação com as listas de prestadores de serviços acreditados só seriam publicadas em 2009, através da Decisão da Comissão de 16/10/2009. *"Commission Decision of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (notified under document C(2009) 7806)"*; (Text with EEA relevance), (2009/767/EC), Official Journal of the European Union, 20.10.2009.

A opção pela não intervenção pública não se revelou tão frutuosa como o esperado no seio da UE. Vários relatórios referem que a fragmentação do mercado das assinaturas eletrónicas nos diversos Estados Membros é um importante entrave à expansão comércio eletrónico em geral, no espaço da UE.[757] Em 2012 é defendida, pela primeira vez, a criação de um sistema de supervisão à escala europeia, com uma intervenção dos próprios órgãos da União.[758] Apontam-se dois modelos de supervisão, sendo o primeiro o da criação de um sistema europeu de supervisão, com poderes diretos sobre os operadores, e o segundo o estabelecimento de um sistema de supervisão de segunda linha, que operaria sobre os sistemas nacionais de supervisão de cada estado.[759]

Dois anos depois, o Regulamento EIDAS viria estabelecer um regime de carácter público, de supervisão dos sistemas de assinatura eletrónica.[760]

O Regulamento veio criar o novo regime europeu das assinaturas eletrónicas, substituindo o da diretiva de 1999, e assume que um dos seus mais importantes objetivos é o da eliminação da fragmentação das assinaturas eletrónicas, criando as condições para a sua interoperabilidade plena no espaço europeu.[761] Assume também que essa interoperabilidade é de tal forma importante que a sua prossecução justifica a adoção de normas imperativas nesta matéria, que se imponham aos Estados Membros.[762]

---

[757] É relevante esse reconhecimento, como fundamento da proposta de criação de um sistema de identificação eletrónica à escala da UE: *"There is no specific framework for mutual recognition and acceptance of elD or for ancillary trust services such as time-stamping or eseals"*. SWD(2012) 136 final.

[758] A proposta da CE para o sistema de identificação eletrónica europeia, ia no sentido da criação de um sistema de supervisão, com várias alternativas, todas elas tendentes a eliminar a fragmentação do mercado europeu das assinaturas eletrónicas. *"A harmonized approach at EU-level for both e-signature and ancillary trust services would improve effective supervision, enhance legal certainty and augment the trust and security of e-transactions"*. SWD(2012) 136 final, ponto 6.3.

[759] A necessidade da acreditação pública é mais aceite no direito continental dos que nos países de tradição anglo-saxónica, cuja influência na UNCITRAL era relevante. Roques-Bonnet refere essa intervenção pública como uma necessidade pacífica: *"Pour qu'une signature électronique soit certifiée, c'est à dire présumée fiable, les pouvoirs publics interviennent em amont du marche de la certification"*. Roques-Bonnet, M.C. (2010). Op. Cit., pag. 379.

[760] Regulamento EIDAS.

[761] Como se refere no ponto 12 do preâmbulo do Regulamento, *"Um dos objetivos do presente regulamento é eliminar os obstáculos existentes à utilização transnacional dos meios de identificação eletrónica utilizados nos Estados-Membros para a autenticação para, pelo menos, os serviços públicos"*.

[762] Essa imperatividade vem justificada no n.º 14 do preâmbulo do Regulamento nos seguintes termos: *"Há que estabelecer no regulamento algumas condições respeitantes aos meios de identificação eletrónica que têm imperativamente de ser reconhecidos e ao modo como os sistemas de identificação eletrónica deverão ser notificados"*. Regulamento EIDAS.

O regime de supervisão instituído pelo Regulamento centra as competências executivas de supervisão nos Estados Membros, assumindo o carácter administrativo e público desta atividade, quando se trate de emissão de certificados qualificados.[763]

Em simultâneo atribui poderes efetivos à CE, nomeadamente em matéria de troca de informação, de controlo, mas também poderes executivos.

A supervisão europeia assenta nos poderes de supervisão pública dos Estados Membros, que devem instituir essas entidades no seio da sua administração, com funções que correspondem à prestação de serviços do mais alto nível de hierarquia de segurança do sistema. Essas entidades têm poderes sobre todos os prestadores de serviços de certificação, incluindo os qualificados e os não qualificados.

Relativamente aos prestadores qualificados de serviços de confiança, releva a importância dos poderes de atribuir e de retirar o estatuto de prestador qualificado de serviços qualificados, de realização de auditorias e inspeções, de determinação de procedimentos de correção de situações de incumprimentos de normas de segurança, bem como outros poderes previstos no n.º 4 do 17.º do Regulamento. O poder de reconhecimento prévio do estatuto de prestador qualificado de serviços de confiança, associado aos poderes de inspeção e de correção de incumprimentos e de recusa de reconhecimento são uma garantia eficaz de segurança e de confiança dos agentes económicos na utilização das assinaturas eletrónicas, mas também de garantia de interoperabilidade, dados os poderes de controlo e inspeção das entidades de supervisão, desde o acesso ao mercado dos prestadores qualificados, até ao seu desempenho e cessação.

Relativamente aos prestadores não qualificados, as entidades de supervisão possuem poderes mais limitados, mas mesmo assim importantes, nomeadamente o poder de supervisão *a posteriori* (alínea b) do n.º 3 do artigo 17.º) e de determinar a tomada de medidas corretivas (alínea f) do n.º 4 do artigo 17.º). Relativamente a estes prestadores de serviços as entidades supervisoras não possuem poderes de lhes retirar o direito de exercício de atividade, tal como acontece com os prestadores qualificados, que podem perder esse estatuto por decisão das entidades de supervisão. Porém, podem estas entidades, em face da constatação de situações de violação de segurança ou de

[763] Este regime, destinado a conferir uma maior confiança à utilização dos suportes eletrónicos, não se pode confundir com um sistema de limitação de acesso à atividade de prestação deste tipo de serviços. Na verdade esse acesso continua a ser livre, mas quando se trate da prestação de serviços qualificados, são estabelecidos requisitos adicionais. No mesmo sentido Nadal, A.G. (2009). Op. cit, pag. 513 e 514.

perda de integridade, informar publicamente, por si mesma, ou através do prestador de serviços, da respetiva perda de confiança (parte final do n.º 3 do artigo 19.º).

A fim de garantir a efetividade dessa obrigação, obrigam-se os Estados Membros a notificar a Comissão da identificação da entidade de supervisão que designam. As funções destas entidades correspondem à prestação de serviços de alto nível de hierarquia de segurança do sistema. Os seus poderes incidem sobre todos os prestadores de serviços, incluindo os qualificados e os não qualificados, e consistem, nomeadamente, nas seguintes competências:[764]

i) Atribuir o estatuto de prestador de serviços qualificados. Essa atribuição depende de reconhecimento prévio das entidades de supervisão, mediante ato administrativo, sempre a pedido do prestador de serviços que o pretenda. Esta medida é uma das mais importantes inovações do Regulamento e representa uma rotura com o modelo tradicional da liberdade de acesso à prestação de serviços que vinha da LMAE e da tradição da maioria das legislações até então vigentes, bem como da própria Diretiva 1999/93/CE (alínea g) do n.º 4 do art.º 17.º do Regulamento). Ao mesmo tempo este regime confere um nível de confiança mais elevado aos agentes económicos, porque passam a conhecer *a priori* a eficácia das assinaturas qualificadas, quando as utilizam;

ii) Realizar auditorias aos prestadores de serviços, quer aos qualificados quer aos restantes, podendo essas auditorias ser efetuadas diretamente ou através de outros organismos de avaliação de conformidade previamente acreditados para o exercício dessas funções (alínea e) do n.º 4 do art.º 17.º);

iii) Analisar os relatórios de auditoria a que os prestadores de serviços qualificados se devem submeter obrigatoriamente de 24 em 24 meses (alínea b) do n.º 4 do art.º 17.º);

iv) Retirar o estatuto de qualificado aos prestadores de serviços, sempre que constate que estes não cumprem os requisitos correspondentes. Também a atribuição deste poder tem carácter inovador e representa

[764] Seguimos em especial, as normas constantes do artigo 17.º do Regulamento EIDAS.

uma transposição para a esfera administrativa das funções de garantia da qualidade e efetividade (alínea g) do n.º 4 do art.º 17.º);

v) Exigir aos prestadores de serviços de certificação que corrijam eventuais incumprimentos de normas de segurança previstas no Regulamento (alínea j) do n.º 4 do art.º 17.º);

vi) Prestar assistência mútua a outras entidades de supervisão, que podem incluir prestação de serviços de informação e ainda atividades de inspeção direta a prestadores de serviços de certificação (art.º 18.º);

vii) Informar as outras entidades de supervisão e o público das violações e das perdas de integridade que tenham sido notificadas pelos prestadores qualificados de serviços de certificação (alínea h) do n.º 4 do art.º 17.º).

Esta configuração legal das entidades de supervisão representa uma mudança de paradigma no sistema da assinatura eletrónica no espaço da UE. O bem jurídico confiança passa a ser tutelado como tendo carácter público, dado que a garantia da sua efetividade é assegurada em última instância por órgão da administração pública, que o regulamento institui e aos quais atribui poderes de autoridade pública.[765]

O carácter publicista do bem jurídico "*confiança nos serviços eletrónicos*" é ainda reforçado pelos poderes que o Regulamento atribui à própria Comissão Europeia, que passa a ser uma entidade com importantes poderes em matéria de assinaturas eletrónicas, nomeadamente os seguintes:

i) Determinar a forma e os procedimentos que devem ser adotados pelos prestadores de serviços de certificação que pretendam prestar serviços de certificação qualificados, incluindo o relatório de avaliação prévia e o requerimento de reconhecimento (n.º 4 do art.º 21.º)

[765] A relevância pública do bem jurídico consubstanciado na confiança, não se limita à confiança na utilização dos meios eletrónicos, mas, num sentido mais geral, à confiança dos agentes económicos. Tal como a fé pública se destina a aumentar a confiança dos agentes, e não especificamente na utilização do papel, também a confiança que é protegida pelo Regulamento EIDAS e pelas leis da assinatura eletrónica tem o mesmo objetivo. Como refere Gustavo Aboso, o bem jurídico protegido é a "*seguridade y confiança del processo probatório en el tráfego jurídico*". E também aqui "*el bien jurídico protegido es la fe pública, es decir, la confianza dispensada por lo general en la apariência de verdade representada por ciertos signos y que es necesaria para el tráfego jurídico*". Aboso, G. E. (2017). Derecho Penal Cibernético. La Cibernética y el Derecho Penal en la Moderna Sociedad de la Información y la Tecnologia de la Comunicación. Euros Editores, S. R. L. Buenos Aires, págs. 384 e 385. Do mesmo modo Benjamim da Silva Rodrigues, "o bem jurídico protegido é a segurança e a fiabilidade dos dados eletrónicos que podem ter consequências nas relações jurídicas (…). Trata-se de proteger a verdade intrínseca do documento (eletrónico) enquanto tal ou, segundo alguma doutrina, a segurança e credibilidade no tráfego jurídico probatório no que respeita à prova documental". Rodrigues, B. S. (2009). *Direito Penal Especial. Tomo I. Direito Penal Informático-Digital*. Coimbra Editora Limitada. Coimbra, pág. 346 e 347.

ii) Receber das entidades supervisoras nacionais relatórios anuais de atividades, que incluem o resumo das notificações de violações de segurança referidas no ponto vii) anterior, sendo esses relatórios elaborados em conformidade com um formato que a Comissão pode determinar (n.º 6 do art.º 17.º);

iii) Determinar os riscos de segurança que a evolução tecnológica pode colocar, nomeadamente quebras de segurança quanto à derivação das chaves privadas a partir das chaves públicas fixar aos prestadores de serviços, qualificados e não qualificados, as medidas a adotar. Este poder reforça o carácter publicístico dos serviços de confiança (alínea a) do n.º 4 do art.º 19.º);

iv) Determinar os procedimentos da obrigação de os prestadores de serviços de certificação informarem o público e as entidades de supervisão, das quebras de segurança referidas no ponto vii) anterior (alínea b) do n.º 4 do art.º 19.º);

v) Determinar as normas de referência para a acreditação dos organismos de avaliação de conformidade, que efetuam as auditorias aos prestadores qualificados de serviços de certificação (alínea a) do n.º 4 do art.º 20.º);

vi) Determinar as regras de auditoria que as entidades auditoras devem respeitar nas auditorias a realizar aos prestadores qualificados de serviços de certificação (alínea b) do n.º 4 do art.º 20.º). A eficácia desta regra alarga-se também às entidades supervisoras, que avaliam os respetivos relatórios de auditoria;

vii) A gestão e a adoção dos procedimentos de acesso à marca de confiança "UE" para os prestadores de serviços de certificação (n.º 3 do art.º 23.º);

viii) Determinar as normas e procedimentos que devem respeitar os sistemas e os produtos considerados fiáveis, que os prestadores de serviços utilizam na prestação de serviços qualificados (n.º 5 do art.º 24.º);

ix) Determinar os procedimentos de referência para as assinaturas eletrónicas avançadas utilizadas pelos órgãos das administrações públicas nos respetivos procedimentos, a fim de estas poderem gozar da presunção de conformidade (n.º 4 do art.º 27.º);

x) Determinar os procedimentos de referência para os certificados qualificados de assinatura eletrónica, que suportam a presunção de conformidade com os respetivos requisitos estabelecidos no anexo I do Regulamento (n.º 6 do art.º 28.º);

xi) Determinar as normas e procedimentos de referência para os dispositivos qualificados de assinatura eletrónica, que sustentam a presunção de conformidade com os respetivos requisitos estabelecidos no anexo II do Regulamento (n.º 2 do art.º 29.º), bem como os procedimentos de avaliação a que ficam submetidos esses dispositivos (parte final do n.º 3 do art.º 30.º);

xii) Determinar as normas e procedimentos de referência para a prestação dos serviços qualificados de validação, bem como de preservação das assinaturas eletrónicas qualificadas (n.º 3 do art.º 33.º e n.º 2 do art.º 34.º). Estes serviços de confiança que o Regulamento institui são importantes para a segurança dos documentos e das mensagens eletrónicas, bem como para a preservação e arquivo dos documentos eletrónicos autenticados;

xiii) A Comissão assume também importantes poderes de informação, nomeadamente no que respeita à elaboração das listas dos prestadores de serviços e à informação ao público dos respetivos incidentes (em especial n.º 4 do art.º 22.º, n.º 2 do art.º 30.º, n.º 3 do art.º 31.º).

O regime do Regulamento que estamos a analisar institui dois novos agentes nos sistemas de assinatura eletrónica, a CE e os Estados Membros, para além das entidades de supervisão. A Comissão adquire poderes que se aproximam de uma entidade reguladora, nomeadamente o poder de estabelecer normas de carácter regulamentar, que são designados de atos de execução, bem como poderes de informação e de controlo das atividades das entidades de supervisão dos Estados Membros.

Os poderes atribuídos às entidades de supervisão dos Estados Membros conferem-lhes funções de autoridades administrativas com competência para a salvaguarda da confiança nas assinaturas eletrónicas. A atribuição destes poderes à Comissão e aos estados, mudam o paradigma da disciplina das assinaturas eletrónicas, porque a segurança jurídica dos documentos e das comunicações eletrónicas passou a relevar como um bem de carácter publicístico sendo que essas entidades passam a ser,

em última instância, os garantes da confiança dos cidadãos e das empresas na utilização destes meios.

A subida destes direitos para a segurança do domínio público é um instrumento fundamental para que a sua utilização seja incrementada e para que se assegure o reconhecimento e a interoperabilidade dos sistemas de assinatura e de segurança jurídica eletrónica no espaço da UE.

Em Portugal, o acesso à atividade de prestação de serviços de certificação é livre e essa atividade funciona em regime concorrencial, mas a lei estabelece um regime de credenciação facultativa para as entidades que pretendam emitir certificados de mais elevado valor jurídico. Essa credenciação é efetuada pela Autoridade Nacional de Segurança, que foi instituída como entidade credenciadora pelo Decreto-Lei n.º 116-A/2006, de 16 de Junho, em especial pelo seu art.º 8.º. O Regulamento do Conselho Técnico de Credenciação seria depois aprovado e publicado.[766]

Com a entrada em vigor do Regulamento EIDAS, o acesso ao estatuto de prestador de serviços de confiança continua a ser voluntário, porque depende da iniciativa dos interessados. Porém, para que esses prestadores de serviços sejam classificados como qualificados, além dessa iniciativa é necessário um ato de reconhecimento expresso do Gabinete Nacional de Segurança.[767] Esse reconhecimento é deferido nos termos previstos ma alínea g) do n.º 4 do artigo 17.º e no artigo 21.º, ambos do Regulamento.

Os prestadores de serviços não qualificados podem prestar serviços de confiança livremente, sem necessidade de autorização das entidades de supervisão. Apesar disso, estão sujeitas às competências de supervisão *a posteriori* destas entidades, nos termos da alínea b) do n.º 2 do artigo 17.º do Regulamento. Essas competências não são, porém, permanentes nem de iniciativa espontânea daquelas entidades, dado que a sua intervenção depende da invocação de que os prestadores de serviços não estão a cumprir os requisitos do Regulamento. Esta competência das entidades de supervisão está em vigor desde 1 de julho de 2016 (n.º 2 do artigo 52.º).

O regime de reconhecimento prévio dos prestadores de serviços qualificados está em vigor em toda a União Europeia. Os prestadores de serviços que emitiam certificados qualificados nos termos do Decreto-Lei n.º 290-D/99, de 2/8, que não

[766] Publicado no Diário da República, 2.ª Série, n.º 22, de 31/1/2007.
[767] Alínea j) do n.º 2 do artigo 2.º do Decreto-Lei n.º 3/2012, de 16 de janeiro, que estabelece a respetiva lei orgânica. Este diploma deveria ter sido já alterado, para acolher as funções de entidade de supervisão.

tenham apresentado o relatório de avaliação de conformidade previsto no n.º 3 do artigo 51.º do Regulamente, perdem a classificação como qualificados a partir de 2 de julho de 2017. Caso apresentem esse relatório, a manutenção do estatuto de prestadores qualificados dependerá da avaliação da entidade de supervisão.

1.3. Os regimes de responsabilidade dos prestadores de serviços de certificação

A função das entidades certificadoras é muito importante no sistema da assinatura eletrónica, pelo que estão sujeitas a um conjunto de obrigações legais e de sanções nos casos de incumprimento.[768] É do cumprimento dessa obrigações que depende a prestação do principal serviço que lhe compete, que é o de geração da confiança nos agentes económicos, no que respeita à utilização dos suportes eletrónicos nos negócios jurídicos. Analisamos de seguida o regime da responsabilidade pelo eventual incumprimento dessas obrigações.

1.3.1. Fundamentos da responsabilidade

O regime da responsabilidade dos prestadores de serviços não tem que ser necessariamente diferente do regime geral de responsabilidade aplicável a qualquer agente económico.[769] São três as razões fundamentais que se enunciam para justificar a existência de normas específicas de responsabilidade na legislação relativa às assinaturas eletrónicas:

i) Porque a assinatura eletrónica é um instituto relativamente jovem, que os agentes económicos necessitam de ver consolidado;

[768] Em Portugal, essas obrigações constam dos artigos 24.º e seguintes, do DL n.º 290-D/99, de 2/8, tendo sido acrescentados, já em 2009, através do DL n.º 88/2009, de 9/4, os artigos 36.º-A, 36.º-B e 36.º-C, que tipificaram as contraordenações praticadas por estas entidades no exercício desta atividade, bem como as respetivas coimas aplicáveis. Só dez anos depois de o diploma legal que regula a assinatura digital ter entrado em vigor é que o legislador veio instituir o regime sancionatório para a violação dos importantes deveres que impendem sobre estas entidades.

[769] Tanto a LMCE como as Guidelines da ABA sobre a assinatura digital, não continham normas acerca da responsabilidade dos sujeitos da assinatura eletrónica. Embora as Guidelines enunciem um conjunto de obrigações dos três tipos de sujeitos, não prevê qualquer tipo de responsabilidade para os casos de incumprimento, doloso ou negligente. A LMAE foi, na verdade, o primeiro documento de carácter legislativo a consagrar essa responsabilidade.

ii) Pela necessidade de existir uma relativa uniformidade nesta matéria a nível internacional, a fim de evitar que as entidades certificadoras se instalem em territórios cuja jurisdição seja menos exigente;

iii) Pela necessidade de proteger os terceiros que confiam e os titulares das assinaturas, nos casos em que sofram prejuízos em razão da violação dos deveres de segurança.

O regime de responsabilidade assenta no conjunto das obrigações dos sujeitos, tanto dos titulares da assinatura, como dos prestadores de serviços de certificação, como ainda dos terceiros que confiam. Todos eles possuem um conjunto de obrigações que devem observar, e que é tanto mais importante quanto todo o sistema assenta na confiança dos agentes.

Os prejuízos sofridos pelos agentes em resultado do incumprimento das obrigações funcionais dos prestadores de serviços de confiança, podem ser relevantes, em especial quando uma pessoa se faz passar ilicitamente por outra. Este é um risco comum a todos os sistemas de autenticação, incluindo os que são baseados no papel, mas o facto de as redes abertas generalizarem o relacionamento jurídico com pessoas desconhecidas, aumenta os riscos de utilização errónea da identidade e da autenticação.

A LMAE estabelece um regime de responsabilidade baseado no princípio geral de que todos os sujeitos devem atuar com a diligência razoável, tendo sempre em vista evitar a utilização indevida das assinaturas eletrónicas. Trata-se de um regime de responsabilidade subjetiva, não sendo estabelecidas quaisquer previsões em matéria de responsabilidade pelo risco nem de responsabilidade contratual.[770] Relativamente à primeira, entendeu-se que não se justificaria previsão expressa nessa matéria, até para não desencorajar os agentes económicos do exercício de atividades conexas com as transações eletrónicas, e também porque não existiria fundamento para a existência de normas que derrogassem os regimes gerais nessa matéria existentes no direito interno de cada país.[771]

---

[770] Na elaboração da LMAE foram ponderadas várias possibilidades de configuração do regime de responsabilidade dos sujeitos da assinatura eletrónica, desde o regime da responsabilidade contratual, ao da responsabilidade objetiva ou pelo riso, e ainda o da responsabilidade pela culpa, tendo este último prevalecido. *"It is assumed that the liability of the parties involved in a PKI framework would essentially be based on three possible standards: ordinary negligence or fault; presumed negligence (or fault with reversed burden of proof); and strict liability"*. A/CN.9/630/Add.4; 16 April 2007, par. 19.

[771] Esse entendimento dominou na elaboração da LMAE. *"There was no compelling reason why certification authorities should be subject to a regime of strict liability. Moreover, such a regime would have the undesirable consequence of discouraging the emerging industry of certification authorities, thus limiting the possibilities of use of digital signatures"*. "A/CN.9/437", par. 56.

Os prestadores de serviços de confiança, devem adotar particulares regras de diligência no que respeita à sua prevalência, em três domínios fundamentais:[772]

i) Ao processo de criação e fornecimento de pares de chaves de assinatura eletrónica e dos respetivos certificados. Relevam particularmente os momentos críticos deste procedimento, em especial os que se referem:
   a. À identificação do titular da assinatura eletrónica. É da segurança destes procedimentos que depende a prevenção dos principal risco de eventuais tentativas de roubo ou usurpação de identidade.[773];
   b. À entrega do dispositivo de assinatura eletrónica por elas criado ao efetivo titular, garantindo, deste modo, que o dispositivo fica na sua exclusiva disponibilidade. A segurança acerca da identidade da pessoa a quem esse dispositivo é entregue é determinante da integridade da vinculação dessa pessoa aos seus instrumentos de assinatura eletrónica;
   c. À integridade do par de chaves que foi emitido. São instrumentos essenciais de segurança a conexão lógica entre a chave pública e a chave privada e a certeza de que foram adotados todos os procedimentos necessários para que a chave privada não seja derivada da chave pública. O primeiro garante que a informação fornecida pela entidade que presta serviços de segurança, acerca da identidade do titular da chave pública é segura e o segundo garante a segurança da conexão entre a chave privada e o seu titular e que essa chave não pode ser utilizada por um terceiro que se faça passar por ele.[774]

---

[772] Essas obrigações são especificadas no artigo 9.º da LMAE. "A/CN.9/WG.IV/WP.88", pág. 9.

[773] Caso esse dever de diligência não seja respeitado, pode a entidade certificadora emitir um par de chaves e um certificado que entrega a uma pessoa que se está a fazer passar por outrém abrindo assim a possibilidade de realização de fraudes em cadeia, por cujos prejuízos, tanto para a vítima da usurpação da identidade como para os terceiros que confiaram no certificado, deve ser responsabilizada a entidade certificadora. É essa a função principal das entidades certificadoras: *"The principal task of a certification services provider is to verify, in conformance with its stated practices, that an applicant is the purported signatory"*. A/CN.9/630/Add.5; par. 6.

[774] O regime estabelecido na Diretiva da Assinatura Eletrónica da UE assentava nos mesmos pressupostos da LMAE no que respeita à responsabilidade dos prestadores de serviços de certificação, vinculando os Estados Membros a adotar um regime de responsabilidade dos prestadores de serviços pelos prejuízos que causarem pelo incumprimento dos deveres de verificação da informação relativa à identidade do titular da assinatura; da certeza de que no momento da entrega do certificado de assinatura eletrónica este estava na posse exclusiva do respetivo titular, e de que, finalmente, estava garantida a correspondência e complementaridade entre a chave privada e a chave pública. A Diretiva exclui, porém esta responsabilidade nos casos em que a entidades prestadora de serviços demonstre não ter sido por culpa

ii) Relativamente ao conteúdo dos certificados de assinatura eletrónica, todos os elementos que deles constam são essenciais para que os terceiros que confiam possam verificar a vinculação do autor da assinatura ao documento. Trata-se, por exemplo, dos elementos relativos à validade do certificado e à sua vigência, à qualidade em que o autor do documento o assinou, à identidade da entidade certificadora, à data da assinatura, etc.;

iii) Na gestão das chaves públicas, os prestadores de serviços estão sujeitos a um conjunto de obrigações contínuas, de que são sujeitos ativos tanto os titulares das assinaturas como as partes que confiam. No primeiro caso trata-se, por exemplo, da disponibilização de serviços que possam receber do titular da assinatura os pedidos de cancelamento ou de suspensão da validade dos certificados, por exemplo nos casos em que estes verifiquem que pessoas estranhas acederam indevidamente à sua chave privada ou que passaram a conhecer a palavra-passe que protege esse acesso.[775] Do mesmo modo, devem aquelas entidades disponibilizar um serviço que permita ao titular comunicar o pedido de cancelamento do certificado, sempre que se verifique um facto que o determine, por exemplo, que deixe de exercer uma determinada função na entidade para a qual tinha sido emitido o certificado. Devem ainda disponibilizar informação acerca das práticas e dos compromissos de segurança utilizados, dos seguros contra riscos e das limitações de responsabilidade que praticam;

---

sua que ocorreu a produção dos prejuízos causados. "A/CN.9/630/Add.5", par. 9. O Regulamento EIDAS, que classifica os prestadores de serviços de confiança em qualificados e não qualificados, estabelece um regime de responsabilidade de ambos pelos danos causados por incumprimento das regras previstas no Regulamento. O incumprimento depende de prova depende de quem invoque o dano quando seja demandado um prestador não qualificado, invertendo-se o ónus de prova e presumindo-se a culpa quando de trate de prestadores qualificados.

[775] O prestador de serviços deve disponibilizar dois serviços, sendo um destinado à comunicação, pelo titular do certificado, das situações sem que este ficou exposto a uma possível utilização indevida. O outro serviço é a disponibilização púbica de uma consulta onde possam verificar se um determinado certificado por elas emitido está válido, ou então se está suspenso ou foi cancelado. A não disponibilização desses serviços, mesmo que parcial e em determinado momento, que tenha causado prejuízos, pode fazê-la incorrer em responsabilidade. Do mesmo modo, o atraso na disponibilização da informação acerca da suspensão ou do cancelamento de um certificado, que tenha causado prejuízo a uma das partes pode também ser fundamento de responsabilidade. No que respeita ao titular da assinatura, o dever de comunicação dos factos de que tenha conhecimento, que tenham colocado em situação vulnerável o dispositivo de assinatura, é também fundamento de responsabilidade quando não for cumprido com diligência. Estes serviços são essenciais para garantir a confiança no funcionamento do sistema de assinatura eletrónica.

iv) No que respeita aos serviços prestados aos terceiros que confiam, as entidades certificadoras devem disponibilizar a informação necessária à sustentação da sua necessidade de confiança, desde aquela que é intrínseca aos certificados, àquela que lhes é externa, como seja o facto de terem sido cancelados ou suspensos, as práticas utilizadas pela entidade no que respeita aos procedimentos de certificação, as limitações de responsabilidade, etc.

A violação das obrigações antes referidas é fundamento de responsabilidade para os prestadores de serviços, sempre que lhe seja imputável culpa por esse incumprimento que tenha conduzido à produção dos danos suscetíveis de indemnização. O n.º 2 do art.º 9.º da LMAE, que anteriormente citamos, consagra esta responsabilidade dos prestadores serviços sobre o conjunto das obrigações que relativamente a elas estabelece.

Tratando-se de uma responsabilidade subjetiva, ela é afastada nos casos em que não tenha sido por culpa das entidades certificadoras que ocorreu a vulnerabilização da confiança e da segurança do sistema.[776]

O regime de responsabilidade civil extracontratual das entidades certificadoras assenta, assim, na culpa resultante do incumprimento dos seus deveres funcionais legalmente estabelecidos, incluindo ainda as declarações de boas práticas que publicam. A base concetual deste regime é a violação das garantias de fiabilidade e confiança que os próprios prestadores de serviços de confiança haviam assumido como o fundamento dos serviços que prestam, de confiança a todos os agentes.

No regime da LMAE o ónus da prova da culpa caberá a quem invocar a responsabilidade, sendo certo que não é fácil essa atividade probatória num domínio com elevada componente técnica nos procedimentos, e em que as entidades

[776] Seria, por exemplo o caso das situações em que um terceiro se apropria da chave privada de outra pessoa e consegue assinar documentos com ela, em nome desta última, provocando-lhe sérios prejuízos. Se essa apropriação ocorreu em razão de uma conduta negligente do titular da assinatura que não adotou a diligência necessária para evitar aquela apropriação, omitindo também o dever de comunicar o cancelamento do certificado à entidade certificadora, então nenhuma responsabilidade será imputável a esta. Com se refere num dos documentos preparatórios da LMAE, *"In the event of erroneous identification of a person or erroneous attribution of a public key to a person, the certification authority would be held liable for the loss sustained by any injured party, unless the certification authority could demonstrate that it had done its best efforts to avoid the error"*. "A/CN.9/437", par. 58. E mais adiante, *"The certification authority should be exempt from liability if it could demonstrate that it exercised reasonable care in identifying the public key holder or performing its authentication functions; that the errors resulted from the user's own fault"*. *Idem*, par. 59.

certificadoras dispõem não só de um conhecimento superior aos restantes sujeitos, como de todos os instrumentos técnicos que lhe permitem apurar com rigor as causas dos danos que eventualmente tenham sido produzidos.[777]

Este regime de responsabilidade não é, porém, universal, nem sequer o que foi adotado na maioria das jurisdições nacionais, que penderam para o regime da presunção de culpa das entidades prestadoras de serviços, nos casos em que os terceiros que confiam nas assinaturas eletrónicas sofrem prejuízos quando essa confiança se frustra. Esse regime opera mediante inversão do ónus da prova, sendo que caberá a essas entidades a prova da sua falta de culpa para se eximirem da responsabilidade no caso de danos produzidos pela utilização indevida da assinatura eletrónica. Foi esse o regime adotado pela Diretiva 1999/93/CE[778], bem como pela China[779] e da Turquia, cuja legislação sobre a assinatura eletrónica estabelece uma presunção de culpa, que pode ser afastada no caso de a entidade provar que não atuou de forma negligente.

A diretiva 1999/93 estabelece, no art.º 6.º, um regime de responsabilidade presumida pelos prejuízos causado a terceiros de boa-fé, salvo se o prestador de serviços provar que não atuou de forma negligente, no que respeita à exatidão dos dados dos certificados e da segurança do processo de criação dos pares de chaves.

A lei alemã da assinatura eletrónica, de 1997, não estabelecia nenhuma previsão em matéria de responsabilidade, mas a lei de 2001 consagra uma norma idêntica à da diretiva no n.º 2 da secção 11 do art.º 1.º

---

[777] Nos trabalhos preparatórios da LMAE discutiu-se a possibilidade da inversão do ónus da prova, fundamentalmente pelo facto de as entidades certificadoras estarem numa posição de vantagem no que respeita ao acesso aos factos que estiveram subjacentes à produção do dano verificado. Porém, foi considerado que essa opção poderia aproximar a configuração do regime da responsabilidade objetiva, o que desde logo se pretendia afastar, para não criar constrangimentos ao acesso a estas atividades pelas empresas privadas, dado que se pretendia promover esse acesso. A inversão do ónus da prova, nomeadamente pela instituição de uma presunção de culpa das entidades certificadoras, poderia ser, ela própria um ónus e um risco elevado para o exercício desta atividade. *"Differing views were expressed as to whether the burden of proof of negligence should be on the certification authority or on the relying party. One view was that the burden of proof should be on the relying party"*. "A/CN.9/446", par. 162.

[778] A adoção deste regime de responsabilidade pela diretiva da UE conduziu a que a generalidade dos Estados-Membros o seguissem *"Under the European Union Directive on electronic signatures, for example, the certification services provider is liable for damages towards any entity that reasonably relies on the qualified certificate unless the certification services provider proves that it has not acted negligently"*. "A/CN.9/630/Add.4", par. 29. Do mesmo modo muitos países da América Latina seguiram este modelo, com destaque para a Argentina e o Chile. *Ibidem* par. 30.

[779] A lei chinesa da assinatura eletrónica de 2004, estabelece o artigo 28.º uma responsabilidade pela culpa com inversão do ónus da prova, mediante o estabelecimento de uma presunção de culpa da entidade certificadora, nos seguintes termos: *"If an electronic signatory or a person who relies on an electronic signature incurs a loss as a result of relying on the electronic signature certification service provided by an electronic certification service provider while engaging in civil activities, and if the electronic certification service provider fails to provide evidence that the provider was not at fault, then the electronic certification service provider shall bear liability for damages"*. "A/CN.9/630/Add.4", nota de rodapé 34.

A lei espanhola de 2003 institui um regime idêntico de responsabilidade, assente no regime geral da responsabilidade pela culpa, mas com a especificidade de o ónus da prova caber aos prestadores de serviços.[780]

A lei portuguesa da assinatura eletrónica, de 1999, na linha da LMAE, não estabelecia qualquer regime de responsabilidade específico, prevendo apenas uma responsabilidade pela culpa, no art.º 27.º. Este regime viria a ser alterado em 2003, pelo Decreto-Lei n.º 62/2003, de 3/4, que harmonizou o regime com a diretiva da UE, estabelecendo uma presunção de culpa em caso de culpa, competindo à entidade prestadora de serviços a prova de que "não atuou de forma dolosa ou negligente" (atual art.º 26.º).

O Regulamento EIDAS consagra também um regime de responsabilidade pela culpa, mas divide o ónus da prova, consoante se trate de prestadores de serviços qualificados ou não. Em caso afirmativo, presume-se a culpa dos prestadores de serviços, cabendo-lhe o ónus de demonstrarem que os danos não resultaram de uma sua ação culposa ou negligente.

Nos casos em que se trate de prestadores não qualificados, o ónus da prova da culpa passa a recair sobre os lesados.[781]

No regime do Regulamento EIDAS o fundamento da responsabilidade é o incumprimento das regras que nele estão previstas. Essas regras são genéricas para os prestadores de serviços não qualificados e específicas para os que possuem o estatuto de qualificados. Relativamente aos primeiros, estabelecem-se as seguintes obrigações:[782]

i) De ação, que são de dois tipos:
   a. Em primeiro lugar, uma obrigação de diagnóstico e de avaliação dos riscos de segurança tendo em conta o estado de evolução mais recente da tecnologia. Esta avaliação consiste num dever de cuidado e de vigilância na deteção dos riscos de segurança;

[780] O n.º 1 do artigo 22.º da "*Ley 59/2003, de 19 de diciembre*", tem a seguinte redação: *"Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone esta ley. La responsabilidad del prestador de servicios de certificación regulada en esta ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible"*.

[781] O n.º 1 do artigo 13.º do Regulamento EIDAS estabelece o princípio da responsabilidade dos prestadores de serviços de confiança por dolo ou negligência, por incumprimento dos seus deveres legais. O regime geral do ónus da prova é de quem invocar os dados produzidos, mas quando se trate de prestadores qualificados presume-se a sua culpa, *"exceto se este provar que os danos referidos no primeiro parágrafo não foram causados por sua intenção ou negligência"*.

[782] Artigo 19.º do Regulamento EIDAS.

b. Em face dessa avaliação devem essas entidades adotar a tomada de "*medidas de caráter técnico e organizativo*" que forem adequadas para gerir esses riscos de segurança. Incluem-se as medidas relativas à qualidade dos sistemas, da organização interna, dos procedimentos e da sua execução, da qualificação dos recursos humanos, etç;

c. Notificar todas as situações de violação de segurança ou de perdas de integridade, nos casos em que delas resulte impacto significativo sobre o serviço de confiança prestado ou sobre os dados pessoais conservados pelo prestador de serviços. Essa notificação deve ser efetuada à entidade de supervisão e a outras, conforme as situações, no prazo de 24 horas após a tomada de conhecimento. Essa notificação deve também ser feita ao adquirente do serviço.

ii) De resultado. Essas medidas devem ser as adequadas e necessárias para impedirem ou reduzirem ao mínimo o impacto dos incidentes de segurança, devendo proporcionar um nível de segurança que seja proporcional aos riscos diagnosticados.

Os prestadores qualificados de serviços de confiança, além de estarem também sujeitos às obrigações que acabamos de enunciar, estão sujeitos às obrigações específicas que estão enunciadas no artigo 24.º do Regulamento EIDAS, e que analisamos no ponto 1.5 do presente capítulo.

1.3.2. Limites da responsabilidade

O valor dos prejuízos causados por incumprimento dos deveres funcionais, tanto das entidades prestadoras de serviços como pelos titulares de assinaturas eletrónicas e pelos terceiros que confiam, pode ser muito relevante e de difícil previsão. Potencialmente, a utilização das assinaturas eletrónicas pode ocorrer em contratos ou atos com relevância jurídica de valor muito elevado.

É necessário distinguirmos os prejuízos que as partes sofrem em resultado do incumprimento das obrigações dos agentes que intervêm na criação dos instrumentos e assinatura eletrónica, daqueles que emergem da relação jurídica subjacente.

É necessário também analisar a questão da limitação do valor em que a responsabilidade se pode traduzir, bem como a possibilidade de os prestadores de serviços de confiança o estabelecerem. As assinaturas eletrónicas podem ser utilizadas em operações com relevância jurídica muito diversa e de valor muito elevado, cujo limite dificilmente poderá ser previsto com rigor. Essa dificuldade pode afastar deste tipo de atividade muitos agentes. A inexistência de um limite máximo previsível e gerível de responsabilidade poderia conduzir a que esse tipo de atividade viesse a ser apenas desenvolvido por entidades públicas, o que se pretendia evitar.

Esse problema poderia refletir-se também na dificuldade dos prestadores de serviços de confiança em constituírem seguros por preços aceitáveis, o que também poderia dificultar a utilização da assinatura eletrónica.[783]

Para a elaboração da LMAE ponderou-se o estabelecimento de limites legais ao valor da responsabilidade, tendo sido analisados vários critérios que se haveriam de projetar em diversas normas em várias jurisdições. As possibilidades eram as seguintes:

i) Fixando uma quantia máxima;[784]

ii) Em função do valor das prestações pagas ao prestador de serviços de confiança pelo titular da assinatura;

iii) Em função do valor do negócio ou do ato jurídico subjacente;

iv) Em função do prejuízo efetivamente sofrido.

O problema destes critérios é que todos apresentavam desvantagens. O primeiro poderia não ter qualquer relação com a perda sofrida, o segundo não tinha conexão com o tipo de serviço prestado e o terceiro poderia depender mais do negócio jurídico subjacente do que do serviço prestado pela entidade certificadora. O problema fundamental é que os serviços prestados pelos prestadores de serviços de confiança não são conexos com o negócio subjacente, do qual poderão advir os prejuízos, pelo que dificilmente será possível o estabelecimento de um critério objetivo e proporcional.[785]

---

783 *"Given the infinite number of transactions to which one single certificate might relate, it was doubtful that certification authorities would be in a position to acquire third-party liability insurance at a reasonable cost"*. "A/CN.9/437", par. 63.

784 Os critérios possíveis de limitação foram enunciados pela primeira vez nos trabalhos preparatórios da LMAE, em 1997. "A/CN.9/437", em especial os par.s 65 e 66. Seguimos com alguma distância essa enunciação, bem como os que constam de documentos seguintes, como é o caso do "A/CN.9/446", em especial nos par.s 163 e 164.

785 *"Service rendered by a certification authority, and the fees it charged, often bore no relationship to the value of the transactions to which they related or to the damage that might be sustained by the parties"*. A/CN.9/WG.IV/WP.73, par. 67.

Por outro lado, embora seja admissível que se proporcione aos prestadores de serviços de confiança um quadro de relativa segurança que lhes permita prever com razoabilidade os limites da sua possível responsabilidade, também não seria desejável que estes pudessem estabelecer um conjunto tão vasto de limitações que praticamente eliminem as possibilidades de responderem pelos dados que causassem. É dentro deste equilíbrio que o quadro legal se dever situar.

Apesar da dificuldade da configuração de um regime de limitação de responsabilidade, a legislação publicada, subsequente à LMAE, tem adotado, maioritariamente, o critério da limitação voluntária, estabelecida pela própria entidade prestadora de serviços de certificação, seja nos contratos que celebra com os titulares da assinatura, seja nas declarações de boas práticas, seja nos próprios certificados que emitem.

No que respeita à responsabilidade perante o titular da assinatura, a entidade certificadora poderia assumir uma limitação por cada assinatura ou por cada incidente, bem como excluir certo tipo de danos ou um certo tipo de utilizações da assinatura.[786]

A LMAE não viria a consagrar qualquer critério de limitação da responsabilidade de nenhuma das partes, mas prevê que os prestadores de serviços de confiança estabeleçam um limite, desde que lhe deem a devida publicidade, em especial no que respeita às partes que confiam nos certificados.[787] A LMAE não exclui a possibilidade de serem estabelecidos critérios de limitação máximos ou mínimos, deixando para as legislações nacionais a possibilidade de regularem essa matéria.[788]

A Diretiva 1999/93/CE reconhece o direito de os estados membros legislarem acerca da previsão dessa limitação.[789] Essa previsão consta dos n.ºs 3 e 4.º do art.º 6.º da

---

[786] *"Such statements may impose a cap to the liability per incident, per series of incidents, per period of time and exclude certain classes of damages"*. "A/CN.9/630/Add.4", par. 42.

[787] Esta possibilidade de limitação da responsabilidade é assumida de forma implícita, dado que a LMAE se limita apenas a estabelecer a obrigação de a entidade certificadora lhe dar publicidade e acesso às partes terceiras que confiam. Essa obrigação consta da alínea d), iv), do n.º 1 do artigo 9.º da LMAE. "A/CN.9/WG.IV/WP.88", pág. 10.

[788] Uma das razões do abandono da ideia de consagrar essa limitação na LMAE foram as reservas que se levantaram acerca da inadequação da sua aplicação aos terceiros que confiam na assinatura, dado que são estranhos à relação estabelecida entre o prestador de serviços de certificação e o titular da assinatura, sendo que pode ser lesado pelo incumprimento de ambos. *"Aggregate liability limits could not function since a relying party would have no way of knowing, under existing technology applications, whether a certain limit had been reached"*. "A/CN.9/446", par. 164.

[789] Atualmente os limites mais utilizados são de dois tipos, sendo um por tipo de operações, mediante o qual se excluem determinado tipo de operações da abrangência da responsabilidade e um limite de valor por cada operação. *"These limitations may be typically of two categories: there may be limits on the types of transaction for which particular certificates or classes of certificates may be used; there may also be limits on the value of the transactions in connection with which the certificate or class of certificates may be used"*. "A/CN.9/630/Add.4", par. 47.

Diretiva, prevendo-se que esse limite conste dos certificados de assinatura eletrónica. Essa limitação passou a constar das especificações obrigatórias que a lei consigna para os certificados, que no caso da lei portuguesa costa da alínea h) do n.º 1 do art.º 29.º do Decreto-Lei n.º 290-D/99, de 2 de agosto.

Do mesmo modo, a previsão de limitação da responsabilidade dos prestadores de serviços de confiança está prevista no Regulamento EIDAS, no n.º 2 do art.º 13.º. Nos seus termos, podem os prestadores de serviços de confiança limitar a sua responsabilidade, desde que se cumpram cumulativamente as seguintes condições:

i) Estabelecerem um limite de utilização dos seus serviços;

ii) Informarem previamente, e em forma devida, os seus clientes, acerca desses limites;

iii) Esses limites serem identificáveis por terceiros.

A possibilidade do estabelecimento destes limites aplica-se tanto aos prestadores de serviços qualificados como aos não qualificados.

1.4. Reconhecimento internacional das assinaturas eletrónicas

O reconhecimento internacional das assinaturas eletrónicas assume um relevo importante na sua disciplina jurídica, desde a sua génese nos fóruns internacionais de regulação das operações financeiras e do transporte transnacional de mercadorias.

Se a assinatura eletrónica constitui o instrumento essencial de garantia de vinculação jurídica dos suportes eletrónicos no comércio globalizado, a sua eficácia pode ficar comprometida pela limitação geográfica da validade dos certificados emitidos em cada jurisdição nacional, dado que não estaria garantida a validade e eficácia jurídicas dos documentos eletrónicos nas operações internacionais. E essa limitação impediria o crescimento da sua utilização.[790]

A questão da validade internacional das assinaturas eletrónicas divide-se em duas dimensões. Por um lado a validade, na jurisdição de um país, de uma assinatura eletrónica colocada num documento por um cidadão de outro país, onde se localiza

[790] Esta era a preocupação essencial nos trabalhos preparatórios da LMAE, até porque na data em que eles decorriam havia-se já expandido a utilização das comunicações eletrónicas nos mercados internacionais, e a utilização das assinaturas eletrónicas como instrumento de autenticação era já generalizada. *"The inclusion of provisions dealing with issues of cross-border recognition represented a significant step towards enhancing the trustworthiness of certificates. It was said that commercial practice was increasingly making use of certificates and that confidence in this new technology might be fostered through adherence to international standards"*. "A/CN.9/446", par. 190.

também a entidade certificadora que gerou os respetivos certificado e par de chaves. Por outro lado a possibilidade de um cidadão de um país possuir um par de chaves e um certificado gerados por uma entidade certificadora sedeada noutro país.

No primeiro caso está em causa a validade de uma assinatura em concreto em diferentes jurisdições internacionais. No segundo caso a validade de um certificado, também em diferentes jurisdições internacionais. No primeiro caso está em causa a circulação internacional dos documentos eletrónicos e a sua validade em jurisdições diferentes daquelas onde foi assinado. No segundo caso está a possibilidade de uma mesma pessoa possuir um único par de chaves e um certificado, e poder assinar documentos eletrónicos em qualquer país.

Nos trabalhos preparatórios da LMAE foram ponderadas duas possíveis vias para se alcançar a validade jurídica internacional, das assinaturas e dos certificados:

i) O reconhecimento pelos estados da validade dos certificados emitidos noutros estados. Esse reconhecimento poderia assumir a forma convencional, mediante acordos bilaterais ou multilaterais. Reconhecida a validade dos certificados, estaria, em consequência, reconhecida a validade das assinaturas;[791]

ii) A certificação, mediante um organismo nacional, tendencialmente de natureza administrativa da validade dos certificados internacionais, após avaliação, e mediante a existência de mecanismos eventuais de reciprocidade.[792]

Em ambos os casos a validade internacional das assinaturas eletrónicas dependeria sempre de uma intervenção orgânica do Estado, que seria um fator de incerteza, no primeiro caso porque os agentes económicos estariam sempre à espera

[791] Exemplo deste modelo é o que foi consagrado na lei da assinatura eletrónica de Singapura (Electronic Transactions Act 1998, Act No 25 of 1998), que faz depender do membro do governo a adoção de medidas de reconhecimento dos certificados estrangeiros, ficando esse reconhecimento dependente de uma entidade de controlo central. *"The Minister may by regulations provide that the controller may recognise certification authorities outside Singapore that satisfy the prescribed requirements for any of the following purposes: … "*. "A/CN.9/WG.IV/WP.82", pág. 36.

[792] No início dos trabalhos da LMAE eram estas as possibilidades em ponderação. *"Draft article I is based on the notion that recognition of foreign certificates should be provided under the responsibility of a local certification authority on the basis of reciprocity"*. "A/CN.9/WG.IV/WP.71", par. 74. E mais adiante: *"The Working Group may consider the approach taken in draft legislation in certain countries, under which recognition of foreign certificates could only be provided on the basis of bilateral or multilateral international agreements"*. *Idem*, par. 75. Tratava-se ainda de uma visão limitada, assente num pressuposto de ineficácia primária das assinaturas geradas em jurisdições estrangeiras, que só pode ser ultrapassada mediante ação dos estados. Esta perspetiva envolve uma limitação significativa da eficácia internacional da assinatura eletrónica, que produziria no futuro desenvolvimentos significativos nesta matéria.

dessa intervenção e no segundo porque essa sua intervenção seria sempre de resultado não seguro. Em ambos os casos o papel do Estado seria um fator de descontinuidade das assinaturas eletrónicas, cuja validade deveria sempre ser tendencialmente universal e estabelecida de uma só vez, logo desde a criação dos certificados, quando as partes de assegurassem da sua segurança e do seu grau de fiabilidade.

Esta opção orgânica seria a única possível nos casos em que a certificação de segundo nível dos sistemas utilizados pelas entidades certificadoras fosse da responsabilidade da administração pública, bem como nos casos em que existisse apenas uma PKI do Estado.

Neste caso, um agente económico que pretendesse verificar a validade de uma assinatura cujo certificado foi emitido por uma entidade estrangeira, poderia solicitar a esse órgão, tendencialmente da administração pública, do seu país, que certificasse o grau de fiabilidade dessa assinatura ou desse certificado.[793]

A esse modelo orgânico de reconhecimento, contrapõe-se outro, que faz sedear na própria lei os pressupostos objetivos da validade internacional dos certificados e das assinaturas eletrónica. Este modelo tem a vantagem de ser objetivo, dado que o grau de segurança e de fiabilidade dos certificados e das assinaturas seriam sempre suscetíveis de verificação, comparando as suas caraterísticas técnicas específicas com os pressupostos legais estabelecidos na legislação de cada país. A possibilidade de essas normas serem harmonizadas nas várias legislações nacionais seria também um importante fator de eficiência.[794] [795]

O problema deste segundo modelo reside no facto de existirem jurisdições nacionais que preveem a existência de certificados qualificados, que asseguram um grau de confiança mais elevado e *a priori* aos respetivos utilizadores, nos casos em que a

[793] Na conceção desse possível modelo foram identificados quatro níveis de certificação a efetuar por essa entidade nacional. No nível mais elevado essa entidade garantia a segurança dos procedimentos adotados pela entidade estrangeira que emitiu o certificado e atestava a validade e segurança desses procedimentos e do certificado. Neste caso, a entidade nacional teria que conhecer os procedimentos da outra e assumia a responsabilidade pelos respetivos certificados. No segundo nível, a entidade nacional fazia uma declaração de fiabilidade sobre a informação que lhe seria enviada pela entidade estrangeira, mas com reserva da veracidade dessa informação. No terceiro nível, a entidade nacional limitava-se a declarar a fiabilidade da entidade estrangeira, sem se pronunciar especificamente em relação ao certificado em concreto. No quarto nível, a entidade nacional certificava apenas a identidade da entidade estrangeira, com base exclusiva no seu certificado. "A/CN.9/437", par. 82.

[794] Essa possibilidade adquirira particular significado no contexto dos trabalhos preparatórios da LMAE, dado que era esse o seu objetivo final.

[795] A perceção das dificuldades da adoção do modelo do reconhecimento orgânico, assente no princípio da reciprocidade, resultou das primeiras discussões dos trabalhos preparatórios da LMAE, que, de seguida, avançou para o estudo do modelo da certificação cruzada. *"After considering the different views expressed in the Working Group, it was generally felt that it was appropriate to deal with the issues of cross-border certification in the draft uniform rules"*. "A/CN.9/437", par. 89.

entidade prestadora de serviços que os emite é reconhecida como cumprindo um determinado conjunto de requisitos legais. Ora, essa certificação vale apenas para aquela ordem jurídica. Por essa razão, as assinaturas emitidas com base nesse certificado podem não conferir o mesmo grau de segurança apriorística nas jurisdições estrangeiras.

O princípio da não discriminação dos certificados emitidos no estrangeiro garante que eles não possam deixar de ter validade noutro país, só pelo facto de terem sido emitidos no estrangeiro, mas o problema é que se perde aquela validade apriorística, por exemplo nos casos das assinaturas qualificadas, que confere uma segurança acrescida aos agentes económicos, e que é particularmente relevante nas relações comerciais estabelecidas a nível internacional.[796]

Os dois modelos antes referidos não são incompatíveis entre si, podendo as garantias e a confiança dos agentes económicos ser reforçadas com a consagração das normas substanciais que garantem a segurança e o reconhecimento dos certificados ser idênticos para aqueles que são emitidos por entidades nacionais ou estrangeiras. Em simultâneo, pode o sistema de certificação de segunda linha (ou seja a certificação dos procedimentos dos prestadores de serviços), aplicar-se tanto às empresas sedeadas num determinado país, como a entidades certificadoras estrangeiras. Um sistema de certificação cruzada de entidades certificadoras de primeiro ou de segundo nível, sedeadas em países diferentes, proporcionaria maior confiança aos agentes económicos. Para que um certificado emitido no estrangeiro tivesse a mesma eficácia jurídica dos que são emitidos na jurisdição nacional, seria necessário que uma entidade nacional certificasse que a entidade que o emitiu cumpre os pressupostos legais correspondentes, consignados na legislação nacional.[797]

Este modelo de reconhecimento cruzado é ainda mais vantajoso para a eficiência do comércio internacional se a certificação puder ser efetuada, tanto pelas

[796] É por essa razão que a aplicação minimalista do princípio da não discriminação, sendo simples e facilitadora da utilização transnacional dos certificados de assinatura eletrónica, não é suficiente para garantir esta eficácia apriorística. *"The consequence of this approach, however, is that such conditions are typically only confirmed a posteriori, and there is no assurance that a court will recognize the use of any particular method"*. "A/CN.9/630/Add.3", par. 5.

[797] Este é um dos problemas mais relevantes da adoção, pelas legislações nacionais, de mecanismos de regulamentação de tipos de certificados qualificados, que conferem aos respetivos utilizadores uma segurança reforçada, que opera *a priori*. Essas especificações nacionais tornam o reconhecimento internacional mais difícil, em face das respetivas especificidades. *"Conflicting technology-specific national legislation may therefore inhibit rather than promote the use of electronic signatures in international commerce. This could happen in two distinct but closely interrelated ways"*. "A/CN.9/630/Add.3", par. 7.

entidades certificadoras públicas, nos casos em que existam, como pelas entidades privadas.[798]

Em termos substanciais, o sistema de certificação cruzada pode ainda seguir dois modelos:

i) No primeiro, a lei estabeleceria tipos e requisitos específicos de credenciação de certificados emitidos por entidades estrangeiras. De entre os tipos de credenciação, o mais forte seria aquele que incidia sobre os procedimentos internos da entidade estrangeira que emitiu o certificado;

ii) No segundo modelo, essa certificação cruzada seria idêntica à certificação normal efetuada de forma voluntária entre entidades certificadoras no mercado interno.[799] Ela incidiria sobre o cumprimento dos requisitos legais da legislação do país onde seria efetuada. E, nesta matéria, o essencial é que os certificados ofereçam garantias de fiabilidade correspondentes àquelas que são exigidas pela legislação nacional.[800] No seio deste modelo são ainda possíveis dois tipos distintos de equivalência:

---

[798] Nos trabalhos preparatórios da LMAE constata-se como evoluiu o pensamento dos respetivos autores, desde um ponto de partida em que faziam depender a validade das assinaturas e dos certificados emitidos noutra jurisdição, do seu reconhecimento por um órgão da administração pública, para uma posição em que, admitindo-se a certificação cruzada, ela dependeria numa primeira fase das entidades certificadoras de segundo nível e só numa segunda fase das restantes. *"At an initial stage it was expected that cross-certification would be reserved exclusively to the "root authorities" (i.e., those authorities that certified the technology and practices in connection with the use of key pairs and registered subordinate certification authorities). At a later stage, as the industry developed, it was anticipated that also subordinate certification authorities placed below the "root" authority could become directly involved in guaranteeing the correctness of certificates issued by foreign certification authorities"*. "A/CN.9/437", par. 80.

[799] A certificação cruzada entre entidades certificadoras nacionais e estrangeiras foi um procedimento que se foi consolidando na prática comercial das entidades certificadoras, como forma de proporcionarem maior segurança aos agentes económicos, perante a ausência de regulação desta matéria nas legislações nacionais. Por essa razão, embora tenham sido estudadas diversas metodologias possíveis de reconhecimento internacional, foi para esse modelo que se orientaram progressivamente os trabalhos preparatórios da LMAE. *"The recognition of foreign certificates is often achieved by a method called "cross certification". In such a case, it is necessary that substantially equivalent certification authorities (or certification authorities willing to assume certain risks with regard to the certificates issued by other certification authorities) recognize the services provided by each other, so their respective users can communicate with each other more efficiently and with greater confidence in the trustworthiness of the certificates being issued"*. "A/CN.9/WG.IV/WP.88", par. 58.

[800] Ao estudarem-se os diversos critérios possíveis de estabelecimento da equivalência internacional dos certificados. Foi o critério objetivo da fiabilidade equivalente, frente As exigências legais nacionais, o que ficou consagrado. *"The prevailing view in the Working Group was that reliability was an appropriate criterion upon which to make a determination of equivalence for the purposes of recognition of foreign information certifiers"*. "A/CN.9/465", par. 27.

a. O reconhecimento reciproco, mediante o qual uma entidade certificadora estrangeira solicita a sua própria certificação a uma entidade certificadora nacional, mediante um pedido de concessão de licença ou então através de um pedido de auditoria. Este tipo de reconhecimento permite a interoperabilidade entre duas PKI, mas a responsabilidade pela confiança depositada num certificado estrangeiro será sempre do terceiro que confia.[801] Este tipo de reconhecimento não abrange a qualidade dos certificados, mas as práticas dos procedimentos de certificação de uma PKI sobre a outra.[802] Trata-se, fundamentalmente, de um reconhecimento formal e não substancial.[803] Ele não engloba a determinação dos certificados qualificados e limita-se a uma certificação de que uma determinada entidade que emitiu um par de chaves no estrangeiro exerce essa atividade;[804]

b. A certificação recíproca corresponde a uma certificação dos próprios certificados e do seu nível de confiança. Este tipo de certificação faz-se normalmente por via contratual entre duas entidades certificadoras de países diferentes, e tem normalmente efeitos recíprocos, salvo nos casos em que a certificação é unilateral. Em condições normais, a certificação cruzada dá origem à harmonização das práticas de certificação das entidades envolvidas e a uma declaração mútua e conjunto de práticas de certificação. Em resultado dessa harmonização, produz-se um alargamento das duas PKI das entidades envolvidas, pelo que todos os certificados emitidos quer numa quer na outra, passam a estar

---

801 *"The relying party makes an informed decision unilaterally based on the policies stipulated in the certificate policy or certificate practice statement in the foreign PKI domain"*. "A/CN.9/630/Add.4", par. 8.

802 *"The certification services provider is regarded as trustworthy if it has been licensed or accredited by a formal licensing or accreditation body, or has been audited by a trusted independent third party"*. "A/CN.9/630/Add.4", par. 8.

803 *"Cross recognition entails issues of technical interoperability at the application level only, i.e. the application must be able to process the foreign certificate and access the directory system of the foreign PKI area to validate the status of the foreign certificate*". "A/CN.9/630/Add.4", par. 7.

804 *"Cross recognition would typically occur at the PKI level rather than at the level of the individual certification services provider. Thus, where a PKI recognizes another PKI, it automatically recognizes any certification services providers accredited under that PKI scheme. Recognition would be based on assessment of the other PKI's accreditation process rather than assessing each individual certification services provider accredited by the other PKI"*. "A/CN.9/630/Add.4", par. 6.

> automaticamente reconhecidos em ambas.[805] Este tipo de certificação envolve uma responsabilização das entidades certificadoras pelas práticas seguidas pelas entidades certificadas, dado que correspondem à emissão de um juízo de conformidade entre os certificados emitidos e as exigências da legislação nacional do país da entidade certificadora.[806]

Este último modelo de reconhecimento é o mais eficiente e o que melhores garantias oferece às partes que confiam. É também o mais rápido. A desvantagem advém do facto de ele ser o mais exigente para as entidades que efetuam o reconhecimento, pelo grau de compromisso que assumem e de garantias que oferecem a entidades que não dependem delas e são estrangeiras. Esse nível de comprometimento pode afastar este tipo de reconhecimento, pelo facto de potencialmente poderem fazer incorrer essas entidades em níveis de responsabilidade de risco elevado.

Os sistemas de reconhecimentos das assinaturas e dos certificados emitidos em jurisdições estrangeiras deve respeitar um princípio de não discriminação, não devendo o facto de serem emitidos por agentes estrangeiros, ser fundamento para que sejam discriminados relativamente aos que são emitidos por sujeitos nacionais. Esta é uma regra fundamental do sistema.

Por outro lado, sempre que um certificado ou uma assinatura eletrónica gerados, respetivamente, por entidades certificadoras ou por titulares de assinatura estrangeiros cumpram os requisitos legais de validade, fiabilidade e eficácia estabelecidos na legislação nacional, devem ser suscetíveis de gerar o mesmo grau de segurança e de confiança.

O regime de equivalência internacional dos certificados, consignado na LMAE assenta, assim, no critério substancial da fiabilidade equivalente, nos termos do qual os certificados emitidos no estrangeiro devem ter a mesma validade daqueles que são emitidos pelos certificadores sedeados no próprio país, desde que cumpram os mesmos requisitos de fiabilidade consignados na legislação nacional.[807] Afastou-se, assim, a

---

[805] *"Cross certification involves technical interoperability and the harmonization of certificate policies and certificate practice statements"*. "A/CN.9/630/Add.4", par. 10.

[806] *"Recognizing the equivalence in legal duties and liability regimes entails a finding that the duties imposed on the parties operating under a PKI regime correspond in substance to those existing under the domestic regime and that their liability for breaches of those duties is substantially the same*". "A/CN.9/630/Add.4", par. 10.

[807] Esse consenso foi expresso do seguinte modo nos trabalhos preparatórios: *"A certificate issued by a foreign supplier of certification services should have the same legal effect as a certificate issued by a*

necessidade de um reconhecimento orgânico e de um procedimento de reconhecimento.[808]

São estes dois princípios – da não discriminação e da equivalência – que hão de enformar um sistema adequado de reconhecimento internacional, como aliás deve ocorrer nos mercados nacionais.[809]

Estes princípios e a objetividade do sistema, nos termos do qual a validade e a eficácia dos certificados dependem do cumprimento dos pressupostos estabelecidos na legislação de cada estado, e não de qualquer reconhecimento orgânico, são a base do regime adotado na LMAE.[810] De acordo com o princípio da não discriminação não se devem estabelecer na legislação requisitos objetivos para a validade dos certificados emitidos no estrangeiro, diversos daqueles que são aplicáveis aos emitidos por entidades certificadoras internas.[811]

A estes princípios deve associar-se também o da liberdade contratual, devendo a lei relevar a possibilidade de as partes convencionarem um método de autenticação, incluindo nos casos em que o respetivo instrumento foi gerado numa jurisdição estrangeira.[812] [813]

---

domestic supplier of certification services when such certificate afforded a substantially equivalent level of reliability". "A/CN.9/483", par. 36.

[808] *"The notion of recognition, which was known in other areas of the law (for example in connection with recognition and enforcement of foreign arbitral awards), was said to imply that a special procedure might be required in each instance, before a foreign certificate could produce legal effects in the enacting State"*. "A/CN.9/483", par. 34.

[809] A problemática da validade universal das assinaturas eletrónicas levou National Notary Association (NNA) dos EUA a propor a criação de uma assinatura eletrónica qualificada que utilizasse uma credencial notarial, conferida pela participação de um notário, que fosse válida e automaticamente reconhecida em todos os países. Reiniger, T.S. (2008). The Proposed International E-Identity Assurance for Electronic Notarization. *Digital Evidence and Electronic Signature Law Review*. Vol 5: pag.78..

[810] Foram esses os princípos que progressivamente foram ganhando corpo nos trabalhos preparatórios: *"Foreign entities should not be discriminated against, provided that they met the standards set forth for domestic certification authorities"*. "A/CN.9/446", par. 179.

[811] Nos trabalhos preparatórios da LMAE ponderou-se um conjunto de requisitos objetivos, mas essa ideia foi abandonada por se ter entendido como discriminatória, tendo, em alternativa, sido consensualizado que os requisitos legais da legislação interna deveriam ser suficientes para que, uma vez cumpridos pelos certificados emitidos no estrangeiro, fossem considerados válidos. *"An alternative draft of article 13 should be prepared, based on the view that criteria set forth with respect to signatures or certificates should apply equally to foreign and domestic signatures or certificates"*. "A/CN.9/465", par. 35.

[812] Também esta preocupação esteve presente nos trabalhos preparatórios da LMAE. *"Parties to commercial and other transactions should be accorded the right to choose the particular information certifier, class of information certifiers or class of certificates that they wished to use in connection with messages or signatures that they received"*. "A/CN.9/WG.IV/WP.82", par. 70.

[813] Este princípio ficou consagrado no texto da LMAE, no n.º 5 do artigo 12.º: *"Where, notwithstanding paragraphs (2), (3) and (4), parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law"*. "A/CN.9/WG.IV/WP.88", pág. 12.

A adoção destes princípios pela LMAE, fazendo prevalecer a atividade privada das entidades certificadoras, em detrimento da intervenção pública, seria também adotada pela Diretiva 1999/93/CE ,[814] sendo estabelecidos dois regimes diferentes:[815]

i) Quando o prestador de serviços que emitiu o certificado esteja estabelecido num estado membro, o art.º 4.º da Diretiva estabelece o princípio da livre circulação e, portanto, da validade em qualquer estado membro. Não se prevê, porém, qualquer mecanismo de execução deste princípio da equivalência, limitando-se a Diretiva a estabelecer que cada estado não pode aplicar a esses prestadores de serviços condições diferentes daquelas que aplica aos que estão sedeados no seu território;

ii) Quando os prestadores de serviços que emitiram o certificado estejam sedeados em países terceiros, o art.º 7.º da Diretiva prevê que os Estados Membros devem assegurar a equivalência entre os certificados qualificados emitidos noutros Estados Membros, desde que cumpram os requisitos substanciais da diretiva e simultaneamente o prestador se tenha acreditado voluntariamente num estado membro. Do mesmo modo se deve conferir equivalência em mais duas situações:

   a. Quando o certificado seja garantido por um prestador de serviços estabelecido na UE que cumpra os requisitos da diretiva;
   b. Quando o prestador de serviços seja reconhecido com base num acordo bilateral ou multilateral entre a UE e países ou organizações internacionais.

Apesar desta abertura da diretiva da UE existem, ainda assim, regimes diferenciados nos diversos Estados Membros. Irlanda e Malta reconhecem os certificados estrangeiros sem qualquer discriminação mas, noutros casos, a lei nacional exige uma avaliação específica, como é o caso do Luxemburgo e da Áustria, sendo que no caso da Estónia, Polónia e República Checa se exige uma verificação casuística e prévia por um serviço da administração pública.[816]

[814] "Directive 1999/93/Ec of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures".
[815] O n.º 1 do artigo 7.º da Diretiva.
[816] *"Ireland and Malta, for instance, recognize foreign digital signatures (qualified certificates, under European Union terminology) as equivalent to domestic signatures, as long as other legal requirements are satisfied. In other cases, recognition is subject to domestic verification (Austria, Luxembourg) or a decision of a domestic authority (Czech Republic, Estonia, Poland)"*. "A/CN.9/630/Add.3", par. 19.

A Lei Alemã de Assinaturas Eletrónicas, de 13/1/1997, anterior à diretiva europeia, consagrava um regime mais restritivo, estabelecendo uma equivalência limitada apenas às assinaturas digitais e às entidades certificadoras estabelecidas no espaço da UE e do Espaço Económico Europeu, desde que fosse previamente comprovada a equivalência da sua segurança relativamente ao disposto para o direito interno alemão. Relativamente aos certificados emitidos por entidades externas àqueles espaços, só era admitida equivalência mediante acordos internacionais.[817]

A lei alemã de 2001, que transpõe a diretiva prevê, na Secção 23, prevê a plena equivalência dos certificados qualificados emitidos por prestadores de serviços estabelecidos noutro estado membro. Caso o prestador seja estabelecido num país terceiro, aplica-se um regime idêntico ao da diretiva.

A lei portuguesa de 1999 consagrava, no art.º 37.º do Decreto-Lei n.º 290-D/99, de 2 de agosto, a equivalência dos certificados emitidos ou garantidos por prestadores de serviços credenciados noutros Estados Membros, mas limitava essa equivalência às assinaturas digitais. Nos casos em que tenham sido emitidos por prestadores de serviços estabelecidos em países terceiros, serão válidos caso exista acordo internacional que vincule o estado português.

Após a diretiva, Decreto-Lei n.º 62/2003, de 3/4, veio harmonizar o respetivo regime, estabelecendo a equivalência para as assinaturas eletrónicas qualificadas que tenham sido emitidas por entidades credenciadas em outro estado membro. Do mesmo modo, gozam do mesmo regime de equivalência os certificados emitidos pelas mesmas entidades.

No que respeita aos certificados qualificados emitidos por entidades estabelecidas em países terceiros, a equivalência só ocorre se essa entidade preencher os requisitos da diretiva e estiver credenciada num estado membro, bem como se o certificado estiver garantido por uma entidade estabelecida num estado membro, ou ainda se o certificado ou o prestador de serviços que o criou forem reconhecidos por

[817] O §15 tem a seguinte redação:
"§ 15 Foreign Certificates
(1) Digital signatures which may be checked with a public signature key for which a foreign certificate of another Member State of the European Union or of another contracting State of the Treaty on the European Economic Area exists are equivalent to digital signatures under this law, insofar as they demonstrate an equivalent level of security.
(2) Para. 1 also applies to other States, insofar as supranational or international agreements concerning the recognition of certificates have been concluded". "A/CN.9/WG.IV/WP.82", pág. 36.

acordo internacional.[818] Este regime de equivalência tem também a limitação de ser restrito às assinaturas qualificadas.

A lei espanhola de 1999 antecipava o regime da diretiva do mesmo ano. Estabelecia-se, logo na parte final do n.º 1 do art.º 4.º, o princípio da plena equivalência dos certificados e das assinaturas emitidos por prestadores de serviços estabelecidos em qualquer estado membro.[819] Nos casos em que esses prestadores estivessem estabelecidos em países terceiros, o regime era igual ao da diretiva. A lei de 2003 manteve este regime.[820]

A temática do reconhecimento internacional dos certificados de assinatura eletrónica é também a problemática da interoperabilidade das comunicações e das transações eletrónicas a nível internacional e entre diferentes jurisdições. A progressiva expansão das redes eletrónicas abertas é um fator constante de maior exigência da atividade económica no sentido de se alcançar uma maior integração dos sistemas de autenticação eletrónica.

Apesar da evolução que ocorreu no início do século XXI ao nível da eliminação dessas barreiras, em especial mediante a aplicação do princípio da não discriminação, a atividade económica exige sempre mais, dada a sua necessidade de crescimento permanente.[821]

O desafio atual é a criação de um sistema de autenticação universal, ou de um "paradigma universal de autenticação", que permita que cada pessoa possua apenas um instrumento de autenticação eletrónica que possa utilizar de forma universal, como uma espécie de identidade eletrónica, que tivesse a virtualidade de ser válido e imediatamente reconhecido em qualquer jurisdição.[822]

---

[818] Artigo 38.º do DL n.º 290-D/99, de 2/8, alterado pelo DL n.º 62/2003, de 3/4.

[819] A redação do n.º 1 do artigo 4.º do *"Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica"* era a seguinte: *"La prestación de servicios de certificación no está sujeta a autorización previa y se realiza en régimen de libre competencia, sin que quepa estabelecer restricciones para los servicios de certificación que procedan de alguno de los Estados miembros de la Unión Europea"*.

[820] "*Ley 59/2003, de 19 de diciembre, de firma electrónica"*, artigos 5.º e 14.º.

[821] Num estudo de 2005, a OCDE constatou a evolução ocorrida em matéria de autenticação eletrónica transfronteiriça, nomeadamente no que respeita ao aperfeiçoamento dos métodos de autenticação, da vigência dos princípios da neutralidade tecnológica e da não discriminação dos certificados estrangeiros, relevando a necessidade de maior integração internacional no que respeita à interoperabilidade eletrónica, sendo que a existência de um sistema internacional de autenticação era identificado como um fator decisivo. "The Use of Authentication Across Borders in OECD Countries". OECD Working Party on Information Security and Privacy. DSTI/ICCP/REG(2005)4/FINAL; 24-Nov-2005, disponível em http://www.oecd.org/internet/ieconomy/35809749.pdf (consulta em 19/11/2015).

[822] *"One scenario, the so-called "universal authentication paradigm", assumes that the principal purpose of authentication technologies will be to verify identities and attributes among persons who have no pre-existing relationship with each other and whose common use of technology is not the subject of contractual agreement"*. "A/CN.9/630/Add.3", par. 12.

Nesse sentido têm sido desenvolvidos esforços de vários organismos internacionais, com destaque para a UE, com a criação de organismos com a missão específica de promoverem a interoperabilidade eletrónica, como é o caso do CEN – Centro Europeu de Normalização e do ETSI - Instituto Europeu de Normas e Telecomunicações.[823] No entanto esse paradigma está ainda distante de se tornar uma realidade.

A falta de interoperabilidade dos sistemas nacionais de certificação da UE levou a CE a reconhecer o insucesso relativo da diretiva de 1999 no que respeita à criação de uma matriz europeia de assinatura eletrónica no espaço de toda a união.[824] Esse reconhecimento é manifesto com a sua inserção no Programa da Agenda Digital Europeia, em 2010[825] e é reconhecido em vários documentos.[826] [827]

Nesta sequência, o Regulamento EIDAS,[828] viria estabelecer um regime imperativo de interoperabilidade à escala europeia, que analisamos de seguida.

1.5. O regime de reconhecimento mútuo da União Europeia

O Regulamento EIDAS veio estabelecer, de forma imperativa, um regime de reconhecimento mútuo das assinaturas eletrónicas qualificadas baseadas em certificados

[823] O ETSI desenvolveu um modelo de verificação de serviços de confiança mútua, mediante o qual se pode verificar se um prestador de serviços de certificação a nível internacional desenvolve a sua atividade com o reconhecimento de alguma entidade. Para isso publicou a norma TS 102321. "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust Service Provider status information", disponível em http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ts_102231v010201p&RGW.doc (última consulta em 19/11/2015). Nele se prevê, nomeadamente, que a informação deve estar disponível para uma ampla gama de serviços e sistemas, incluindo o uso de certificados qualificados. A importância desta informação é especialmente significativo para as transações internacionais, devendo ser acessível usando um protocolo *on-line.*

[824] Como se refere no Regulamento EIDAS, *"There is no comprehensive EU cross-border and cross-sector framework for eIAS services. At EU level, a legal framework exists only for e-signatures but not for e-identification and authentication nor for related ancillary trust services"*. SWD(2012) 136 final, ponto 1.

[825] Como se refere textualmente, *"As tecnologias de identidade eletrónica (eID) e os serviços de autenticação são essenciais para as transacções na Internet tanto no sector privado como no público"*. COM(2010)245 final, pág. 12

[826] É relevante esse reconhecimento como fundamento da proposta de criação de um sistema de identificação eletrónica à escala da UE: *"There is no specific framework for mutual recognition and acceptance of elD or for ancillary trust services such as time-stamping or eseals"*. SWD(2012) 136 final.

[827] O Documento de trabalho que acompanha a proposta da CE para a implementação de um sistema de identificação eletrónica europeia, propõe a adoção de um sistema de supervisão, com várias alternativas, todas elas tendentes a eliminar a fragmentação do mercado europeu das assinaturas eletrónicas. *"A harmonized approach at EU-level for both e-signature and ancillary trust services would improve effective supervision, enhance legal certainty and augment the trust and security of e-transactions"*. SWD(2012) 136 final, ponto 6.3.

[828] Regulamento EIDAS.

qualificados, em todo o espaço da União Europeia. O regime aplica-se apenas às assinaturas qualificadas, desde que tenham sido emitidas por um prestador de serviços instalado num dos seus Estados Membros. Este regime não está dependente de qualquer ato de reconhecimento de qualquer Estado Membro, porque emerge diretamente do Regulamento (n.º 3 do artigo 25.º).

O regime aplica-se, de igual forma, aos selos eletrónicos qualificados baseados em certificados qualificados emitidos num Estado Membro (n.º 3 do artigo 35.º), bem como aos selos temporais (n.º 3 do artigo 45.º).

O Regulamento cria, na verdade, um sistema europeu de assinaturas eletrónicas qualificadas, de selos eletrónicos e de selos temporais, comum a todos os Estados Membros. Esse sistema assenta num princípio fundamental, que é o da mais elevada confiança e garantias de segurança. O legislador europeu faz acompanhar o caráter imperativo do reconhecimento mútuo, de um conjunto de normas destinadas a garantir a mais elevada qualidade e confiança possível no sistema. Por essa razão, a imperatividade do regime só se aplica às assinaturas eletrónicas qualificadas. E também por essa razão é criado um quadro jurídico assente em cinco medidas fundamentais:

i) O estabelecimento de um regime específico dos prestadores qualificados de serviços de confiança, que são os únicos que podem emitir certificados qualificados de assinaturas eletrónicas, que analisaremos no ponto 1.6 do presente capítulo, já a seguir;

ii) O estabelecimento de um regime específico das assinaturas eletrónicas qualificadas (como analisámos no ponto 3.5 do Capítulo II da Parte II);

iii) O estabelecimento de um sistema de supervisão à escala europeia, como analisámos no ponto 1.2.3 do presente Capítulo II da Parte III;

iv) O estabelecimento de um regime de certificação dos dispositivos qualificados de assinatura eletrónica, nos termos do artigo 30.º do Regulamento. Mediante este reconhecimento, entidades públicas ou privadas designadas pelos Estados Membros, certificam a conformidade destes dispositivos com os requisitos estabelecidos no Anexo II do Regulamento, para a classificação destes certificados como qualificados;[829]

[829] O regime de certificação foi publicado na Decisão de Execução (UE) 2016/650 da Comissão, de 25 de abril de 2016.

v) A instituição da marca de confiança UE, que pode ser utilizada pelos prestadores qualificados de serviços de confiança, nos termos do artigo 23.º do Regulamento, depois de ter sido publicada na lista correspondente, a atribuição desse estatuto.[830]

Além de estabelecer os pressupostos legais para o reconhecimento mútuo, o Regulamento assegura os procedimentos operativos mediante a exigência de que a verificação das assinaturas e dos certificados pelos terceiros interessados possa ser feita de forma automatizada, nomeadamente estabelecendo essa obrigação como condição para os certificados qualificados (alínea a) do Anexo I e alínea a) do Anexo III para os selos eletrónicos), obrigando os Estados Membros a publicarem as listas antes referidas num formato adequado ao tratamento automático (n.º 2 do artigo 22.º e alínea b) do n.º 1 do artigo 33.º). Estes mecanismos permitem que a verificação das assinaturas possa ser efetuada em qualquer Estado Membro de forma automatizada e simples, independentemente do Estado Membro onde foram criadas, criando-se assim um sistema de interoperabilidade das assinaturas eletrónicas qualificadas e dos selos eletrónicos qualificados.

Embora a base fundamental de confiança do sistema assente no estatuto dos prestadores qualificados de serviços de confiança, o Regulamento não impede, naturalmente, que operem no mercado da prestação de serviços de confiança prestadores não qualificados, mas as assinaturas eletrónicas não qualificadas não beneficiam do regime imperativo do reconhecimento mútuo que o Regulamento estabelece.

O regime de supervisão assume o carácter administrativo e público do bem jurídico proporcionado pelos prestadores qualificados de serviço de certificação, que é a confiança eletrónica à escala europeia.

Do regime reconhecimento mútuo e de interoperabilidade faz parte também um regime de publicação de duas listas de confiança:

i) Lista dos prestadores qualificados de serviços de confiança, elaboradas e disponibilizadas por cada Estado Membro, contendo a sua identificação e a identificação dos serviços que prestam (n.º 1 do artigo 2.º). As listas devem ser suscetíveis de o acesso e tratamento automático dos respetivos dados, para efeitos de verificação das assinaturas;

[830] As especificações relativas à forma do símbolo da Marca de Confiança UE foram publicadas pela Comissão no Regulamento de Execução (UE) 2015/806, da Comissão, de 22 de maio de 2015.

ii) Lista dos dispositivos qualificados e certificados de criação de assinatura eletrónica, nos termos do artigo 30.º do Regulamento, como estabelece o artigo 31.º. Inclui-se, também, a lista de dispositivos dos selos eletrónicos qualificados (n.º 3 do artigo 39.º).

A interoperabilidade é ainda reforçada pela liberdade de prestação de serviços em todos os Estados Membros, consignada no art.º 4.º.

No que respeita ao reconhecimento internacional dos certificados emitidos por prestadores de serviços de confiança estabelecidos em países terceiros, o art.º 14.º do regulamento faz depender a sua equivalência aos certificados qualificados, desde que os serviços de confiança desse país forem reconhecidos nos termos de um acordo bilateral ou multilateral.

Assim, um prestador de serviços de confiança que se estabeleça num Estado Membro da União Europeia e adquira nele o estatuto de prestador qualificado pode passar a emitir certificados de assinatura eletrónica qualificada, suscetíveis de beneficiarem do reconhecimento mútuo.

Embora se trata de modelos distintos, a interoperabilidade das assinaturas eletrónicas qualificadas e dos selos eletrónicos qualificados representam um passo relevante na criação do designado espaço digital europeu. O Regulamento pretende ser uma resposta abrangente ao problema da fragmentação e da falta de interoperabilidade, criando um verdadeiro regime europeu das assinaturas eletrónica, substituindo o da diretiva de 1999.[831]

Apesar disso, o Regulamento fica ainda longe de alcançar esse objetivo porque é ainda parcial o regime de interoperabilidade que cria, ficando de fora as assinaturas eletrónicas não qualificadas.

Do mesmo modo é ainda parcial o regime da interoperabilidade europeia da identificação eletrónica, dado que só é imperativo para a identificação eletrónica dos cidadãos europeus perante os serviços eletrónicos das respetivas administrações

[831] Como se refere no par. 54 dos considerandos do regulamento, *"A interoperabilidade e o reconhecimento transfronteiriço de certificados qualificados é um requisito prévio do reconhecimento transfronteiriço de assinaturas eletrónicas qualificadas"*.

públicas.[832] E embora ele não exclui a sua utilização por entidades privadas de forma voluntária, trata-se ainda de um primeiro passo.[833]

No que respeita à interoperabilidade das assinaturas eletrónicas, é estabelecido um regime imperativo comum a todos os Estados Membros, nos termos do qual as assinaturas eletrónicas qualificadas que cumprem os requisitos do Regulamento são válidas em todos os Estados Membros, independentemente daquele onde estejam estabelecidos os respetivos prestadores de serviços. Para isso, o Regulamento impede os Estados Membros de instituírem, na sua legislação interna, requisitos obrigatórios que excedam os previstos no seu Anexo I.[834] Esse impedimento garante o reconhecimento pleno e automático dos certificados em todos os Estados Membros.[835]

1.6. Os prestadores qualificados de serviços de confiança

O Regulamento EIDAS institui, pela primeira vez o estatuto dos prestadores qualificados de serviços de confiança, sendo esse um dos instrumentos fundamentais de controlo da qualidade dos serviços por eles prestados e da geração de confiança em todos os agentes, no que respeita à utilização dos meios eletrónicos.

O acesso a esse estatuto é controlado previamente pelas entidades de supervisão, mediante uma avaliação prévia dos pressupostos legais correspondentes. Esses pressupostos são os seguintes (seguimos a anunciação do artigo 24.º do Regulamento):

1. - Relativos aos próprios prestadores de serviços:

[832] Como se refere no ponto 12 do preâmbulo do Regulamento, *"Um dos objetivos do presente regulamento é eliminar os obstáculos existentes à utilização transnacional dos meios de identificação eletrónica utilizados nos Estados-Membros para a autenticação para, pelo menos, os serviços públicos"*.
[833] A extensibilidade do programa às entidades privadas é admitida e desejada pela proposta, tendo sido consignada na proposta: *"The concept of notified eID is not limited to public-sector issued eIDs: Member States could also notify eIDs issued by the private sector that they recognise for use in their own public-sector services. This approach is necessary since not all Member States authorities issue eIDs The cross-sector approach of the legislation would allow the private sector to integrate the use of notified eIDs in e-services when secure e-identification is needed"*..SWD(2012) 136 final, pág. 6.
[834] Esse impedimento consta do n.º 2 do artigo 38.º do Regulamento, acrescentando o n.º 3 que os estados membros podem estabelecer requisitos facultativos, desde que não impeçam a interoperabilidade.
[835] O Regulamento permite que os Estados Membros estabeleçam, em legislação interna, a possibilidade de os certificados qualificados de assinatura eletrónica incluírem "*caraterísticas específicas adicionais não obrigatórias*", mas desde que delas não resulte prejuízo para a interoperabilidade das assinaturas (n.º 3 do artigo 28.º do Regulamento), dado ser esse o objetivo fundamental do Regulamento. Esta regra aplica-se também aos selos eletrónicos, nos termos do n.º3 do artigo 38.º.

1.1. – Possuírem o estatuto correspondente, nos termos do artigo 21.º, devendo previamente o prestador de serviço entregar uma notificação com a intenção de iniciar uma atividade como prestador qualificado, acompanhada de um relatório de avaliação da conformidade. Mediante a análise desse relatório, se estiverem cumpridos os pressupostos legais, a entidade supervisora atribui o estatuto, só depois podendo esta iniciar a atividade (n.º 3 do artigo 21.º);

1.2. Possuírem recursos humanos especializados e de confiança adequados para o nível de confiança dos serviços que prestam; bem como recursos financeiros ou seguros capazes de responderem à responsabilidade em que possam vir a incorrer (alíneas b) e c) do n.º 2 do artigo 24.º);

1.3. Mantêm um plano de cessação de atividade que garanta a continuidade do serviço que prestam.

2. - Relativos aos procedimentos:

2.1. – Informarem a entidade supervisora das alterações aos serviços qualificados que prestam, incluindo a intenção da sua cessação (alínea a) do n.º 2 do artigo 24.º);

2.2. – Informarem previamente os seus clientes dos termos e condições da prestação de serviços de confiança (alínea d) do n.º 2 do artigo 24.º);

2.3. – Verificam a identidade e caraterísticas específicas das pessoas, singulares e coletivas a quem emitem certificados qualificados de assinatura eletrónica ou de selos eletrónicos (n.º 1 do artigo 24.º). Essa identificação rigorosa tem natureza crítica para a segurança e confiança nas assinaturas e nos selos eletrónicos qualificados, e deve assentar sempre a sua base nos serviços de identificação, de acordo com as legislações dos Estados Membros, para a identificação civil ou comercial. No caso de pessoas físicas, a base da identificação é sempre a presença física, podendo, porém, essa presença ser substituída por um documento ou meio de identificação que tenha sido emitido com base nela e a comprove (alíneas a) a d) do n.º 1 do artigo 24.º). No entanto esse meio de

identificação tem necessariamente que corresponder a um nível de garantia substancial ou elevado, nos termos que analisamos no ponto 4 do Capítulo V da Parte II.

3. - Relativos à segurança na geração dos dispositivos de assinatura e de selos eletrónicos qualificados:
   - 3.1. - Utilizam sistemas e produtos fiáveis de geração dos dispositivos, bem como de armazenamento de dados;
   - 3.2. - Tomam medidas contra a falsificação e o roubo dos dados;
   - 3.3. - Garantem um tratamento lícito dos dados pessoais.
4. Requisitos relativos à gestão dos certificados emitidos:
   - 4.1. Mantêm acessíveis todas as informações relativas aos certificados que emitem;
   - 4.2. Disponibilizam serviços de comunicação das situações que implicam a anulação dos certificados, que devem ser rápidos e seguros, a possibilidade de se verificar a data e a hora de emissão dos certificados, a adoção de medidas contra a falsificação, bem como o registo de todos os acontecimentos relevantes relativos aos certificados;
   - 4.3. Em caso de revogação dos certificados qualificados, registam-na e publicam-na no prazo de 24 horas.

A verificação do cumprimento dos requisitos para o estatuto de prestador qualificado de serviços de confiança é da competência das entidades de supervisão, sendo que essa verificação é permanente, iniciando-se com o seu caráter apriorístico relativamente à atribuição do estatuto e continuando sucessivamente, dado que o Regulamento estabelece que as entidades de supervisão podem desencadear auditorias pelos seus próprios meios ou pedi-las a organismos de avaliação da conformidade, nos termos previstos no n.º 2 do artigo 20.º. Essas auditorias são obrigatoriamente feitas de 24 em 24 meses (n.º 1 do artigo 20.º). Essa competência inclui-se na função de supervisão genericamente enunciada no artigo 17.º e inclui a possibilidade de essas entidades ordenarem a correção de situações de incumprimento, bem como de retirarem o estatuto de qualificado ao prestador (n.º 3 do artigo 20.º). As auditorias são efetuadas nos termos determinados pela Comissão Europeia (n.º 4 do artigo 20.º) e delas deve ser efetuado reporte anual a Comissão, nos termos do n.º 6 do artigo 17.º.

O caráter integrado do controlo sobre os prestadores qualificados revela a intervenção pública a que o legislador europeu submeteu o sistema de reconhecimento mútuo. Essa intervenção pública é efetuada com o propósito de tornar mais efetivo os sistema de interoperabilidade, dentro de uma opção de liderança púbica e da prossecução de um nível mais elevado de garantia de confiança.

Trata-se de uma opção que não é isenta de riscos e que marca uma rotura com o modelo anterior, tanto da Diretiva de 1999 como da LMAE, assentes na liberdade de acesso, na liberdade de exercício das atividades económicas e na autorregulação dos agentes. Compreende-se que num espaço europeu que se pretende integrado, resultando essa integração de uma opção política dos Estados, exista também uma intervenção pública relevante. No entanto a opção não é isenta de riscos, em especial pela ineficiência que pode advir na menor rapidez de resposta às solicitações da economia e dos agentes, pelos organismos públicos, que não operam em regime de concorrência.

Analisaremos adiante, no ponto 5.8 do capítulo V, os efeitos da entrada em vigor do Regulamento EIDAS, no que respeita aos prestadores qualificados de serviços de confiança.

2. O titular da assinatura eletrónica

No paradigma do papel não existe o conceito de dispositivo de assinatura, por ela ser inata à pessoa que assina. Assinar um documento em papel corresponde ao ato de escrever o nome ou de o desenhar no papel com um determinado formato, caraterístico e irrepetível.

No paradigma eletrónico, a assinatura eletrónica só existe mediante a utilização de um dispositivo tecnológico que aplique a um documento um conjunto de dados cuja detenção é exclusiva de uma pessoa. Esse dispositivo não é intrínseco ao sujeito, pelo que, sendo uma entidade distinta, terá que ser por ele detido, o que significa que é um objeto suscetível de posse e de apropriação por terceiro. A segurança do sistema de assinatura depende da exclusividade da detenção desse dispositivo. O elemento essencial que garante a vinculação de quem assina a um documento assinado é o da exclusividade da detenção desse instrumento. A preservação do segredo do acesso à chave privada e aos restantes instrumentos de criação da assinatura eletrónica que

constam daquele dispositivo é a primeira obrigação do titular do par de chaves que a própria lei estabelece.[836]

Esse conceito de detenção exclusiva, sendo essencial à assinatura eletrónica não tem qualquer correspondência na assinatura manuscrita, pelo que se trata de um conceito jurídico. Por essa razão, a lei estabelece ao titular do dispositivo um conjunto de obrigações que não têm paralelo na assinatura manuscrita. Uma dessas obrigações é a de o titular adotar os comportamentos de diligência e cuidado, necessários e adequados, a garantir a exclusividade do acesso ao dispositivo de assinatura eletrónica.

No direito da assinatura eletrónica devemos distinguir entre o conceito de "*assinante*" (ou "*signatário*") e de "titular de um dispositivo de assinatura". Enquanto o primeiro só existe depois de o seu titular ter aplicado o seu dispositivo de assinatura para autenticar um documento, o segundo existe desde que é gerado o par de chaves e o certificado correspondente.

Outra importante diferença entre o paradigma do papel e o eletrónico é a de que, na assinatura eletrónica, a pessoa que aplica a assinatura sobre o documento não tem que ser necessariamente o titular da assinatura. Enquanto a assinatura de um documento em papel tem que ser necessariamente colocada pelo respetivo titular, a assinatura de um documento eletrónico por uma pessoa, pode não ser necessariamente efetuada materialmente por essa pessoa. É possível que, com o consentimento do titular do respetivo dispositivo, um terceiro possa ter acesso autorizado aos dados de assinatura e que aplique esses dados sobre um documento eletrónico, que passará a estar assinado e a vincular juridicamente o titular do dispositivo.[837]

Do mesmo modo, o facto de o dispositivo de assinatura eletrónica ser um objeto que se separa do seu titular, torna possível que uma pessoa coletiva possua uma assinatura eletrónica e que com ela se possam assinar documentos eletrónicos que a vinculam. Ao contrário da assinatura manuscrita, que é própria de pessoas físicas, a assinatura eletrónica, sendo um instrumento objetivado de vinculação de uma pessoa a

---

[836] O n. 1 do artigo 31.º do DL n.º 290-D/99, de 2/8 estabelece o titular deve *"preservar a confidencialidade da informação transmitida"*, acrescentado o n.º 2 que *"em caso de dúvida quanto à perda de confidencialidade dos dados de criação de assinatura* (na verdade a chave privada, ressalvamos nós)*, o titular deve pedir a suspensão do certificado e, se a perda for confirmada, a sua revogação"*.

[837] O regulamento EIDAS, só admite que terceiros efetuem a geração de assinaturas eletrónicas em nome do signatário, nos casos em que se trate de assinaturas eletrónicas qualificadas e os esses terceiros sejam prestadores qualificados e serviços de confiança (n.º 3 e 4 do Anexo II do Regulamento). Porém, para que a assinatura se mantenha como qualificada, será necessário que o signatário mantenha a exclusividade do acesso aos instrumentos para a aplicação da assinatura, nomeadamente que o canal utilizado seja controlado pelo signatário. No ponto iii) do Capítulo VI da Parte III, desenvolvemos este tópico.

um documento, pode esse objeto ser instrumento de vinculação de pessoas coletivas.[838] Dado que uma assinatura eletrónica garante a origem de um documento e as pessoas coletivas emitem documentos, então podem existir assinaturas eletrónicas de pessoas coletivas.[839]

Em todos os casos que acabamos de enunciar se levanta o problema de definir qual o conceito de "assinante", "signatário" ou pessoa que assina. A dificuldade que se coloca refere-se à separação entre a pessoa que fica vinculada juridicamente com a assinatura de um documento eletrónico e a pessoa que concretamente executa o ato material de assinar. Ou, dito de outro modo, a diferença entre a pessoa que é titular e está identificada no certificado de assinatura eletrónica e a pessoa que em concreto executa os atos materiais de aplicação da chave privada da assinatura eletrónica ao documento eletrónico.

A LMAE utiliza o conceito de "assinante", reportando-o à pessoa que executa os atos materiais correspondentes à aplicação da chave privada sobre um documento eletrónico. Nos termos da respetiva disposição normativa, o assinante é a pessoa que possui o dispositivo de assinatura eletrónica em seu poder e que o aplica ao documento eletrónico assinado. Esta definição inclui, nos seus próprios termos, a pessoa que é o próprio titular em nome próprio de um dispositivo de assinatura eletrónica e a pessoa que possui um dispositivo em nome de outrem, seja como seu procurador, seja como seu representante legal ou voluntário.[840]

É sobre o assinante que a LMAE faz reportar a verificação dos pressupostos de exclusividade de acesso, bem como a responsabilidade por reportar eventuais situações causadoras do cancelamento ou da suspensão do certificado.[841] Do mesmo modo é sobre o assinante que recai a responsabilidade pela eventual violação dos seus deveres de cuidado no que respeita à segurança do acesso aos dados de assinatura.

---

838 *"In a paper-based environment, for instance, legal entities cannot strictly speaking be signatories of documents drawn up on their behalf, because only natural persons can produce authentic hand-written signatures"*. "A/CN.9/WG.IV/WP.88", par. 101.

839 Não foi assim que se entendeu na elaboração do Regulamento EIDAS, onde se reserva o conceito da assinatura eletrónica para as pessoas singulares, segundo um princípio de plena equivalência funcional entre as assinaturas eletrónicas e as assinaturas manuscritas. Em alternativa cria-se, no mesmo Regulamento, a figura dos selos eletrónicos, cuja função é a mesma das assinaturas eletrónicas, mas se reserva à autenticação dos documentos emitidos por pessoas coletivas.

840 Alínea e) do artigo 2.º da LMAE: *"(d) "Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents"*. "A/CN.9/WG.IV/WP.88", pág. 8.

841 *"Under the Model Law, the notion of "signatory" cannot be severed from the person or entity that actually generated the electronic signature, since a number of specific obligations of the signatory under the Model Law are logically linked to actual control over the signature creation data"*. "A/CN.9/WG.IV/WP.88", par. 102.

Ao contrário do que o conceito em língua portuguesa pode envolver, o assinante previsto na LMAE não é a pessoa que assinou um documento em concreto, mas antes a pessoa que possui, em seu nome, ou no nome de outrem, um dispositivo de assinatura eletrónica, mesmo que nunca o tenha aplicado na assinatura de nenhum documento. No caso em que o possuidor do dispositivo assina em nome e representação de outra pessoa, física ou coletiva, que é o real titular do par de chaves e do dispositivo, é ela em concreto que é o assinante, sendo que essa assinatura que essa pessoa executa vincula o seu representado.[842] Neste caso existe uma clara separação entre o titular do dispositivo de assinatura, que é a pessoa que fica vinculada juridicamente com a aplicação dos dados de assinatura constantes desse dispositivo, e a pessoa que em concreto efetua os atos materiais correspondentes a essa aplicação. Distinguimos, então, a pessoa a quem todos os terceiros que confiam atribuem a assinatura do documento, por um lado, e a pessoa que em concreto gerou a assinatura, por outro lado.[843]

Em nosso entendimento, a LMAE deveria ter centrado a definição de assinante na pessoa que é o titular da assinatura, que é a mesma que é titular do dispositivo de assinatura. É a essa pessoa que a entidade certificadora se deve assegurar que entrega pessoalmente o dispositivo de assinatura eletrónica e é também ela que, em correspondência, deve garantir a exclusividade do acesso aos respetivos dados, assegurando-se de que não ficam, em momento algum, vulneráveis ao acesso de terceiros. Do mesmo modo é essa pessoa que é responsável pela eventual violação da exclusividade do acesso aos dados de assinatura, quando isso se deva a um comportamento menos diligente da sua parte.

Quando se trate de pessoas coletivas, a assinatura eletrónica pode ser efetuada diretamente por estas entidades com um dispositivo de assinatura eletrónica de que uma entidade desse tipo seja titular.[844] Esta é uma das diferenças entre a assinatura eletrónica e a assinatura manual, como já anteriormente referimos. Porém, o ato de assinatura, em si mesmo, de um documento eletrónico, terá que ser executado por uma pessoa singular.

---

842 *"Signed a contract as an agent for another person was still regarded as the signatory of the contract, even though the contract was to become binding on the person whom he or she was representing"*. "A/CN.9/483", par. 83.

843 *"In the context of communications by electronic means, the notion of signatory might need to be defined in a manner that encompassed both the person that actually generated the electronic signature and the person to whom the signature was attributed"*. "A/CN.9/483", par. 84.

844 Como referimos anteriormente, o regime do Regulamento EIDAS reserva a assinatura eletrónica para as pessoas singulares e não permite a utilização deste conceito para as pessoas coletivas. Admite, porém, naturalmente, que as pessoas coletivas emitem documentos, que terão que ser autenticados, mas, para isso, cria de novo a figura dos selos eletrónicos, cuja função e modo de operação é igual ao das assinaturas eletrónicas.

Essa pessoa terá que possuir os poderes correspondentes que lhe confiram legitimidade para ter acesso aos dados de assinatura eletrónica da pessoa coletiva. Mas a verdade é que é a pessoa coletiva que assina, que fica vinculada juridicamente ao documento assinado, e que é o titular dos dados da assinatura eletrónica, pelo que é ela que é o sujeito da assinatura. Deveria ser sobre esta entidade que devia incidir a norma da LMAE que tipifica quem é o sujeito da assinatura eletrónica.

A incidência da definição sobre o titular do dispositivo de assinatura seria também importante para os terceiros que confiam na assinatura. Para estes, a pessoa que assina é aquela cuja identidade consta do certificado que acompanha a assinatura eletrónica, em todos os casos, incluindo aqueles em que a pessoa que executa materialmente os atos correspondentes de aplicação do dispositivo sobre o documento, é um terceiro. Este terceiro executante, não é, aliás, nunca, do conhecimento daqueles que recebem os documentos por ele assinados, dado que o seu nome e a sua identificação não constarão do certificado.

A explicação que é dada nos documentos dos trabalhos preparatórios da LMAE, para a opção da definição do conceito de assinante em redor da pessoa que materialmente executa a aplicação dos dados de assinatura sobre os documentos a assinar, é a de que todas as obrigações e responsabilidades que a LMAE estabelece para as pessoas que assinam documentos eletrónicos estão dirigidas para eles.[845] Afastam-se dessas obrigações e responsabilidades os titulares de assinaturas eletrónicas, nos casos em que os seus dispositivos de assinatura são utilizados por terceiros com a sua autorização e de forma legítima, transferindo-se para estes as respetivas obrigações e responsabilidades. Ficam ressalvados, porém, os casos de representação, que a própria definição legal exceciona.

Tendo em vista assegurar que nesses casos em que terceiros utilizam legitimamente os dispositivos de assinatura eletrónica do respetivo titular, a LMAE concentra a definição do conceito na pessoa desses utilizadores, acrescentando que a

[845] A explicação é dada no seguinte trecho: *"The Working Group was nevertheless of the view that the notion of signatory for the purposes of the uniform rules could not be severed from the person or entity that actually generated the electronic signature, since a number of specific obligations of the signatory under the uniform rules were logically linked to actual control over the signature creation data"*. "A/CN.9/483", par. 86.

definição abrange as situações em que eles agem em seu próprio nome e também as situações em que agem em representação de outrem.[846]

Este problema da diferenciação entre o titular da assinatura e a pessoa que, em concreto, aplicou os dados de assinatura sobre um documento só se coloca nas assinaturas de pessoas singulares, nos casos em que não se trata de assinaturas qualificadas, nos termos do art.º 6,º da LMAE, dado que é pressuposto essencial destas que os dados de criação de assinatura sejam exclusivamente do signatários e, além disso, estejam sob o seu controlo exclusivo.

De qualquer forma, parece-nos que teria sido preferível que a definição do conceito de assinante fosse dirigida ao titular do dispositivo de assinatura e sobre ele se centrassem as obrigações e as responsabilidades correspondentes, sem prejuízo de essas responsabilidades se poderem alargar a todas as pessoas que possam agir em sua representação.[847]

Este nosso entendimento parece ter sido seguido pelas legislações posteriores à LMAE, embora a Diretiva 1999/93/CE, define signatário de forma em tudo idêntica.[848]

A lei portuguesa da assinatura eletrónica de 1999 não contém a definição de signatário, mas a alteração efetuada em 2003 veio acrescentar uma definição de "titular de assinatura", centrado na pessoa que o certificado indica como sendo a detentora do dispositivo de criação da assinatura.[849]

O Regulamento EIDAS contém apenas uma definição de signatário, como a "*pessoa singular que cria uma assinatura eletrónica*"[850], sendo que se aplica, quanto ao resto, o regime de vinculação aplicável para cada tipo de assinatura, nomeadamente em matéria de acesso e detenção exclusiva dos dispositivos da sua criação. Deste modo, para o Regulamento, o signatário é o titular do dispositivo de criação da assinatura

---

[846] *"In order to cover situations where the signatory would be acting in representation of another person, the phrase "or on whose behalf" or another equivalent phrase, should be retained in the definition of "signatory""*. "A/CN.9/483", par. 86.

[847] Aliás é o próprio Grupo de Trabalho da LMAE que concorda em que normalmente, nos casos em que a pessoa que executa os atos materiais de aplicação dos dados de assinatura sobre um documento eletrónico não é o respetivo titular, de pouco interessa o conhecimento da sua identidade, até porque ela não será do conhecimento dos eventuais terceiros que confiam, bem como dos destinatários do documento. *"There may be situations where the identity of the person who actually generates the signature, where human action is required, is not relevant for the purposes for which the signature was created"*. "A/CN.9/WG.IV/WP.88", par. 101.

[848] O n.º 3 do artigo 1.º define signatário do seguinte modo: *"«Signatário», uma pessoa singular que detém um dispositivo de criação de assinaturas e o utiliza em seu próprio nome, ou em nome da pessoa singular ou coletiva ou da entidade que representa"*.

[849] Alínea r) do artigo 2.º do DL n.º 290-D/99, de 2/8, com a redação do DL n.º 62/2003, de 3/4: *"«Titular» a pessoa singular ou colectiva identificada num certificado como a detentora de um dispositivo de criação de assinatura"*.

[850] N.º 9 do artigo 3.º.

eletrónica e é ele que a cria. E embora o Regulamento preveja a possibilidade de as assinaturas serem geradas em nome do signatário, nos pontos 3 e 4 do Anexo II, essa geração e efetuada na condição de o signatário possuir o controlo de todo o processo, pelo que ele se mantém sempre como signatário.

O mesmo raciocínio se aplica aos instrumentos de autenticação eletrónica dos documentos pelas pessoas coletivas, que são os selos eletrónicos, como estabelece o n.º 1 do artigo 39.º do Regulamento, sendo que o criador do selo é sempre a pessoa coletiva que vincula, como analisamos de seguida.

2.1. A assinatura eletrónica de pessoas coletivas. Os selos eletrónicos.

O direito das assinaturas eletrónicas nasceu para corresponder a uma necessidade de segurança jurídica na utilização dos meios eletrónicos nas atividades comerciais. É uma necessidade fundamental do comércio eletrónico, onde uma parte significativa dos negócios jurídicos é efetuada entre pessoas coletivas. E se muitos contratos são efetuados com base em declarações verbais, sem outro formalismo, nos meios eletrónicos não existem declarações verbais, porque tudo assenta em dados que se comunicam. Quer as partes pretendam formalizar um negócio jurídico, quer não, existem sempre dados, porque sem eles não existe comunicação. Ora, se nas declarações verbais pode ser fácil autenticar a voz, porque conhecemos o interlocutor, nos meios eletrónicos o problema da autenticação dos dados é sempre igual.

Esses dados podem ser autenticados mediante mecanismos com elevado grau de fiabilidade, como são as assinaturas digitais, adicionados de outros instrumentos de segurança, como é o caso da sua qualificação. E essa autenticação, que garante a origem dos dados, bem como a identificação de quem os emitiu, sendo um dispositivo que consistem num objeto, tanto pode pertencer a uma pessoa física como a uma pessoa coletiva. Dado que muitas relações de natureza comercial se estabelecem entre pessoas coletivas, a assinatura eletrónica passou a ser utilizada pelas pessoas coletivas.

As assinaturas eletrónicas tornaram possível que as pessoas coletivas assinassem documentos eletrónicos. Essa possibilidade, que não tem paralelo nos documentos em papel, resulta do facto de a assinatura eletrónica ser o resultado de um procedimento de aplicação de um objeto sobre um documento eletrónico e de esse

objeto ter uma identidade própria, diferente da do seu titular.[851] O dispositivo do qual constam os dados de criação da assinatura eletrónica de uma determinada pessoa, seja ela singular ou coletiva, pode ser utilizado de forma legítima por uma terceira pessoa devidamente habilitada para tal, como anteriormente vimos. É possível que uma entidade prestadora de serviços de certificação emita pares de chaves e certificados de assinatura eletrónica a pessoas coletivas. Quando os dados de assinatura eletrónica de uma pessoa coletiva são aplicados a um documento eletrónico, eles vinculam juridicamente essa pessoa ao conteúdo do documento assinado. O ato material de aplicação dos dados de assinatura ao documento terá que ser efetuada por uma pessoa física, que esteja habilitada com os poderes correspondentes, mas a assinatura será, nesse caso, sempre da própria pessoa coletiva.

Este procedimento de vinculação de pessoas coletivas a documentos eletrónicos, sendo novo, não é, porém, o único. A outra forma de vinculação das pessoas coletivas a documentos eletrónicos pode seguir a via tradicional, de a assinatura em nome da pessoa coletiva ser efetuada por um representante legal agindo em seu próprio nome, utilizando o seu próprio dispositivo de assinatura eletrónica, mas no exercício dos seus poderes de representação da pessoa coletiva.

Nem a LMAE nem a legislação da assinatura eletrónica de cada país devem interferir com os regimes legais de representação das pessoas coletivas nas respetivas ordens jurídicas, seguindo o princípio da inalteração do direito pré-existente. A definição do conceito de assinante da LMAE, estabelecendo que se trata da *"pessoa que possui os dados de criação da assinatura …"*[852] não limita a definição às pessoas singulares, abrangendo também as pessoas coletivas, naturalmente.[853] Do mesmo modo, todas as referências aos titulares de dispositivos de assinatura adotam a mesma regra.[854]

---

[851] Esta diferença entre as assinaturas manuscritas e as assinaturas eletrónicas, que permite que as pessoas coletivas possam assinar diretamente documentos eletrónicos, era reconhecida nos trabalhos preparatórios da LMAE. *"The analogy to hand-written signatures, it was stated, was in principle acceptable, but might not always be suitable for taking advantage of the possibilities offered by modern technology. In a paper-based environment, for instance, legal entities could not strictly speaking be signatories of documents drawn up on their behalf, because only natural persons could produce authentic hand-written signatures"*. "A/CN.9/483", par. 85.

[852] Alínea d) do artigo 2.º da LMAE, que anteriormente citamos.

[853] A possibilidade de a LMAE regulamentar a assinatura eletrónica das pessoas coletivas foi ponderada nos trabalhos preparatórios e chegou a existir o projeto de uma norma nesse sentido, que veio a ser eliminada, passando, em contrapartida, a definição de assinante a ser genérica, de modo a incluir as pessoas coletivas. *"Distinguishing between legal and natural persons for the purposes of digital signatures was inappropriate in view of the fact that no such distinction was made in the Model Law, where the notion of "person" covered both natural and legal persons"*. "A/CN.9/437", par. 115.

[854] É o caso, por exemplo, do artigo 6.º que estabelece os requisitos de fiabilidade de uma assinatura, bem como do artigo 8.º, relativo às obrigações do titular da assinatura.

Os dispositivos de assinatura eletrónica de pessoas coletivas são utilizados particularmente nas transações eletrónicas automatizadas, entre sistemas informáticos. Muitas transações são atualmente efetuadas de forma repetida e massificada, sem intervenção humana imediata, apenas mediante a interação entre sistemas informáticos, devidamente programados pelos respetivos responsáveis para esse fim. Essas transações possuem relevância jurídica e a aplicação da assinatura eletrónica, mesmo que efetuada também de forma automatizada pelos sistemas informáticos de cada pessoa coletiva interveniente, é o instrumento jurídico de vinculação, para além de ser, ao mesmo tempo, um instrumento essencial de segurança para as partes se protegerem contra a intrusão de terceiros ou contra a atividade ilícita da outra parte.

Por outro lado, nas comunicações eletrónicas entre empresas, efetuadas através de redes abertas, os dispositivos de assinatura eletrónica da respetiva pessoa coletiva são também utilizados como instrumento para garantir a confidencialidade das transações efetuadas.[855]

Finalmente os dispositivos de criação de assinaturas eletrónicas são indispensáveis para garantirem a segurança nas transações eletrónicas efetuadas entre consumidores e pessoas coletivas, através dos *sites* destas na Internet. Para que essas transações vinculem juridicamente a entidade proprietária do *site*, é necessário que este esteja certificado com um dispositivo de autenticação que garanta aos respetivos clientes que estão a operar com a pessoa coletiva que é sua proprietária, e não com alguém que se está a fazer passar por ela de forma ilícita.

Na atual economia digital, a realização de operações comerciais através dos *sites* das empresas, adquire uma importância crescente, substituindo progressivamente o tradicional comércio a retalho em estabelecimentos comerciais. Mas enquanto neste comércio tradicional a segurança das transações é dada pelo pagamento imediato e pela

[855] Nestes casos, o carácter automatizado das transações implica que a aplicação dos dados de assinatura eletrónica da empresa seja efetuado de forma também automática pelos sistemas informáticos. Para isso é necessário instalar no computador, o respetivo dispositivo e, mediante programação, estabelecer os casos e as regras em que esse sistema procederá à colocação da assinatura eletrónica de determinado documento, mensagem ou conjunto de dados. Nos trabalhos da LMAE considerou-se que nesse caso o sistema informático é uma entidade diferente da empresa, mas essa ficção de identidade do sistema, diferente da empresa faz pouco sentido em nosso modo de ver. O sistema informático de uma empresa, que executa atos materiais em função da sua programação, não faz mais do que aplicar a vontade dessa entidade, nos termos exatos em que essa programação foi determinada e estabelecida pelas entidades que exteriorizam a vontade dessa entidade. *"Another example may be found in business applications such as the one where the signature device exists on a network and is capable of being used by a number of people. In that situation, the network would presumably relate to a particular entity which would be the signatory and maintain control over the signature creation device"*. "A/CN.9/WG.IV/WP.86/Add.1", par. 23.

presença física das partes, no comércio eletrónico efetuado em operações diretas entre os consumidores e os *sites* das empresas comerciantes, pressupõe sempre uma autenticação de ambas as partes. Para segurança da empresa vendedora é indispensável a autenticação do consumidor que demanda os seus serviços através da Internet, mas para o consumidor é também indispensável a segurança de que está a operar efetivamente com a empresa que é titular do *site*.[856] Essa segurança só é conferida mediante a verificação do certificado do *site*, que deve dele constar, e que é emitido por uma entidade certificadora, utilizando um certificado de assinatura eletrónica.[857]

Mas a possibilidade de existência de dispositivos de assinatura eletrónica de pessoas coletivas coloca diretamente a questão da forma da expressão da vontade destas, uma vez que essa vontade se forma e se exprime através dos seus órgãos e dos respetivos titulares com poderes de representação. Por essa razão, nos casos em que são comunicados documentos eletrónicos ou dados entre empresas, mediante a operação automática dos seus sistemas informáticos, coloca-se sempre a questão de saber se esses sistemas podem vincular juridicamente as pessoas coletivas respetivas.

A mesma questão se coloca nos casos em que os clientes das empresas operam com os seus *sites* e realizam, através deles, operações com relevância jurídica. Também nesses casos as interações são provocadas pelos clientes, sendo que a interação se efetua com um sistema informático que pode emitir documentos com valor jurídico.

Em ambos os casos, os documentos gerados pelos sistemas informáticos das empresas refletem a sua vontade negocial, dado que os respetivos sistemas informáticos repetem os procedimentos para que foram programados pelos órgãos internos das empresas com poderes para as vincular juridicamente.[858]

---

[856] O reconhecimento desta necessidade de autenticação dos sítios da Internet foi expresso ainda recentemente pela UNCITRAL. *"In many electronic transactions conducted via a website, for example, there is a need to verify the identity of a website owner to ensure that the website belongs to and is managed by the entity that purports to operate it"*. A/CN.9/854, 5 May 2015, par. 11.

[857] Esta questão da certificação dos *sites* era entendida como de escassa relevância nos trabalhos preparatórios da LMAE. Num relatório apresentado em janeiro de 2000, exemplificavam-se essas situações com desprovidas de relevância jurídica. *"Certificates or electronic signatures sometimes used in practice were not always intended to be legally relevant. The example was given of situations where an electronic signature would be used for authenticating a browser"*. "A/CN.9/483", par. 79. Nos dias de hoje as transações efetuadas através de *sites*, quer de natureza comercial, quer administrativa, revestem-se de elevada importância, não só pela sua abrangência cada vez maior, como também pelos valores que envolvem, como ainda pela sua própria natureza. A segurança jurídica nessas transações é essencial para o seu crescimento, dado que a simulação de um site de uma empresa para fins ilícitos é relativamente simples. Por essa razão, a utilização dos certificados de assinatura eletrónica para garantir aos utilizadores a genuinidade do site e a certeza de que as transações que efetuarem através dele vinculam a empresa respetiva, é muito importante.

[858] A LMAE não contém nenhuma disposição específica que preveja a assinatura eletrónica de pessoas coletivas, que chegou a existir em projeto, exatamente para que ela não pudesse ser entendida como

A Diretiva 1999/93/CE, não regula especificamente as assinaturas eletrónicas de pessoas coletivas, mas prevê a sua existência, na definição do conceito de signatário, onde alarga o conceito às pessoas que assinam documentos em seu nome ou em representação de pessoas singulares e coletivas. Esta previsão admite a possibilidade de uma assinatura de pessoas coletivas, que terá que ser criada por ação de um seu representante.[859] Essa possibilidade está também prevista nos requisitos de identificação que a diretiva enuncia para a identificação dos titulares da assinatura eletrónica pelos prestadores de serviços de certificação.[860]

A lei portuguesa também previa implicitamente a assinatura eletrónica de pessoas coletivas, mas sem qualquer regime específico.[861] Esta previsão, sem regulamentação específica era comum à legislação prévia à diretiva europeia de 1999.[862]

A lei espanhola de 2003 desenvolve, de forma inovadora, o regime das assinaturas eletrónicas de pessoas coletivas, estabelecendo, nomeadamente, que cabe aos seus representantes legais ou voluntários a emissão do pedido de geração dos pares de chaves e dos certificados, a custódia do respetivo dispositivo de criação da assinatura.

A lei espanhola estabelece que esse tipo de assinaturas pode ser utilizado nas relações da pessoa coletiva com as administrações públicas, bem como com outras entidades privadas, mas apenas no exercício do seu objeto social.[863]

O Regulamento EIDAS veio alterar o paradigma das assinaturas eletrónicas das pessoas coletivas, abandonando esse conceito e reservando-o apenas para as pessoas singulares. Para isso, na própria definição do conceito de assinatura eletrónica,

---

contendente com o regime da representação legal das pessoas coletivas. *"It was decided, however, that draft article 6 should be deleted, since it might be seen as inappropriately interfering with other bodies of law (e.g., the law of agency, and the provisions of company law dealing with representation of companies by natural persons)"*. "A/CN.9/446", par. 86.

[859] O n.º 3 do artigo 2.º da Diretiva 1999/93/CE, de 13/12/1999, define signatário do seguinte modo: *"uma pessoa singular que detém um dispositivo de criação de assinaturas e o utiliza em seu próprio nome, ou em nome da pessoa singular ou colectiva ou da entidade que representa"*.

[860] A alínea d) do Anexo II estabelece a seguinte obrigação dos prestadores de serviços qualificados: *"d) Verificar, através dos meios adequados e de acordo com a legislação nacional, a identidade e, se for caso disso, os atributos específicos da entidade ou pessoa singular ou colectiva à qual é emitido um certificado qualificado".*

[861] Essa previsão constava do n.º 2 do artigo 7.º, que estabelecia que a assinatura só se podia referir a uma pessoa "singular ou colectiva".

[862] Também a lei espanhola da assinatura eletrónica de 1999 previa as assinaturas eletrónicas de pessoas coletivas, em especial na própria definição do conceito de signatário, e na possibilidade de as pessoas coletivas se relacionarem por via eletrónica com as administrações públicas, bem como no conteúdo dos certificados qualificados, quando se trate de assinaturas de pessoas coletivas. Respetivamente alínea c) do artigo 2.º, n.º 3 do artigo 5.º e alínea f) do n.º 1 do artigo 8.º, todos do *"Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica"*.

[863] Artigo 7.º da *"Ley 59/2003, de 19 de diciembre, de firma electrónica"*.

estabelece-se é o instrumento que é utilizado pelo "*signatário para assinar*", acrescentando-se que "*signatário*" é a pessoa singular que assina.[864]

Esta limitação do conceito não significa que o legislador do Regulamento entenda que não possam existir meios de autenticação eletrónica para os documentos ou para os dados emitidos por pessoas coletivas. Para isso é criada a figura jurídica dos selos eletrónicos, cujas funções são as mesmas das assinaturas eletrónicas. Do mesmo modo, os procedimentos técnicos que se utilizam nos selos eletrónicos são em tudo idênticos aos das assinaturas eletrónicas. E como o seu regime jurídico é também idêntico no Regulamento EIDAS, podemos dizer que se trata mais de uma questão semântica do que de conceitos e de regimes jurídicos. Os selos eletrónicos são instrumentos jurídicos de autenticação de dados eletrónicos gerados por pessoas coletivas, do mesmo modo que as assinaturas eletrónicas o são para as pessoas singulares.

2.2. A assinatura eletrónica de entidades públicas

Os órgãos da administração pública utilizam no procedimento administrativo os suportes eletrónicos, de modo idêntico às empresas, tanto no que respeita à receção de documentos eletrónicos como ao seu envio, nomeadamente através de notificações eletrónicas, como ainda à utilização de *sítios web*, à troca de informação com outros órgãos e à tramitação dos procedimentos administrativos.

Do mesmo modo a tecnologia da assinatura eletrónica é importante para a realização de transações com salvaguarda do sigilo nas comunicações.[865]

As decisões proferidas nos procedimentos administrativos são tomadas pelos titulares dos órgãos que são competentes, e serão esses titulares que assinam, com a sua

[864] O n.º 10 do artigo 3.º define assinatura eletrónica como "*os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar*". O n.º 9 define signatário como "*a pessoa singular que cria uma assinatura eletrónica*". Limita-se, assim, às pessoas singulares a utilização da assinatura eletrónica.

[865] A possibilidade de os órgãos das administrações públicas serem titulares de dispositivos de assinatura eletrónica foi analisada e consensualizada nos trabalhos preparatórios de elaboração da LMAE. *"Electronic signatures, in turn, could be conceived so as to be attributable to companies, or other legal entities (including governmental and other public authorities)"*. "A/CN.9/483", par. 85. E mais adiante é apresentado um exemplo de utilização dos meios de autenticação eletrónica como instrumento de incremento da eficiência pela administração pública: *"Recent measures to improve and modernize domestic tax collection and administration systems in some jurisdictions were already taking advantage of that possibility by assigning signature creation data to legal entities, rather than to the individuals acting on their behalf"*. *Ibidem, idem.*

assinatura eletrónica pessoal, as respetivas decisões. No entanto, essas assinaturas devem identificar esse titular, o órgão e o cargo que exerce, não devendo ser utilizada a assinatura privada que eventualmente essa pessoa possua.

A LMAE não regula a utilização da assinatura eletrónica nos procedimentos administrativos, mas admite a possibilidade de as pessoas coletivas de direito público serem titulares de assinatura eletrónica como qualquer pessoa, bem como de os titulares dos órgãos da administração pública utilizarem a assinatura eletrónica na autenticação dos documentos que suportam os atos que praticam.[866] Essa possibilidade é admitida no próprio texto do Guia de Transposição da LMAE.[867]

A Diretiva 1999/93/CE previa a utilização das assinaturas eletrónicas pela administração pública no seu preâmbulo, tanto no interior dos respetivos órgãos, como nas relações entre eles, como ainda nas relações que estabelecem com os administrados.[868]

Para isso, a diretiva previa a existência dos chamados certificados de atributos, que são certificados de assinatura eletrónica de uma pessoa determinada, que age no cumprimento de uma missão específica, como é o caso dos titulares de órgãos da administração pública com competência para a prática de determinados atos. Nesses casos o certificado utilizado deve ser específico para a prática desses atos e deve identificar o órgão, o titular e o cargo que desempenha e no âmbito do qual pratica o ato.[869]

A diretiva admitia também que os Estados Membros submetessem a utilização da assinatura eletrónica pelos serviços públicos a requisitos especiais, desde que fossem

---

[866] Embora se considerasse que a especificação dos termos da utilização da assinatura eletrónica nos procedimentos administrativos, seria matéria regulada pela legislação interna de cada país.. *"In particular, the Uniform Rules do not deal with aspects of public policy, administrative law, consumer law or criminal law that may need to be taken into account by national legislators when establishing a comprehensive legal framework for electronic signatures"*. "A/CN.9/WG.IV/WP.84", par. 15.

[867] *"While the focus of the Model Law is not on the relationships between users of electronic signatures and public authorities, the Model Law is not intended to be inapplicable to such relationships"*. "A/CN.9/WG.IV/WP.88", par. 89.

[868] O parágrafo 19.º dos considerandos prévios à diretiva enunciava o seguinte: *"As assinaturas eletrónicas serão utilizadas no sector público no âmbito das administrações nacionais e comunitárias e nas comunicações entre essas administrações, assim como com os cidadãos e os operadores económicos, por exemplo em contratos públicos, em matéria de sistemas de fiscalidade, de segurança social, de saúde e judiciário;"*.

[869] A menção dos atributos é obrigatória nos certificados qualificados, como consta do Anexo I da Diretiva: "*Uma cláusula para a inclusão, se relevante, de um atributo específico do signatário, segundo os objectivos visados com a emissão do certificado"*.

objetivos, transparentes, proporcionais e não discriminatórios, não devendo também constituir um entrave à interoperabilidade no seio da UE.[870]

Nessa linha, a lei portuguesa prevê que as administrações públicas possam emitir documentos eletrónicos, desde que autenticados por assinatura eletrónica qualificada, devendo essa certificação ser efetuada nos termos do Sistema de Certificação Eletrónica do Estado.[871] A lei tem também o cuidado de obrigar a que os documentos eletrónicos identifiquem sempre a entidade que os autentica, o titular do órgão e a respetiva função, em especial quando se trate de atos administrativos.[872]

O Regulamento EIDAS reserva para as pessoas singulares as assinaturas eletrónicas, mas cria os selos eletrónicos para a autenticação de documentos emitidos por pessoas coletivas, com as mesmas funções das assinaturas eletrónicas. Os selos eletrónicos são também instrumentos de autenticação de dados e de documentos gerados por organismos públicos, de acordo com o atrigo 37.º do Regulamento.

O Regulamento estabelece, de forma imperativa, que o regime de interoperabilidade e de reconhecimento mútuo das assinaturas eletrónicas e dos selos eletrónicos de aplicam plenamente na autenticação dos documentos e dos dados que os administrados comunicam aos organismos administrativos.

Tanto os selos eletrónicos utlizados por pessoas coletivas que se relacionem com organismos administrativos como as assinaturas eletrónicas, tratando-se de pessoas físicas, quando sejam qualificados, devem sempre ser aceites como instrumentos de autenticação por esses organismos públicos. E essa obrigatoriedade aplica-se independentemente da localização do prestador de serviços que emitiu os respetivos certificados. Assim o estabelecem os artigos 27.º e 37.º do Regulamento respetivamente para as assinaturas eletrónicas e para os selos eletrónicos.

Do mesmo modo, quando os organismos públicos exijam apenas assinaturas eletrónicas avançadas, devem aceitar sempre os documentos e os dados que as pessoas físicas ou coletivas lhes enviam, quando estejam autenticados com assinaturas eletrónicas ou selos eletrónicos avançados, bem como quando o estejam por assinaturas eletrónicas qualificadas ou selos eletrónicos qualificados.

---

[870] Trata-se do n.º 7 do artigo 3.º da Diretiva ".

[871] Este sistema foi criado pelo DL n.º 116-A/2006, de 16/6, e cria a PKI do Estado. O sistema cria uma entidade certificadora do estado, que é o CEGER e uma entidade credenciadora, que é a Autoridade Nacional de Segurança (respetivamente n.º 2 do artigo 6.º e artigo 8.º).

[872] Artigo 5.º do DL n.º 290-D/99, de 2/8.

Estabelece-se assim um regime mais amplo de interoperabilidade entre os Estados Membros, quando a entidade que recebe os dados é um organismo administrativo, justificando-se esse facto pela circunstâncias de muitos organismos públicos utilizarem apenas assinaturas eletrónicas avançadas como instrumento de autenticação nos seus sistemas eletrónicos internos.[873]

E embora o Regulamento estabeleça que não se aplica aos serviços de confiança utilizados exclusivamente dentro de sistemas fechados, nos termos do n.º 2 do artigo 2.º, ele obriga os organismos públicos a aceitarem sistemas de autenticação de quem se relaciona com esses organismos por via eletrónica.[874]

Esta exclusão dos sistemas fechados só opera nos casos em que esses sistemas não operem com terceiros e sirvam exclusivamente para os procedimentos internos dos, neste caso de organismos públicos, dado que o Regulamento impõe que se trate de sistemas fechados. Mas trata-se de uma exclusão problemática, dado que, tratando-se de órgãos da administração pública, mesmo os procedimentos internos possuem relevância jurídica, nomeadamente quando se trate de procedimentos administrativos. Desenvolveremos esta problemática no Capítulo V, na parte relativa ao procedimento administrativo eletrónico.

A garantia da eficácia do reconhecimento mútuo e da interoperabilidade das assinaturas eletrónicas e dos selos eletrónicos no que respeita às transações com as administrações públicas é ainda defendida mediante a proibição da exigência de níveis de garantia superiores aos dos selos qualificados ou das assinaturas eletrónicas qualificadas (n.º 3 do artigo 27 e n.º 3 do artigo 37.º). Estão assim os Estados inibidos de estabelecer exigências de garantia superiores aos qualificados, quando se trate de uma utilização transfronteiriça. Estas normas não impedem os Estados Membros de exigirem esses níveis de garantia superiores aos serviços qualificados para as operações internas, mas mesmo que isso aconteça, tratando-se de utilizações transfronteiriças, essas exigências não são aceites. Admite-se, assim, uma discriminação positiva a favor dos utilizadores desses sistemas situados noutro Estado Membro, mas essa é uma consequência da necessidade de garantir um nível de interoperabilidade eficaz e que não seja vulnerável a procedimentos dos Estados tendentes a diminui-la.

[873] O regime de utilização das assinaturas eletrónicas avançadas nos organismos públicos foi especificado na Decisão de Execução (UE) 2015/1506 da Comissão, de 8 de Setembro de 2015.

[874] Essa preocupação é expressa no parágrafo 21 dos considerandos prévios ao regulamento, nos seguintes termos: *"Por exemplo, os sistemas que sejam criados em empresas ou administrações públicas para a gestão de procedimentos internos e que recorram a serviços de confiança não deverão ficar sujeitos aos requisitos do presente regulamento"*.

As normas constantes dos artigos 27.º e 37.º do Regulamento respeitam aos serviços em linha disponibilizados pelos órgãos das administrações públicas dos Estados Membros, especialmente através de sítios *web*, e destinam-se a garantir que esses órgãos aceitem que os cidadãos de qualquer Estado Membro utilizem esses sítios, mediante a autenticação de documentos ou dados com assinaturas eletrónicas ou selos eletrónicos. Essa utilização é já viabilizada pelo regime de interoperabilidade da identificação eletrónica. Porém, a especificidade destas normas tem por objeto a autenticação dos documentos que os cidadãos, depois de se identificarem e serem autenticados eletronicamente, necessitem de enviar aos organismos públicos respetivos. Trata-se, portanto, de autenticação de documentos ou de dados, mais do que a mera identificação.

A utilização dos selos eletrónicos pelas administrações públicas é possível, nos termos do Regulamento, como o é para qualquer pessoa coletiva, destinando-se a garantir a autenticidade e integridade dos documentos emitidos pelos respetivos órgãos.

Também é aplicável aos organismos públicos, a previsão da autenticação dos sítios *web*, que conferem segurança aos utilizadores, de que estão a operar com sites dos órgãos competentes das administrações públicas. Esta autenticação é importante, porque impede a fraude que se traduz na simulação desses sites por agentes maliciosos (art.º 45.º do Regulamento).

Do mesmo modo são relevantes as inovações do Regulamento no que respeita à previsão dos selos temporais, que são certificações, emitidas por entidades terceiras, que garantem a data da prática de um determinado ato, incluindo o cumprimento de obrigações, a data e hora de determinada notificação ou diligência, a data de emissão de determinado documento eletrónico. Dada a relevância jurídica do tempo nos procedimentos administrativos, nomeadamente na contagem dos prazos para a prática dos atos, estes instrumentos de certificação possuem elevada importância na sua tramitação. Esta importância é elevada pelo facto de as tecnologias atualmente disponíveis permitirem a automatização de componentes procedimentais meramente instrumentais ou rotineiras, sendo que a contagem dos prazos é uma delas.[875]

Finalmente a previsão dos serviços de envio registado eletrónico, que constituem a base das notificações eletrónicas seguras, mediante os quais entidades terceiras de confiança certificam o envio e a receção de mensagens eletrónicas. Em

[875] O regime dos selos temporais consta dos artigos 41.º e seguintes do regulamento.

linha com a previsão da lei portuguesa de 1999, o Regulamento acrescenta a certificação das entidades terceiras, estabelecendo uma presunção de envio e de receção nos casos em que se utiliza um sistema de envio qualificado, nos termos dos art.ºs 43.º e seguintes.

2.3. A sede eletrónica

Através dos sítios *web* dos agentes económicos realizam-se transações imediatas e automatizadas, em que os clientes das empresas demandam a aquisição de bens ou serviços que lhe são fornecidos ou expedidos de imediato, mediante a operação dos mecanismos automatizados e previamente programados dos sistemas informáticos. Estas operações, designadas transacionais, traduzem-se muitas vezes em contratos celebrados e executados, ou outros negócios e atos jurídicos.

Nas relações administrativas ocorreram fenómenos idênticos, havendo muitos órgãos da administração pública cuja atividade está total ou parcialmente desmaterializada e o relacionamento com os administrados é efetuado, de forma significativa através desses *sites*.

A importância dos *sites* na atividade destas empresas e entidades foi progressivamente formando o conceito de sede eletrónica. Esse conceito é importante para garantir às partes que operam com esses *sites* a segurança acerca da autenticidade e da genuinidade desses locais, bem como a vinculação jurídica das respetivas entidades no que respeita às interações efetuadas através deles.

São também relevantes do conceito de sede eletrónica a determinação da localização das operações realizadas, nomeadamente para se apurar em que país ocorreram, bem como para que esses locais sejam equiparados à sede e à localização dos estabelecimentos e dos serviços para se determinar o local do cumprimento de obrigações, tanto de comunicação como de entrega de documentos, de informação, de petições, etc.[876]

[876] A problemática da determinação da sede eletrónica tem a sua origem na necessidade de determinar a localização dos negócios jurídicos realizados mediante a interação de sistemas informáticos e através de *sites*. Essa questão colocou-se quando começaram a ser utilizados os *sites* para a realização de operações interativas e já não meramente informativas, nomeadamente a venda e compra de bens e serviços através deles. A mesma questão se coloca nos casos em que se realizam negócios e contratos mediante a troca de declarações negociais através de correio eletrónico. Foi em 2003 que se colocou a questão determinar se os nomes de domínio utilizados nos *sites* e nos endereços eletrónicos, referentes ao país de localização dos servidores podiam ser utilizados para a fixação da localização das operações: *"Another related question is the extent to which the address from which the electronic messages were sent could be taken into account to determine a party's location, so that in the case of addresses linked to domain names*

O conceito de sede eletrónica, veio substituir o de sistema informático, dada a relevância jurídica que resulta daqueles conceitos para a realização dos negócios jurídicos. A sede eletrónica pode englobar um *site* de uma empresa ou de um agente económico, o sistema de correio eletrónico e ainda a localização do sistema informático.[877]

Com a entrada em vigor do Regulamento EIDAS,[878] a criação dos instrumentos de confiança jurídica eletrónica da assinatura eletrónica, da autenticação dos sítios *web*, dos selos eletrónicos, dos selos temporais, dos serviços de envio registado eletrónico e da assinatura eletrónica, para além do regime da identificação eletrónica, foram criadas as condições para que praticamente toda a atividade das administrações públicas pudesse ser desenvolvida de forma desmaterializada, em especial nos seus interfaces com os administrados.[879]

Do mesmo modo para as empresas, o quadro legislativo atual proporciona as condições para um crescimento substancial das operações eletrónicas. Neste contexto em que as comunicações eletrónicas ganharam condições para substituírem o relacionamento presencial entre as partes nas relações jurídicas, o conceito de sede eletrónica adquire uma importância relevante, dado que o local de cumprimento das obrigações é um dos elementos determinantes das relações jurídicas.

O conceito da sede eletrónica não existe na lei portuguesa nem no Regulamento EIDAS, mas trata-se de um conceito operativo, dado que os sítios *web* são, em si mesmos locais do cumprimento de obrigações jurídicas pelas partes.

2.4. Responsabilidade dos titulares da assinatura eletrónica

A posse do dispositivo de assinatura e dos instrumentos necessários para assinar documentos eletrónicos, bem como da informação que lhe dá acesso (por

---

connected to specific countries (such as addresses ending with ".at" for Austria, ".nz" for New Zealand, etc.) the party could be presumed to have its place of business in the corresponding country". A/CN.9/WG.IV/WP.104, par. 18.

877 *"The term "electronic address" may, depending on the technology used, refer to a communications network, and in other instances could include an electronic mailbox, a telecopy device or another specific "portion or location in an information system that a person uses for receiving electronic messages""*. A/CN.9/608/Add.3, 22 March 2006, par. 57.

878 Regulamento EIDAS.

879 Como se refere numa publicação da UNCITRAL, *"digitally signed certifi cates are often used, for instance, to "authenticate" servers or websites, for example in order to guarantee to their users that the server or website is the one it purports to be or is genuinely attached to the company that claims to run the server or website"*. UNCITRAL, "Promoting Confidence …". Op. cit., par. 32.

exemplo uma palavra-passe), é suficiente para que qualquer outra pessoa o possa utilizar para assinar documentos em nome do titular da assinatura e com a sua chave privada. Por essa razão, sobre ele recaem um conjunto de deveres de diligência e de medidas de segurança para garantir que nenhum terceiro possa aceder de forma não autorizada a esses instrumentos, sendo certo também, que será ele o principal, embora não o único, beneficiário da sua salvaguarda.[880]

A validade da assinatura depende, desde logo, da legitimidade da posse do dispositivo que a cria e da sua exclusividade, continuada no tempo. A partir do momento em que lhe é entregue pelo prestador de serviços, a garantia da segurança dessa posse e da exclusividade do acesso cabe apenas ao titular.

A LMAE utiliza a formulação jurídica de "*evitar a utilização não autorizada"* do dispositivo de assinatura, estabelecendo assim um dever de cuidado que impende sobre o titular.[881] A formulação é suficientemente aberta para permitir que o titular possa habilitar um terceiro a utilizar em seu nome o seu dispositivo de assinatura, cabendo-lhe, nesse caso, o dever de cuidado para garantir que não ocorra quebra de segurança nessa utilização, pelo qual é ele sempre o responsável.

Casos existem em que um mesmo certificado e dispositivo de assinatura eletrónica podem ser partilhados por várias pessoas. É esse o caso, por exemplo, dos certificados de pessoas coletivas, que servem para autenticar os documentos eletrónicos por elas emitidos.[882] O mesmo ocorre com os selos eletrónicos.

Nestes casos levanta-se a questão de determinar a responsabilidade de cada uma dessas pessoas no caso de não ter sido adotada a diligência necessária a evitar a utilização não autorizada de terceiros. Uma das possibilidades seria a responsabilização solidária de todos, mas essa solução não recebeu cobertura na redação da LMAE. Dado que se trata de uma responsabilidade pela culpa, é necessária uma determinação prévia dessa responsabilidade à pessoa que em concreto não cumpriu os seus deveres de

---

880 *"The signatory is expected to exercise reasonable care to avoid unauthorized use of that signature device"*. "A/CN.9/WG.IV/WP.88", par. 78.

881 Esta formulação da norma é também inspirada nas Guidelines da ABA, que preveem uma obrigação expressa do titular da assinatura, de não adotar comportamentos que comprometam a segurança da sua chave privada, incluindo durante o período em que eventualmente o certificado esteja suspenso (ponto 4.3). *"During the operational period of a valid certificate, the subscriber shall not compromise the private key corresponding to a public key listed in such certificate, and must also avoid compromise during any period of suspension"*. "A/CN.9/WG.IV/WP.84", par. 53.

882 Como se refere no parágrafo 51 dos considerandos do Regulamento, *"Os dispositivos qualificados de criação de assinaturas eletrónicas deverão poder ser confiados a terceiros pelo signatário, desde que sejam aplicados mecanismos e procedimentos adequados para garantir que o signatário tenha o controlo exclusivo da utilização dos dados necessários para a criação da sua assinatura eletrónica e que a utilização do dispositivo cumpra os requisitos da assinatura eletrónica qualificada"*.

diligência.[883] Por outro lado a responsabilidade pela comunicação da utilização indevida ou da sua possibilidade, não é conjunta de todas as pessoas que eventualmente partilhem o acesso a um dispositivo de assinatura eletrónica, mas sim uma responsabilidade pessoal, limitada a cada um dos titulares que especificamente tenha conhecimento desse acesso ou utilização. É esse o sentido da utilização, pela LMAE, dos termos "*cada titular*", bem como da limitação do dever de comunicação às situações em que tenha havido conhecimento desse acesso.[884]

Em segundo lugar, caso tenha ocorrido um acesso indevido ao seu dispositivo, mesmo que não tenha havido uma utilização indevida, devem adotar-se os procedimentos correspondentes que estão previstos na lei ou nas práticas da entidade certificadoras, nomeadamente dando conhecimento dessa contingência a esta entidade para que proceda ao seu cancelamento.[885] A LMAE especifica que esse dever de comunicação só ocorre, neste caso, quando exista conhecimento de que o dispositivo de assinatura esteve acessível a terceiros de uma forma que tenha tornado possível essa utilização. A formulação da norma não contempla a possibilidade de responsabilização do titular do dispositivo nos casos em que, não tendo tido conhecimento daquela vulnerabilização da segurança, devesse, em condições normais, tê-lo tido.[886]

Tendo em conta que a responsabilidade do titular da assinatura se fundamenta num dever de cuidado, que inclui a obrigação da adoção de todos os comportamentos necessários a evitar a utilização indevida do dispositivo, é legítimo que se questione se a obrigação de comunicação não se aplica também nos casos em que tendo ocorrido uma vulnerabilização da segurança de que o titular não teve conhecimento, embora devesse

---

[883] Assim se assumiu nos trabalhos preparatórios. *"e.g., in case of unauthorized use of a corporate signature device held by a number of employees. It was decided that each holder should only be liable to the extent that it had personally failed to meet the requirements in paragraph (1)".* "A/CN.9/465", par. 105.

[884] Essa especificação foi acordada no Grupo de Trabalho: *"The reference to "each" holder has been introduced to reflect the general view that, in certain cases, it might be unfair to provide that each holder of the device was liable for the entire loss that might have resulted from unauthorized use of the device (e.g., in case of unauthorized use of a corporate signature device held by a number of employees)"*. "A/CN.9/WG.IV/WP.84", par. 52.

[885] A LMAE não especifica as responsabilidades dos sujeitos da assinatura eletrónica, estabelecendo apenas uma previsão dos procedimentos que cada um deles deve adotar e consignando que o seu incumprimento será suscetível de os fazer incorrer em responsabilidade. "A/CN.9/WG.IV/WP.88", pág. 9.

[886] Essa possibilidade de responsabilizar o titular por não ter adotado a diligência necessária para ter conhecimento da vulnerabilização das regras de segurança, foi ponderada nos trabalhos da LMAE, mas considerou-se que seria uma exigência excessiva, em face do princípio de que se trata de uma responsabilidade subjetiva. *"The words "or ought to have known" had not been included in draft article 9 on the basis that it would be difficult for the signature holder to satisfy a duty of notification that was based on something it ought to have known, but did not in fact know"*. "A/CN.9/465", par. 103. Do mesmo modo, "A/CN.9/WG.IV/WP.82", par. 51.

tê-lo tido. A LMAE e as normas correspondentes não contemplam esse dever, até por uma razão de praticabilidade, dado que não se pode assinalar um facto de que não se tem conhecimento. Isso não significa, porém, que o titular da assinatura fique isento de responsabilidade, que poderá sempre fundamentar-se no respetivo regime geral.

Este regime de responsabilidade não abrange apenas um dever de diligência contra um resultado, mas também relativamente a um perigo, ou seja, a um risco de ocorrência de um resultado. Ou seja, o dever de comunicação nasce no momento em que o titular tenha tido conhecimento da existência do risco, porque ocorreu uma exposição do dispositivo a uma possibilidade de utilização indevida. É esse o sentido da subalínea b) ii) do n.º 2 do art.º 9.º da LMAE.[887]

A terceira obrigação estabelecida no art.º 8.º respeita ao fornecimento de todos os elementos de identificação à entidade que presta serviços de certificação, para que o certificado que for emitido e o par de chaves que for gerado contenham esses elementos com o rigor necessário. Trata-se de uma obrigação que é correspondente àquela que incide sobre a entidade certificadora, de se assegurar do rigor dessa identificação. A responsabilidade por esta informação vincula simultaneamente o titular da assinatura e a entidade certificadora, dado que se o primeiro tem o dever de proporcionar a informação correta, a segunda tem também o dever de a verificar e confirmar, sendo que tanto uma obrigação como a outra estão expressa na LMAE.[888]

A responsabilidade do titular da assinatura eletrónica tem natureza extracontratual, apesar de os procedimentos que a LMAE lhe consigna serem relativos

---

[887] Esse alargamento da obrigação do titular foi ponderado e refletido na LMAE, constando dos trabalhos preparatório que a responsabilidade do titular , *"covered both cases where the signatory knew that the signature creation data had been compromised and cases where the circumstances known to the signatory gave rise to a substantial risk that the signature data might have been compromised"*. "A/CN.9/483", par. 124.

[888] As Guidelines da ABA, que servem de base a muitas das normas da LMAE, extabelecem essa responsabilização mútua. *"All material representations made by the subscriber to a certification authority, including all information known to the subscriber and represented in the certificate, must be accurate to best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the certification authority"*. A Lei da Assinatura Eletrónica de Singapura adota idêntica redação. Do mesmo modo, quando o titular da assinatura recebe o dispositivo de assinatura eletrónica e o certificado, é responsável por toda a informação que dele consta, sempre que utilizar esse certificado para assinar documentos eletrónicos. Essa responsabilização está expressa, por exemplo, na lei da assinatura eletrónica do Estado do Illinois dos EUA (alínea b) da secção 20-105): *"By accepting a certificate, the subscriber listed in the certificate represents to any person who reasonably relies on information contained in the certificate,in good faith and during its operational period, that: (1) the subscriber rightfully holds the private key corresponding to public key listed in the certificate; (2) all representations made by the subscriber to the certification authority and material to the information listed in the certificate are true; and (3) all information in the certificate that is within the knowledge of the subscriber is true"*. Esta responsabilização mútua é consagrada também na LMAE. "A/CN.9/WG.IV/WP.84", par. 53.

às relações estabelecidas entre esses sujeitos e a entidade certificadora. Tanto os comportamentos de receção e de guarda dos dispositivos de assinatura eletrónica, como de entrega dos elementos dos elementos de identificação, como ainda de comunicação das situações em que terceiros possam ter acesso àquele dispositivo, são do domínio das relações entre o titular da assinatura e a entidade prestadora de serviços de certificação.

Essa natureza relacional não desvirtua, porém, o facto de se tratar de procedimentos cuja finalidade excede o âmbito estrito dessa relação, e os situa no domínio da própria essência do sistema, que é o da perenidade da confiança. E, assim sendo, o sujeito ativo destas obrigações dos titulares das assinaturas eletrónicas são todos os eventuais interessados na verificação dessas assinaturas.[889] São esses os virtuais lesados em caso de violação desses deveres e da eventual produção de prejuízos correspondente.[890]

O Regulamento EIDAS não prevê expressamente qualquer tipo de responsabilidade dos signatários, pelo que se aplicará o regime da responsabilidade civil contratual ou extracontratual, consoante os casos de violação que vierem a ocorrer. Do mesmo modo a Diretiva de 1999 e a lei portuguesa nada refere a esse respeito.

Em nosso entendimento justificar-se-ia a existência de normas que estabelecessem obrigações de cuidado para os titulares das assinaturas eletrónicas, em especial no que respeita à custódia dos dispositivos de criação de assinatura e ao dever de comunicação aos prestadores de serviços, das situações de eventual exposição a terceiros que possam fazer perigar a segurança no seu acesso.[891]

A lei portuguesa estabelece no art.º 31.º do Decreto-Lei n.º 290-D/99, de 2/8, cinco obrigações fundamentais do titular da assinatura:

i) Uma obrigação genérica de tomar todas as medidas necessárias para evitar danos a terceiros;

---

[889] *"Those obligations were owed to either the certification authority or any other party who might rely on a digital signature in the context of contractual relationships with the key holder"*. E mais adiante *"The text of the Uniform Rules should make it clear that the obligations of the key holder should be owed to any party who reasonably relied on the use of a key and suffered a loss as a result of the keyholder's failure to fulfil its obligations"*. "A/CN.9/457", par. 71.

[890] Esse também foi o entendimento consensualmente estabelecido nos trabalhos preparatórios: *"The prevailing view, however, was that the obligations of the key holder were owed to any party who might reasonably rely on a digital signature, irrespective of whether or not that party was linked to the key holder by a contractual relationship"*. "A/CN.9/457", par. 71.

[891] O Regulamento deixou intencionalmente essa matéria para ser regulada pelos estados membros, como refere no parágrafo 53 dos considerandos: *"O presente regulamento não deverá impor aos prestadores de serviços de confiança nem aos Estados-Membros o recurso à suspensão, mas prever regras de transparência quando e onde tal prática existir"*.

ii) Uma obrigação específica de "*preservar a confidencialidade da informação transmitida*";

iii) Comunicar, à entidade certificadora, todas as situações em que pode ter sido colocada em causa a confidencialidade dos dados de criação de assinatura, pedindo a suspensão do certificado;

iv) Nos casos em que se confirme que foi violada a confidencialidade, comunicar esse facto e requerer a revogação do certificado;

v) Não utilizar o dispositivo de assinatura a partir do momento em que efetue a comunicação referida no ponto anterior.

A lei não prevê qualquer consequência jurídica em caso de violação dos deveres anteriormente referenciados, nem em matéria sancionatória, nem de responsabilidade civil, pelo que se aplicará o regime geral desta.

3. As partes que confiam na assinatura eletrónica

As partes que confiam numa assinatura eletrónica são aqueles que designamos como os destinatários dos documentos ou das mensagens eletrónicos. Trata-se, potencialmente, de todos os cidadãos e agentes económicos que pretendam utilizar a chave pública de cada titular de assinatura eletrónica para se certificar, perante uma assinatura, que é o seu autor. Para estes interessados, a credibilidade e a confiança que possuem no prestador de serviços de certificação é essencial para que possam realizar operações com relevância jurídica por via eletrónica.[892] [893]

O art.º 11.º da LMAE estabelece um conjunto de obrigações, também para estas partes, nomeadamente a de se certificarem da validade dos certificados e da fiabilidade da assinaturas dos documentos que recebem.[894]

[892] *"The notion of "relying party" is intended to cover any party that might rely on an electronic signature. Depending on the circumstances, a "relying party" might thus be any person having or not a contractual relationship with the signatory or the certification services provider"*. "A/CN.9/WG.IV/WP.88", par. 145.

[893] *"A relying party is expected to take reasonable steps to verify the reliability of an electronic signature"*. "A/CN.9/WG.IV/WP.88", par. 79.

[894] O artigo 11.º da LMAE. "A/CN.9/WG.IV/WP.88", pág. 11.

Capítulo III – Os efeitos jurídicos da assinatura eletrónica

As assinaturas eletrónicas vieram criar as condições de idoneidade jurídica dos suportes eletrónicos e da própria formação do conceito de documento eletrónico. A existência deste conceito deu origem à formação de outros conceitos externos ao de assinatura, erigidos sobre a base dos documentos eletrónicos. É o caso do conceito de documento escrito eletrónico, do conceito de original, dos efeitos dos documentos eletrónicos em matéria probatória, dos arquivos eletrónicos e da própria utilização dos suportes eletrónicos no procedimento administrativo.

São esses efeitos que analisamos neste capítulo.

1. Documento escrito eletrónico

Nos documentos em papel, as funções da representação escrita são diversas, sendo identificadas como essenciais as seguintes:[895]

i) A legibilidade, quer pelas partes, quer por terceiros. A redução a escrito cristaliza o conteúdo informacional, tornando-o material e objetivo. Isso permite que ele seja apreciado, da mesma forma e com carácter de permanência, no decurso do tempo, por um universo de pessoas mais abrangente que o das partes intervenientes na sua produção;

ii) A integridade. A representação escrita permite detetar eventuais alterações ao longo do tempo e proporcionar segurança no que respeita ao seu conteúdo. A integridade do documento não advém diretamente do seu carácter escrito, mas, nos documentos em papel, não é possível sem ele;

iii) A possibilidade da reprodução e a sua transmissão e comunicação; permitindo assim a transacionabilidade quando os documentos são títulos que incorporam direitos transacionáveis com a sua posse. Também a reprodução do documento não se basta com o seu carácter escrito, mas este é um pressuposto essencial dela;

iv) A autenticação. A representação escrita permite que se evidencie a sua autenticação, mediante a colocação de uma evidência pelo seu autor ou subscritor, representativa da sua vontade de se vincular ao conteúdo do documento. O carácter escrito do documento é um pressuposto essencial, sem ser suficiente, para essa autenticação;

v) É também um instrumento fundamental de prova em juízo ou nos procedimentos administrativos.

vi) A exigência de redução a escrito dos atos ou dos negócios é também um instrumento que a lei utiliza com alguma frequência para que as partes possam refletir e tomarem plena consciência dos atos que praticam e das suas consequências.

A transição do suporte de papel para o eletrónico coloca um conjunto de questões jurídicas relevantes. Os atributos de legibilidade, integridade, reprodução, autenticação e, em suma, de escrito, dos documentos em papel, não se transportam automaticamente para os suportes eletrónicos, em especial pelas seguintes razões:

[895] Seguimos de perto a enunciação das funções de escrita dos documentos, que é feita pela UNCITRAL. "A/CN.9/608/Add.2", par. 5.

i) Não são objetos materiais e unos como o papel, mas processos complexos. A sua apresentação nos écrans dos computadores, com uma aparência idêntica à dos documentos em papel, é apenas uma imagem, resultante de um processo de transformação. Diz-se, por isso, que um documento eletrónico é um documento virtual, desmaterializado;

ii) Não são completos e autónomos, dado que a sua análise depende sempre da operação de sistemas informáticos e de máquinas, e da conversão de dados em documentos legíveis. Nos documentos eletrónicos existe um processo de transformação dos conteúdos informacionais, desde o momento em que foram expressos pelos emitentes, até ao momento em que são apresentados aos destinatários. Esse processo consiste na digitalização da expressão da vontade, na sua gravação, e na sua posterior reprodução em linguagem alfanumérica. Essa reprodução é essencial para que um documento eletrónico se possa considerar como suscetível de produzir efeitos jurídicos.[896]

Os documentos em papel são sempre escritos, e as previsões legais que exigem que determinados documentos se apresentem em forma escrita assentavam sempre no pressuposto da escrita em papel. No paradigma eletrónico o conceito de escrita não é necessariamente o mesmo, pelo que é necessário analisar cuidadosamente se um documento eletrónico pode ser um documento escrito, e se aquilo que a lei designa como escrita se pode aplicar aos documentos eletrónicos.

Na fase anterior às das redes, os documentos eletrónicos eram fundamentalmente as comunicações efetuadas por telégrafo e telex, bem como as cópias em microfilme dos documentos em papel. Considerava-se então que os documentos eletrónicos eram também documentos escritos, sendo essa a razão pela qual não se incluía nos textos da UNCITRAL qualquer previsão definitória do conceito de escrita.[897]

---

[896] Essa possibilidade de reprodução, aparentemente simples, pode não o ser, em face da mudança tecnológica, que torna obsoletos muitos suportes, como é o caso das bandas magnéticas e das disquetes, que já não podem ser lidas pelos computadores mais recentes, porque não vêm dotados dos equipamentos correspondentes. A mais recente tecnologia, permite guardar na chamada "nuvem", praticamente todos os suportes eletrónicos sem necessidade de os transportarmos em computadores ou em discos magnéticos externos. Brevemente os computadores podem ser apenas terminais ligados à Internet, como são os novos telemóveis designados de *smartphones*, que não possuem nenhum equipamento capaz de operar com discos externos.

[897] "A/CN.9/273", pág. 49.

O problema colocou-se quando emergiram as redes fechadas, como o EDI. Pela primeira vez a comunicação passou a poder ser automatizada, diretamente entre os sistemas informáticos do emitente e do destinatário, utilizando apenas a linguagem binária, pelo que praticamente não existia expressão escrita. E a legislação então vigente, quando exigia forma escrita, reportava-se ao suporte de papel, não existindo previsão acerca dos documentos em forma eletrónica.[898]

Os atributos de legibilidade e de durabilidade são essenciais à segurança jurídica[899]. Mas se esses atributos são dados evidentes dos documentos em suporte de papel, eles não decorrem necessariamente dos documentos em suporte eletrónico. Não sendo possível que a tecnologia conferisse esses atributos aos documento eletrónicos, no contexto histórico em que o EDI surgiu, havia necessidade de a sua prossecução ser obtida pela via legislativa, sendo necessário adaptar a legislação ou, então, criar instrumentos jurídicos novos, de forma que se pudessem alcançar esses objetivos.[900]

A metodologia que se seguiu foi a de estabelecer um conjunto de pressupostos legais que uma vez reunidos permitiriam a equiparação a escrito dos suportes eletrónicos.

O primeiro trabalho efetuado a nível internacional nesta matéria foi o Relatório TEDIS, que concluiu que a relevância jurídica dos documentos eletrónicos dependeria sempre da possibilidade de serem lidos e da sua integridade. A LMCE acolheu esse entendimento e o art.º 6.º, sob a epígrafe "escrito", estabelece que se considera que um documento eletrónico cumpre os requisitos de equivalência funcional correspondentes às exigências legais de forma escrita, nos casos em que reúne dois requisitos fundamentais:[901]

---

[898] Centrava-se aqui a principal observação dos que defendiam que neste caso não se cumpria o requisito de escrita das mensagens eletrónicas, porque não existia cópia da informação produzida. *"Some of the authors who favour this view, argue that messages transferred via computer do not satisfy the writing requirement, fundamentally on the grounds that no hard copy is received"*. A/CN.9/WG.IV/WP.91, par. 36.

[899] E são mencionados como tal no relatório: *"To fulfil a function comparable to writing, a computerized record must be capable of being a stable and durable medium - to satisfy the need for perpetuation - and reliable and unalterable to satisfy the need for security"*. "TEDIS Report", pág. 306.

[900] O relatório releva a importância da integridade, da vinculação, da identificação do autor, da sua conservação, reprodução e leitura. *"should require Member States to adapt their law of evidence and their accounting and tax laws(...). In particular, pertain to: - the integrity of the message transmitted and stored (identification of its author, actual addressee, date and content of the message actually transmitted); - the durability of the message, its recording and storage (incorruptibility of the message taken as a whole comprising the identification of its author(...) the possibility of obtaining the recorded data in a reliable (unalterability of the message when reproduced on its readout medium; compliance with program execution instructions, readability and saving of program documentation and instructions) and directly readable form"*. "TEDIS Report", pág. 306.

[901] N.º 1 do artigo 6.º. "Guide to Enactment LMCE (1996)", pág. 5.

i) Da acessibilidade;

ii) Da possibilidade da sua consulta posterior.

Trata-se apenas de equiparação de um documento eletrónico a um documento em forma escrita, em papel. Não se incluem aqui os requisitos de integridade nem de assinatura ou de autenticação, mas apenas de cumprimento do requisito elementar de escrita, um requisito de forma mínimo, sobre o qual se podem depois erigir os restantes.[902]

Ambos os requisitos se centram na função de comunicação e da validade jurídica das mensagens de EDI. A acessibilidade inclui não só a sua legibilidade pelo entendimento humano, como também a possibilidade da sua utilização por sistemas informáticos, quando estes operem automaticamente.[903] A acessibilidade é um conceito funcional de usabilidade, ou seja, a capacidade ser utilizável pelos destinatários.[904]

A possibilidade de posterior consulta é um requisito básico de durabilidade, prévio ao da integridade, que não a pressupõe, mas será dela pressuposto essencial.[905]

Reunindo-se os pressupostos da acessibilidade e disponibilidade para posterior consulta e usabilidade, produz-se a equivalência funcional a documento escrito, sendo este um pressuposto de base para que sobre ele operem as funções de legibilidade, integridade, reprodução, autenticação, arquivo e prova, nomeadamente mediante assinatura. Tal como nos documentos em papel, estas funções não advêm diretamente

---

[902] É também desta forma que a norma é entendida: *"Thus, when adopting a functional approach, attention should be given to the fact that the requirement of a "writing" should be considered as the lowest layer in a hierarchy of form requirements, which provide distinct levels of reliability, traceability and unalterability with respect to paper documents". Idem*, par. 49.

[903] A acessibilidade consiste tanto na possibilidade da sua leitura humana, como de tratamento automatizado pelos sistemas informáticos. *"The use of the word "accessible" is meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained"*. "Guide to Enactment LMCE (1996)", par. 50. É esse o sentido do projeto de artigo 8.º atualmente em discussão, que tem a seguinte redação: *"Where the law requires that information should be in writing or provides consequences for the absence of a writing, that requirement is met with respect to the use of an electronic transferable record if the information contained therein is accessible so as to be usable for subsequent reference"*. "A/CN.9/WG.IV/WP.130", par. 44.

[904] Na conceção dos títulos transferíveis eletrónicos, considera-se que a acessibilidade à informação é o elemento essencial para a equivalência a escrita, quando ela proporcione as condições para poder ser utilizada para posterior consulta. *"it would be sufficient to state that the written form requirement was met when information contained in or related to the electronic transferable record was accessible so as to be usable for subsequent reference"*. "A/CN.9/797", par. 37.

[905] Nos trabalhos preparatórios da UNCUECIC acrescentou-se ao universo das funções de escrita, as de cristalização e constância da vontade expressa, de permitir o seu arquivo e a sua persistência no futuro, o controlo e auditoria pelas entidades de inspeção, nomeadamente para efeitos fiscais, contabilísticos ou outros, e também para garantir a validade dos atos nos casos em que a lei exija a forma escrita. "A/CN.9/608/Add.2", par. 16.

da equivalência a escrito dos documentos, mas do cumprimento dos requisitos dessa equivalência.[906]

A equivalência dos documentos eletrónicos a documentos escritos, com idênticos requisitos, foi também regulada pela UNCUECIC.[907] Esses requisitos inspiram também o Convénio da Cidade do Cabo.[908]

A lei portuguesa da assinatura eletrónica faz equivaler os documentos eletrónicos a documentos em forma escrita, apenas nos casos em que *"o seu conteúdo seja susceptível de representação como declaração escrita"*.[909] Trata-se de uma norma inspirada na LMAE, dado que não existe norma idêntica na Diretiva de 1999 nem noutras legislações, nomeadamente a espanhola e a alemã.

A diretiva de 1999 da UE não define o conceito de documento eletrónico, mas a definição de assinatura eletrónica como um conjunto de dados associados a outros dados, pressupõe a conceção de que estes segundos são o documento. Em simultâneo, a equivalência funcional entre as assinaturas qualificadas e manuscritas exigidas por lei, estabelece que as assinaturas eletrónicas cumprem, relativamente aos dados em forma digital, os mesmos efeitos das assinaturas manuscritas relativamente aos dados escritos (alínea a) do n.º 1 do art.º 5.º. Esta equivalência é suficiente, pelo que a diretiva abandonou o requisito da representação como forma escrita dos documentos eletrónicos, que apesar disso subsiste na lei portuguesa.

O Regulamento EIDAS estabelece um conceito próprio de documento, nele incluindo os documentos escritos, em forma de texto, as gravações sonoras, visuais, audiovisuais, numa formulação aberta e exemplificativa, sem exigir representação como declaração escrita, mas que está implícita no formato de texto.[910] Essa exigência nem seria razoável, dada a abrangência dos tipos de documentos eletrónicos a dados que nem sequer podem ser visualizados em forma de texto, porque não o são.

---

[906] *"The requirement that data be presented in written form (which can be described as a "threshold requirement") should thus not be confused with more stringent requirements such as "signed" writing", "signed original" or "authenticated legal act"*. "A/CN.9/608/Add.2", par. 17.

[907] O n.º 2 do artigo 9.º da UNCUECIC tem a seguinte redação: *"Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference"*. "UNCUECIC", pág. 5.

[908] *"A (the "Cape Town Convention") which provided that writing meant "a record of information (including information communicated by teletransmission) which is in tangible or other form and is capable of being reproduced in tangible form on a subsequent occasion and which indicates by reasonable means a person's approval of the record""*. "A/CN.9/546", par. 51.

[909] Nº 1 do artigo 3.º do DL n.º 290-D/99, de 2/8.

[910] N.º 35.º do artigo 3.º: *"«Documento eletrónico»: qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual"*.

Trata-se de um conceito abrangente, dado que a norma contém uma parte enunciativa abrangente, seguida de uma parte meramente exemplificativa. Da primeira parte resulta que o legislador do Regulamento entende que um documento é um conteúdo que se encontra armazenado. Podemos dizer que se trata de um conceito composto de dois elementos fundamentais, sendo um relativo ao significado e outro ao suporte. Relativamente ao primeiro, não se exige qualquer qualificação do conteúdo, pelo que se trata de qualquer significante que se reporte ou represente um qualquer significado.[911] Não exige o Regulamento que o documento seja suscetível de qualquer utilização nem efeito, bastando o facto de se tratar de um conteúdo. Porém, um conteúdo deve ser sempre portador de um significado, pelo que se deve tratar de um conteúdo semiótico, capaz de representar um significado ou de um sentido, sem que seja necessário outra qualquer especificação desse sentido, e independentemente da utilização a que possa dar lugar.

No que respeita ao suporte, um documento carateriza-se pela sua capacidade de autonomamente representar o conteúdo, de o preservar e de o transportar no tempo.

Daqui resulta que o conceito de documento eletrónico é mais abrangente que o de documento em papel, dado que, ao contrário das comunicações e das declarações verbais, cujo suporte se volatiliza de imediato, nas relações estabelecidas por meios eletrónicos, que são sempre operadas mediante transmissão de dados, existe sempre um suporte e uma gravação, que são os próprios dados que constituem a base material da comunicação e das declarações. Não existe separação entre declaração verbal e declaração escrita nas relações estabelecidas por meio eletrónico. Em todas elas, pelo contrário, existe registo, suporte e gravação de forma igual, quer nos casos em que as partes decidem formalizar em documentos, com forma específica as suas declarações, quer nos casos em que decidam o contrário. Existirão sempre dados, suporte, gravação. E, portanto, teoricamente, nas comunicações eletrónicas verificam-se sempre cumpridos os pressupostos do Regulamento para a sua qualificação como documentos eletrónicos.

---

[911] Invocando a doutrina italiana, Luís de Sousa distingue o conteúdo intrínseco e o conteúdo extrínseco dos documentos em geral, como meios de prova, da seguinte forma: "*O extrínseco reporta-se ao documento na sua materialidade de continente, de invólucro formal, abrangendo aspetos atinentes à formação e proveniência de documento, Por sua vez o intrínseco refere-se ao conteúdo do documento, ao que este representa, ao conteúdo negocial das declarações representadas*". Sousa, L. F. P. (2017). *O valor Probatório do Documento Eletrónico no Processo Civil, 2.ª Edição*. Edições Almedina, S. A. Coimbra, pág. 24. Os documentos eletrónicos, tendo como suporte dados em suporte eletrónico, não são apenas suporte de conteúdos que podem também ser representados em papel, mas também podem ser, eles próprios, os fatores constitutivos de operações que são efetuadas por meios eletrónicos, como são os exemplo das notificações eletrónicas, a contagem automática de prazos, que são em si mesmas operações que consistem na utilização de dados eletrónicos.

E é adequado que assim seja, porque é natural que as partes em qualquer relação jurídica estabelecida por meios eletrónicos tendam a utilizar com maior frequência os registos de dados para os autenticarem com assinatura ou selo eletrónico, assim alcançando uma maior segurança jurídica. E é natural também que essa vontade advenha do facto de existir uma maior necessidade dessa segurança, porque nas relações estabelecidas por meio eletrónico o nível de risco é sempre mais elevado do que nas restantes. Por essa razão o conceito de documento eletrónico não coincide necessariamente com o de documento em papel, sendo, porém, que o conceito de assinatura eletrónica e de selo eletrónico se baseiam nesse pressuposto de serem os instrumentos jurídicos de autenticação de documentos eletrónicos.

A estabilização do conceito de documento eletrónico e de assinatura eletrónica veio criar as condições para que a legislação deixasse de conter necessariamente uma equiparação das mensagens eletrónicas aos documentos escritos, por desnecessária.

Os documentos eletrónicos assinados passam a ser plenamente equivalentes aos documentos em papel com assinatura manuscrita. Essa equivalência é também efetuada no Regulamento EIDAS, da UE, em especial no n.º 2 do art.º 25.º, para as assinaturas eletrónicas qualificadas. Relativamente aos restantes tipos de assinaturas, o regulamento estabelece um princípio de não discriminação.

O Regulamento efetua uma dupla equivalência. Por um lado faz equiparar as assinaturas eletrónicas e os selos eletrónicos às assinaturas em papel, no artigo 25.º. Por outro lado, e em simultâneo, equipara os documentos eletrónicos aos documentos em papel, no artigo 46.º. Esta dupla equivalência funcional garante a validade jurídica dos documentos eletrónicos. Essa equiparação efetua-se mediante a enunciação do princípio da não discriminação, tanto para as assinaturas eletrónicas como para os documentos eletrónicos. Relativamente às assinaturas eletrónicas, o n.º 2 do artigo 25.º estabelece a presunção do cumprimento de todas as suas funções quando se trate de assinaturas eletrónicas qualificadas, considerando-se que possuem um efeito equivalente aos das assinaturas manuscritas, qualquer que seja a natureza destas. Relativamente aos documentos não existe presunção idêntica no artigo 46.º, por desnecessária, dado que o seu efeito probatório advirá da assinatura.

2. O carácter original dos documentos eletrónicos

A exigência legal da originalidade dos documentos é um instrumento de segurança jurídica quanto à autenticidade e à integridade do seu conteúdo.[912] O original assegura uma mais fácil deteção das eventuais alterações ou adulterações aos documentos.[913] Para os destinatários dos documentos, a constatação da originalidade é um instrumento de confiança, sendo que a simplicidade e rapidez dessa constatação é também importante para a rapidez nas transações.

A garantia da originalidade é especialmente importante quando os documentos incorporam títulos representativos de direitos. Na atividade empresarial, os títulos transacionáveis são um instrumento de rapidez e facilidade nas transações comerciais, dado que a posse do documento que incorpora o título corresponde à titularidade do direito sobre um determinado bem, operando-se a sua transmissão com a mera entrega do documento.

Sendo o título um documento, que é fonte da legitimidade da propriedade dos bens ou direitos que incorpora, é essencial que existam garantias de que seja único e de que não existem outros documentos com eles conflituantes, que confiram idênticos direitos a terceiros. Trata-se do requisito da singularidade dos documentos.

Quando se trate de títulos não negociáveis, por exemplo os certificados de seguro, os certificados de inspeção automóvel, os certificados de garantia, em que o documento só vale como original, a sua eficácia corresponde à certeza acerca da sua origem, ou seja, a sua autenticidade e da sua integridade.[914]

Os títulos negociáveis são utilizados com frequência nas transações de mercadorias em trânsito internacional, sendo essa a razão pela qual a UNCITRAL e outras organizações internacionais se dedicaram à criação de normas que facilitem a sua utilização no comércio internacional.

---

[912] *"It is submitted that the function of an original is to ensure the highest possible level of authenticity of the information"*. "A/CN.9/WG.IV/WP.55", par. 67.

[913] *"Using paper, these types of document are usually only accepted if they are "original" to lessen the chance that they have been altered, which would be difficult to detect in copies"*. "A/CN.9/426", par. 73.

[914] São duas as categorias de documentos relativamente aos quais a lei exige originalidade: Para fins públicos, nomeadamente para a apresentação perante tribunais (para fins probatórios, quando a lei só aceite os originais) e à administração pública (v.g. faturas, cujo original é indispensável ao exercício dos direitos de crédito e de dedução em matéria tributária). Para fins privados, em especial os documentos que incorporam um direito ou um título, por exemplo os conhecimentos de embarque de mercadorias e, em geral, os títulos negociáveis. *"The first one was a requirement contained in rules of evidence according to which, when a writing was to be presented in support of a claim, the original document was required as the best evidence.(...). For reasons of administrative supervision, certain documents (e.g., invoices) were to be kept and presented in the original. The second type of requirement concerned documents that incorporated a right or title (e.g., bills of lading, warehouse receipts and negotiable instruments); in order to obtain or transfer the right or title incorporated in such a document it was necessary to obtain or transfer the possession of the original document"*. "A/CN.9/373", par. 78.

Nas relações administrativas são também emitidos documentos que só valem como originais, como é o caso das certidões, dos certificados, dos atestados, dos selos de conformidade, por exemplo, de aferição de instrumentos de medição, dos títulos de registo e de propriedade, dos títulos de autorização, por exemplo de condução, dos alvarás, e muitos outros. Ainda nas relações administrativas assume elevada relevância a necessidade de as empresas possuírem o original das faturas para exercerem os correspondentes direito em matéria tributária, nomeadamente o direito de crédito sobre o Estado correspondente ao IVA dedutível e o direito à consideração como custo da atividade da despesa por elas documentada.[915] Nestes casos, a originalidade do documento garante a conformidade do seu conteúdo, certificada pela administração pública.

No original em papel a informação é inserida fisicamente no mesmo suporte físico onde é incorporada a autenticação. Trata-se, portanto, de um objeto documental físico, único e irrepetível. As alterações ao documento, tendo que ser também físicas e materializadas, como rasuras, aditamentos, eliminações parciais, são normalmente detetáveis pela observação do papel, dadas as suas caraterísticas físicas. A exigência de originalidade protege as partes contra as adulterações, bem como contra eventuais cópias ilícitas que simulem originalidade. O papel proporciona também que as partes possam, como os seus próprios meios, normalmente, detetarem essas alterações.

Trata-se de duas funções diferentes, a de garantir a integridade e a singularidade dos documentos, que a garantia de originalidade assegura.

A verificação da originalidade de um documento em papel é relativamente simples, sendo que qualquer pessoa pode efetuar essa constatação, mediante a sua análise visual.

E o que é um documento eletrónico original? Não é linear a definição, dado que nos documentos em suporte eletrónico não se pode falar em originalidade. Não há documentos eletrónicos originais, porque eles não são objetos físicos, mas processos compostos.

O acesso a um documento eletrónico implica também o acesso à sua edição e aos instrumentos informáticos necessários à sua alteração. Essa alteração pode facilmente ser efetuada, sem que dela fiquem vestígio correspondentes às rasuras e

915 *"Acceptance by fiscal authoritiesof electronic filings and of documents such as invoices in electronic form"*. "A/CN.9/360", par. 65.

aditamentos nos documentos em suporte papel.[916] Por essa razão, a determinação da originalidade de um documento eletrónico é um processo de elevada dificuldade e complexidade, inacessível a qualquer pessoa, pelos seus próprios meios.[917]

Do mesmo modo, a verificação da singularidade é muito difícil, porque quando alguém envia um documento eletrónico, o sistema informático faz sempre uma cópia a partir da base de dados onde está gravado, e é essa cópia que é enviada, passando a existir pelo menos dois documentos iguais.[918]

Quando a lei exige que o exercício de um direito dependa da existência ou da apresentação do original de um documento, fá-lo, fundamentalmente, para garantir três resultados:

i) A autenticidade,

ii) A integridade;

iii) A exclusividade da sua detenção, ou seja, a sua singularidade.

As garantias de autenticidade e de singularidade são, assim, as duas mais importantes funções do documento original em papel, e devemos analisá-las em separado, dado que as soluções podem também ser diferenciadas.

2.1. Originalidade e autenticidade

916 *"The electronic document is quite different. It takes the form of a magnetic medium whose data content can be changed at any time. Changes or additions will not appear as such"*. A/CN.9/WG.IV/WP.53, Anex, III, pág. 380.

917 Foram discutidas várias possibilidades, desde a de se considerarem originais apenas as mensagens antes de serem comunicadas pelo remetente, até à ponderação da não admissibilidade da existência de originais nas comunicações por EDI (*"It was reported in this regard that there might be some uncertainty as to what constitutes an original in the EDI context"*), e ainda à análise, ainda confusa e aparentemente pouco informada, da possibilidade de se exigirem os procedimentos próprios daquela que viria a ser conhecida mais tarde como a tecnologia das assinaturas digitais, mas que a Comissão revela já conhecer, embora aparentemente de forma incipiente: *"It was further observed that this phenomenon raised the question of whether the "original" should be considered as being the message in the hands of the sender prior to being transmitted and perhaps encrypted, or the data received by the recipient, irrespective of whether that received message had been brought up on the screen or otherwise acted upon by the recipient"*. "A/CN.9/360", par. 49.

918 Não acompanhamos, neste caso, a opinião de Luís de Sousa, que defende a existência de uma separação entre os documentos originais e as reproduções desses originais eletrónicos, dando como exemplo a impressão de um documento eletrónico e a sua posterior digitalização. Só que nesse caso, trata-se de três documentos distintos, não se podendo falar de duplicados eletrónicos. Sousa, L. F. P. (2017). Op. cit., pág. 37. Aliás o próprio Autor refere, logo de seguida, que "*a partir do momento em que ocorre uma impressão em papel de um documento eletrónico com assinatura eletrónica aposta, a assinatura eletrónica deixa de ser verificável de modo que pode afirmar-se que, uma vez impresso, o documento eletrónico deixa de estar assinado*". Ibidem, página 42.

A originalidade dos documentos em papel destina-se a conferir segurança acerca da sua origem, ou seja, da sua autenticidade e, simultaneamente, de que ele não foi alterado após a sua assinatura, ou seja, da sua integridade.

O regime da LMCE reflete a dificuldade de encontrar nos documentos e comunicações eletrónicos um equivalente aos documentos originais, com a mesma força jurídica e as mesmas garantias de autenticidade dos documentos em papel. Sem ela, estava em causa a utilização do EDI e dos suportes eletrónicos nos casos em que a lei exigisse a apresentação dos originais dos documentos. Na sua elaboração foram ponderadas as seguintes possibilidades:

i) Só ser admitida a utilização de suportes eletrónicos quando em paralelo as partes guardassem em arquivo os originais dos documentos em papel;

ii) Reverem-se todas as normas legais que exigem documentos originais, para nelas se contemplarem os documentos eletrónicos;

iii) Estabelecer que se consideram cumpridos os requisitos de documento original, com a única condição de os documentos eletrónicos serem reproduzíveis em forma legível;

iv) Aplicação do princípio da equivalência funcional, analisando as funções que cumpriam os requisitos de original em papel e verificando como poderiam ser garantidas pelos documentos eletrónicos.[919]

Na falta de condições tecnológicas para garantir a autenticidade e integridade dos documentos eletrónicos, a solução encontrada foi, também neste domínio, a aplicação do princípio da equivalência funcional dos documentos eletrónicos aos documentos originais.[920]

E essa equivalência assenta, fundamentalmente, no mecanismo da autenticação dos documentos eletrónicos.[921] A LMCE considera cumprido o requisito da

---

[919] *"The second possible approach, which was sometimes referred to as the "functional-equivalent approach" and was regarded by the Working Group as preferable, was to identify the purposes and functions of the traditional requirement of an original with a view to determining how those purposes or functions could be fulfilled through EDI techniques"*. "A/CN.9/360", par. 63.

[920] Era nessa linha de equivalência dos graus de autenticidade que apontavam os trabalhos da UNCITRAL. *"For the purpose of establishing a functional equivalent that would be relevant in an EDI environment, the requirement of an original may be considered as a variant of a requirement that the data be properly authenticated"*. "A/CN.9/WG.IV/WP.55", par. 67.

[921] O artigo 8.º da LMCE, sob o título "*Original*", estabelece a equivalência functional quando os documentos eletrónicos cumpram os requisitos de "*reliable assurance as to the integrity of the information from the time when it was first generated"*, e quando*"that information is capable of being displayed to the person to whom it is to be presented"*. Assim, é a integridade o núcleo central da

originalidade nos documentos eletrónicos quando exista uma garantia fidedigna da conservação da integridade da informação deles constante, desde que foi gerado pela primeira vez de forma definitiva.

São, assim, dois, os pressupostos da equivalência funcional dos documentos eletrónicos, a autenticidade e a integridade.[922] A autenticidade assegura a origem e a certeza acerca da pessoa que está a ele vinculado, bem como a sua participação pessoal no ato de assinatura.

A integridade é a garantia da inalteração, e só se pode confirmar a partir do momento em que o documento tomou a sua forma definitiva, ou seja, a partir do momento em que foi autenticado pela pessoa ou pela entidade que a ele se vinculou. A integridade de um documento eletrónico é sempre avaliada em confronto com o conteúdo do documento eletrónico autenticado, ou seja, com o momento em que ao documento eletrónico foi colocado o instrumento de autenticação correspondente à assinatura.

O grau de fiabilidade da garantia da integridade também é densificado pela LMCE de forma genérica e aberta, reportando a alínea b) do n.º 3 do art.º 8.º para as circunstâncias em que foi gerado o documento e para os fins a que se destina. Trata-se, também aqui, de uma formulação orientada para a finalidade da LMCE, de eliminar barreiras legais à utilização dos documentos e das comunicações eletrónicas na atividade económica.[923] Essa formulação não escapa, porém, à crítica acerca do seu carácter vago, uma vez que dela não resulta a densificação de critérios objetivos e

---

equivalência à originalidade do papel, pelo que, de seguida, o legislador teve o cuidado de definir o conceito de integridade, para esse fim. O que faz no n.º 3 do artigo 8.º, estabelecendo que ela se certifica quando o documento se manteve inalterado e completo. "Guide to Enactment LMCE (1996)", pág. 6.

[922] Foram ponderadas outras possibilidades de definição dos requisitos de original dos documentos eletrónicos. Numa das definições propostas considerava-se que deveriam reunir-se três pressupostos para o documento ser considerado original, i) que o remetente o considere como tal, ii) que esteja assinado e possua indicação de data e hora e iii) que o remetente o aceite como original e o assinale mediante mensagem de retorno. Esta opção foi rejeitada porque estabelecia requisitos mais exigentes que os existentes para o papel. Estabeleceu-se um consenso no sentido de que, sendo as funções essenciais da exigência de original, a identificação do autor do documento e a sua integridade, era sobre elas que deverá ser erigido o pressuposto da equivalência funcional. *"It was proposed to include in the uniform rules a provision that the requirement of an original was satisfied if the following conditions were met: (a) there was a reliable identification of the originator of the message and (b) there existed reliable assurance as to the integrity of the content of the message as sent and received"*. "A/CN.9/373", par. 88.

[923] Ponderou-se que a LMCE previsse que as partes pudessem convencionar os requisitos necessários para a consideração dos documentos eletrónicos como originais. Essa possibilidade foi abandonada, pelos efeitos que têm sobre terceiros os documentos originais, bem como pelo facto de os efeitos jurídicos dos documentos originais serem imperativamente estabelecidos pela lei. Por essa razão as normas do artigo 8.º devem também elas serem consideradas de aplicação imperativa. *"On the other hand, it was considered that such an agreement could not be invoked against a third party who chose to rely on the statutory requirement that the message had to be presented in the original"*. "A/CN.9/373", par. 95.

apreciáveis de forma transparente, que confiram, por si mesmas, confiança aos agentes económicos.[924]

Além da integridade, exige ainda a LMCE, como requisito de equiparação a original, que o documento eletrónico possa ser "*mostrado*" à pessoa a quem deva ser apresentado. Trata-se do requisito normal da acessibilidade aplicável aos documentos eletrónicos, dada a sua natureza complexa, assente numa estrutura digital lógica e sequencial, só inteligível pelo entendimento humano mediante a sua apresentação em forma legível. O requisito da originalidade depende também dessa possibilidade de o documento eletrónico ser legível, sendo essa legibilidade correspondente à sua aptidão, não só para ser analisado pelo entendimento humano, como também para ser objeto de tratamento automatizado pelos sistemas informáticos.[925]

Com a adoção de um conceito de assinatura eletrónica na LMAE e na Diretiva 1999/93/CE, bem como do conceito de documento eletrónico na legislação nacional posterior, em especial a portuguesa, deixa de ser necessária a equivalência funcional, dado que a lei passa a adotar conceitos próprios de documento e de assinatura eletrónica, passando a ser essa a base da sua validade e eficácia jurídica.

Por essa razão nem a Diretiva nem a lei portuguesa contêm normas de equivalência dos documentos eletrónicos aos requisitos de originalidade dos documentos em papel, sendo substituídas pelos conceitos próprios de documento e de assinatura eletrónicos e pelas garantias de autenticidade e de integridade que as assinaturas eletrónicas conferem. A equivalência das assinaturas qualificadas às assinaturas em papel, quando a lei as exige, é suficiente para que, associadas àquelas garantias se consume a equivalência. É nesse pressuposto que o art.º 4.º do Decreto-Lei n.º 290-D/99, de 2/8, prevê a existência de cópias de documentos eletrónicos, às quais atribui os mesmos efeitos das cópias dos documentos em papel.[926]

---

[924] Essa abertura é reconhecida: *"Article 8 should be regarded as stating the minimum acceptable form requirement to be met by a data message for it to be regarded a the functional equivalent of an original".* "Guide to Enactment LMCE (1996)", e essa preocupação de se estabelecer um parâmetro mínimo e aberto é reforçada mais adiante, convidando os estados a que na legislação nacional que vierem a adotar, não limitem os pressupostos de equivalência dos documentos eletrónicos aos originais de documentos em papel: *"The indication that the form requirements stated in article 8 are to be regarded as the "minimum acceptable" should not, however, be construed as inviting States to establish requirements stricter than those contained in the Model Law"*. United Nations Publication Sales No.: E.99.V.4, ISBN 92-1-133607-4, par. 64.

[925] *"The data as stored in a computer in electronic form cannot be read or interpreted by a human being. Therefore, it cannot be presented to a court unless it takes on a visual form, either on a print-out or on a visual display unit which the court can look at"*. A/CN.9/WG.IV/WP.53, par. 57.

[926] Não seguimos a doutrina de Illescas Ortiz, que defende duas conceções diferenciadas de original eletrónico. Na primeira defende que se trata de *"la información que se encuentra almacenada en las*

A equivalência dos documentos eletrónicos aos originais é atualmente plena, quando estejam autenticados por assinaturas eletrónicas qualificadas, como analisámos no capítulo que dedicámos às funções da assinatura eletrónica. Do mesmo modo, os selos eletrónicos cuja previsão legal foi consagrada no Regulamento EIDAS, que também utilizam a tecnologia das assinaturas eletrónicas qualificadas, garantem a originalidade dos documentos.[927]

O requisito da originalidade, na sua vertente de garantia da autenticidade e da integridade encontra-se atualmente cumprido *a priori* com as assinaturas eletrónicas qualificadas.

Ao estabelecer uma equivalência plena entre os documentos eletrónicos e os documentos em papel, o artigo 46.º do Regulamento EIDAS, inclui a equivalência a documentos originais. Do mesmo modo inclui essa equivalência a presunção da autenticidade consagrada no n.º 2 do artigo 25.º.

2.2. Originalidade e singularidade. Os títulos transacionáveis eletrónicos

O requisito da singularidade dos documentos eletrónicos é próprio dos títulos transacionáveis, porque a posse do documento é a prova da propriedade do bem ou do direito subjacente e a sua tradição corresponde à transferência da propriedade dos bens, que titula. A originalidade do documento que suporta o título é a garantia da exclusividade da propriedade.[928]

---

dichas memórias de los sistemas de información". Entendemos que esses suportes digitais são apenas dados, sem valor informativos sequer, e por isso não podem ser considerados sequer como informação, nem como documentos. Defende o Autor que *"originales son en consecuência los documentos electrónicos o de papel en los que los datos electrónicos se imprimen"*. Ortiz, R.I., (2000). *Derecho de la Contratación Electrónica*. Civitas Ediciones. Madrid, pág. 169. Mas a autenticação de um documento eletrónico não de transporta para um documento em papel, com a sua impressão. Os requisitos de originalidade são plenamente cumpridos com a assinatura eletrónica que garanta a autenticidade e a integridade dos documentos eletrónicos, e por essa razão a sua equivalência a documentos assinados engloba a sua equivalência a documentos originais.

[927] Essa garantia ficou expressa no parágrafo 59 dos considerandos do Regulamento da seguinte forma: *"Os selos eletrónicos deverão servir de prova da emissão de um documento eletrónico por determinada pessoa coletiva, certificando a origem e a integridade do documento"*. Do mesmo modo, o n.º 2 do artigo 35.º estabelece que "*O selo eletrónico qualificado beneficia da presunção da integridade dos dados e da correção da origem dos dados aos quais está associado"*.

[928] Os títulos transacionáveis são documentos que incorporam direitos. Essa incorporação corresponde a uma materialização desses direitos nos documentos, podendo assim ser transacionados como se se tratasse de bens móveis. Os direitos imateriais, os direitos sobre bens imóveis ou móveis, podem ser transacionados com elevada simplicidade, mediante entrega do documento que suporta o título. Como refere Mariliana Carrillo, *"Al materializarse el derecho en un documento, se convierte en una cosa*

Quando se trata de documentos em papel, o envio do original para o destinatário priva o remetente da sua posse.[929] Nos documentos eletrónicos, o envio de um documento não implica a sua eliminação do disco onde está gravado, pelo que se trataria sempre de cópias. E se assim é, relativamente a nenhum documento eletrónico comunicado se poderia cumprir o requisito da originalidade.[930]

A singularidade é um conceito próprio dos documentos em papel, que não é transponível, sem mais, para suporte eletrónico.[931] E embora o n.º 2 do artigo 25.º do Regulamento EIDAS estabeleça a equivalência das assinaturas eletrónicas às assinaturas manuscritas, incluindo, portanto, todas as funções que são próprias da assinatura, não se pode dizer que essa equivalência jurídica corresponda ainda a uma possibilidade técnica e prática, quando falamos da singularidade.

O regime desses títulos só pode funcionar quando a ordem jurídica proporcionar aos agentes económicos a segurança de que funciona adequadamente o princípio da exclusão, e de que aquele título é único, o que não ocorre com os documentos eletrónicos, nem a LMCE garante. Este era o problema mais difícil de resolver, especialmente por falta de condições tecnológicas.

Considerou-se a possibilidade de criação de um registo eletrónico dos títulos de crédito e das suas transações pelos diversos titulares.[932] Seria a única forma de se garantir a proteção de terceiros contra a fraude com a duplicação dos títulos[933]. Este regime viria a ser adotado no que respeita aos conhecimentos de embarque eletrónicos, das mercadorias em trânsito internacional e é também utilizado em muitas práticas

---

mueble objecto de circulación, exigiéndose la presentación del título para el ejercício del derecho". Carrillo, Mariliana Rico; op. cit., pag. 86.

929 Se a incorporação do direito num documento em papel corresponde à sua materialização, a transposição do suporte desse documento do suporte de papel para o suporte eletrónico corresponde a uma desmaterialização do próprio documento, o que coloca desde logo em causa a questão da segurança jurídica. Nesse sentido, Carrillo, Mariliana Rico; op. cit., pag. 87.

930 *"If "original" were defined as a medium on which information was fixed for the first time, it would be impossible to speak of "original" data messages, since the addressee of a data message would always receive a copy thereof"*. "A/CN.9/WG.IV/WP.64", par. 74.

931 Também assim se opinava, nos trabalhos da UNCITRAL. *"The concept of originality was a concept limited to traditional paper-based documents and that, in view of the manner in which computer records were created, maintained and communicated, it was impossible to speak of original computer records"*. "A/CN.9/373", par. 87.

932 *"Registry systems could serve a useful function when the rights of third parties were involved, although it would be difficult to envisage dealing with all types of possible relationships under a single type of approach"*. "A/CN.9/360", par. 67.

933 Merece também realce a menção à possibilidade de utilização de chaves públicas e privadas para garantir essa proteção. Embora estas ideias não tenham sido desenvolvidas no âmbito da LMCE, elas viriam mais tarde a ser importantes no desenvolvimento da tecnologia das assinaturas digitais, como veremos no local próprio. *"In an EDI environment, where possession was not possible, the holder might be protected by other means (e.g., registration, use of public and private key sets) or might not be protected at all"*. "A/CN.9/WG.IV/WP.69", par. 12.

comerciais, por exemplo nos mercados bolsistas com a transmissão de ações e outros títulos.[934] Essa utilização é facilitada com a possibilidade de conexão eletrónica, imediata e automática entre os sistemas informáticos do vendedor, do adquirente e do titular do registo.[935]

A tecnologia das assinaturas digitais também não resolveu, até agora, o problema da singularidade, dado que não se garante a impossibilidade de duplicação dos documentos pelo próprio titular.[936] Esse problema é parcialmente resolvido pela existência dos selos eletrónicos e das assinaturas qualificadas, bem como pela existência de selos temporais, que certificam a data e hora da assinatura. Essas funções diminuem as possibilidades de fraude na duplicação dos documentos. Apesar disso, não existe nos suportes eletrónicos uma equivalência à singularidade.

2.2.1. O objeto da garantia da singularidade

A singularidade de um documento é um atributo diferente do da originalidade.

A originalidade garante autenticidade, porque assegura que foi naquele documento que foi colocada a declaração com relevância jurídica e foi nele que foram

[934] Mariliana Carrillo classifica a desmaterialização dos títulos de crédito em duas dimensões, por um lado a desmaterialização do próprio direito que lhe está associado e, por outro, do suporte físico representativo do direito. A primeira consiste no desaparecimento do título e da sua substituição por um registo contabilístico de carácter informatizado. É esse registo e as correspondentes anotações, que confere eficácia às transações. A segunda corresponde à criação dos próprios títulos de crédito eletrónicos, cuja transmissão de ópera mediante a assinatura eletrónica do respetivo titular. *"El título virtual es creado y firmado electrónicamente por el librador y es susceptible de transmisión*". Carrillo, Mariliana Rico; op. cit., pag. 91.

[935] Nos EUA desenvolveu-se a utilização dos títulos negociáveis eletrónicos associados aos chamados registos centrais ou registos contabilisticos. O exemplo mais conhecido são os títulos hipotecários, designados de *e-Mortgages*, que permitem ao respetivo titular transacioná-los de forma simples e eletrónica. Nesta matéria merecem realce as Guidelines da MISMO (The Mortgage Industry Standards Maintenance Organization), disponíveis em http://www.mismo.org/Guidelines/EngineeringGuidelines (MEGS).htm (última consulta em 9/5/2016).

[936] Apesar disso, tem-se desenvolvido o chamado dinheiro eletrónico, que utiliza a tecnologia da assinatura digital no contexto de uma relação previamente estabelecida entre um agente económico (que designamos por *A*) e uma entidade bancária que carrega num suporte eletrónico um conjunto de dados representativos de dinheiro que fica previamente retido na conta de base. Quando o agente económico utiliza esse dinheiro eletrónico para pagar a outro (que designamos por *B*), disponibiliza-lhe esses dados. O agente económico *B* converte esses dados em dinheiro comunicando-os ao banco que efetua a transferência financeira. Todos os procedimentos são efetuados com carácter imediato e eletrónico. Com refere Mariliana Carrillo, *"En los billetes electrónicos, el papel moneda se substituye por un conjunto de bits representativos de un determinado valor denominados tokens, que s ealmacenan en ficheiros del disco duro del ordenador y que pueden transferirse a través de la Red a cambio de un produto o servício"*. Carrillo, Mariliana Rico; op. cit., pag. 130. Esta tecnologia dos *Token*, que no caso do dinheiro eletrónico são assinados com a assinatura eletrónica da entidade bancária, poderá ser a base para o desenvolvimento futuro das condições de singularidade dos documentos eletrónicos.

colocadas as assinaturas das partes. Garante também a integridade, em especial pela facilidade com que se pode observar e detetar qualquer alteração.

Mas a originalidade não garante a singularidade, mesmo no suporte papel, dado que não garante que o mesmo autor não tenha emitido vários documentos originais, todos iguais.

Para melhor analisarmos o problema, poderíamos dizer que a função de singularidade terá dois sentidos:

i) No sentido material, ela garante que o autor de um documento não emitiu outro igual, com o mesmo conteúdo, passando a haver dois documentos originais iguais. Aqui, a singularidade é uma relação entre um documento e a relação jurídica subjacente, e garante que aquele documento é o único relativamente a ela. Em termos temporais, a singularidade opera relativamente ao momento da emissão do documento;

ii) No sentido formal, garante que um mesmo documento, mesmo quando é único, não é duplicado. Neste caso, a singularidade protege as partes contra a existência de duplicações do mesmo documento. Aqui a singularidade opera relativamente ao momento posterior ao da emissão e assinatura do documento.

A singularidade material tanto pode ser violada quando os documentos têm como suporte o papel, como nos casos em que o seu suporte é o eletrónico. A quebra de segurança jurídica que advém da quebra da singularidade material, não é atinente aos documentos, mas às pessoas e à confiança subjetiva, pelo que está num plano diferente do dos suportes documentais. A singularidade material não apresenta especificidades nos documentos eletrónicos.

Quanto à singularidade formal, ela é particularmente relevantes nos documentos que incorporam títulos, onde é a posse do documento original a garantia de segurança que protege as expectativas dos agentes, incluindo os terceiros.

Nos suportes eletrónicos a entrega de um documento não implica o seu desapossamento, dado que, nos casos em que eles são comunicados por via eletrónica, o seu envio corresponde a uma duplicação.[937]

[937] A assinatura eletrónica garante a integridade de um documento e é essa a sua função. E garante-a sempre, incluindo nos casos em que desse documento é efetuada uma cópia. A função singularidade ultrapassa a função de assinatura eletrónica. Nesse sentido se pronuncia Rivero, que defende que o

A exigência de singularidade dos documentos eletrónicos que incorporem títulos transmissíveis não tem correspondência em nenhuma norma legal para os documentos em papel, sendo que que o instrumento de segurança jurídica quanto a estes últimos é garantido pelo requisito legal da originalidade.

Ora, o requisito da originalidade considera-se cumprido nos documentos eletrónicos quando eles possuam uma garantia fidedigna da sua integridade, ou seja, da sua inalteração desde que foram emitidos pela primeira vez em forma definitiva, como estabelece a alínea a) do n.º 1 do art.º 8.º da LMCE. Assim sendo, bastaria que esse requisito se verificasse para que os documentos eletrónicos possuíssem a virtualidade de incorporar título negociáveis e titulassem também a transmissão dos respetivos direitos neles incorporados.

Porém, para os casos em que os documentos eletrónicos incorporam títulos transmissíveis, o n.º 3 do art.º 17.º da LMCE estabelece como requisito adicional e essencial da sua validade jurídica, que tenha sido utilizado um método fiável que garanta a sua singularidade. Por que razão acrescenta então o requisito da singularidade? Não estará com isso a violar-se o princípio da equivalência funcional e a criar-se exigência legais novas em nome da segurança das transações, que poderiam então ter que ser também aplicáveis às transações em papel?

Por outro lado, em que é que consiste a singularidade de uma mensagem eletrónica? Por exemplo nas comunicações EDI, e nas relações comerciais regulares, a repetição de uma encomenda efetuada por um comerciante a outro, com as mesmas quantidades e a mesma designação do produto é normalmente entendida como uma nova encomenda. Aqui a singularidade da segunda mensagem eletrónica está na data da sua emissão, sendo esse o elemento que permite concluir que não se trata de um lapso de repetição da primeira.

Mas assim sendo, nas comunicações de mensagens eletrónicas não existe repetição e todas serão singulares, porque todas são diferentes, pelo menos em face da data e hora em que foram emitidas.[938] E também são diferentes as mensagens mediante as quais se transmite, porventura de forma ilícita, um mesmo direito a pessoas

conceito de original é próprio do papel e inaplicável aos documentos eletrónicos. Rivero, D.C. (Mayo 2005); op. cit., nota 221. É nesse sentido também que o artigo 8.º da LMCE e o artigo 12.º da UETA estabelecem que o documento se considera original no caso de poder consultado com a mesma forma e conteúdo com que foi arquivado.

[938] No mesmo sentido, *"All data messages are necessarily unique, even if they duplicate an earlier data message, since each data message is sent at a different time from any earlier data message sent to the same person"*. "Guide to Enactment LMCE (1996)", par. 117.

diferentes, dado que essas mensagens são elas próprias diferentes e têm destinatários diferentes. Do mesmo modo, uma mensagem eletrónica emitida ilicitamente por uma pessoa que se faz passar como tendo a identidade de outra, por exemplo porque se apropriou indevidamente das suas credenciais de acesso, é também uma mensagem original. Estas conclusões aplicam-se tanto aos documentos em suporte papel como em suporte eletrónico.

Nestas circunstâncias qual o sentido da exigência de singularidade constante do n.º 3 do art.º 17.º da LMCE? Se nos documentos em papel a segurança jurídica se alcança com a exigência de original e de posse do documento que titula o direito, por que razão essa exigência de originalidade não é suficiente nos documentos eletrónicos?

A primeira questão a resolver é a de saber se a exigência de singularidade acresce à de requisito de original (que nos documentos eletrónicos se consuma com as garantias de autenticidade e de integridade), ou se a substitui. É nosso entendimento que acresce, e é por essa razão que a LMCE a autonomiza, provavelmente pelas preocupações acrescidas que resultam do facto de a duplicação de documentos ser mais fácil, a que acresce a dificuldade na sua deteção por mera observação.

Nos documentos em papel, a segurança não advém apenas da exigência de originalidade. Do universo dos documentos só alguns são títulos negociáveis. E nestes, a garantia de segurança jurídica não advém apenas na originalidade do documento que contém o título, mas também da sua posse. É a posse do documento que prova a titularidade do direito ou da obrigação, e a sua transmissão depende da tradição da posse.

Também nos documentos eletrónicos não basta a originalidade, sendo necessário um sucedâneo da posse, dado que o conceito de posse não existe nos documentos eletrónicos com o mesmo conteúdo dos documentos em suporte de papel. No suporte do papel, a entrega do documento implica o seu desapossamento e isso não acontece nos suportes eletrónicos. Nestes casos, havendo transmissão do direito existe desapossamento dele, mas não existe desapossamento do documento que o titula. E se assim é, o risco para a segurança jurídica que aqui existe é o perigo de a mesma pessoa que transmitiu um determinado direito ou obrigação mediante o envio de um comunicação eletrónica, fazer a emissão de um novo documento, transmitindo esse direito a outra pessoa. Neste caso ambos os documentos são originais e ambos são singulares, pelo que aparentemente nenhuma das exigências resolve a insegurança que

advém desta possibilidade de serem frustradas as expectativas legítimas dos adquirentes. É esta possibilidade que a exigência de singularidade pretende evitar.

Em conclusão, apesar de a redação do n.º 3 do art.º 17.º da LMCE reportar a exigência de singularidade à mensagem de dados mediante a qual se efetua a transmissão dos direitos e obrigações, o que se pretende com essa norma é garantir, ao adquirente, a segurança de que o autor da transmissão não proceda ilicitamente a nova transmissão para terceiro posteriormente.

A singularidade pode ser reportada ao ato ou ao documento, como antes vimos. Do nosso ponto de vista, o objeto desta norma da LMCE é o próprio ato, e a sua singularidade. Pretende-se, então, evitar que a utilização de meios eletrónicos facilite a prática de atos ilícitos de transmissão de títulos negociáveis e dos correspondentes direitos associados, mais do que uma vez.[939] É essa possibilidade que produz insegurança e é suscetível de violar as expectativas legítimas dos adquirentes, que a lei pretende evitar. Quando o titular de um direito pratica o ato de emitir, e enviar para terceiro, um documento eletrónico que transmite um direito, todas as repetições desse ato são potencialmente ilícitas e são elas que a LMCE pretende evitar.[940]

Este nosso entendimento parece-nos ser confirmado pelo n.º 5 do art.º 17.º da LMCE, que tem como objetivo impedir que o titular que transmita o seu direito mediante uma mensagem eletrónica, efetue nova transmissão, agora mediante documento em suporte de papel.[941] Nos termos desta norma, quando seja utilizada uma mensagem eletrónica como instrumento de transmissão de um direito ou de uma obrigação, o respetivo autor fica inibido de praticar idêntico ato através de um

---

[939] Embora o texto da LMCE a que nos vimos referindo (o n.º 3 do artigo 17.º): *"(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique"*), se refira apenas à singularidade da própria mensagem e não à singularidade do ato de transmissão, parece-nos que é a singularidade do ato que a lei pretende garantir. Também nesse sentido: *"The words "a reliable method is used to render such data message or messages unique" should be interpreted as referring to the use of a reliable method to secure that data messages purporting to convey any right or obligation of a person might not be used by, or on behalf of, that person inconsistently with any other data messages by which the right or obligation was conveyed by or on behalf of that person"*. "Guide to Enactment LMCE (1996)", pág. 12 e par. 117, respetivamente.

[940] *"Yet, all but the first transfer might be fraudulent"*. "Guide to Enactment LMCE (1996)", par. 117.

[941] A redação do n.º 5 do artigo 17.º é a seguinte: *" Where one or more data messages are used to effect any action in subparagraphs (f) and (g) of article 16, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved"*. "Guide to Enactment LMCE (1996)", pág. 13.

documento em suporte papel. E caso o faça, a LMCE prevê a sua invalidade, e não apenas a sua ineficácia. Esta norma destina-se a garantir a singularidade do ato de transmissão operado mediante a emissão da mensagem eletrónica e a proteger a singularidade desta, ficando assim manifesto que é o próprio ato de transmissão que a lei pretende proteger na sua unicidade, irrepetibilidade e singularidade.

2.2.2. O instrumento de garantia da singularidade

A exigência de singularidade deve ser garantida mediante a utilização, na mensagem eletrónica emitida, de um método fiável. Daqui podemos extrair a conclusão de que a LMCE exige, como requisito de verificação da singularidade dos documentos eletrónicos, que as redes informáticas através das quais são efetuadas as comunicações deste tipo de documentos possuam sistemas de autenticação e de segurança que garantam de alguma forma o requisito da singularidade. Caso isso não aconteça, deve essa falta ser substituída pela existência de um mecanismo alternativo que garanta aqueles requisitos.

Qual o método de garantia da singularidade que se considera fiável, a LMCE não prevê, deixando para o intérprete e o aplicador da lei a consubstanciação desse enunciado. Acrescenta, porém, dois importantes parâmetros de aplicação, que são as circunstâncias concretas do caso e a existência de uma qualquer convenção anterior.

Esta formulação legal deixa às partes a liberdade de conformação de um meio de garantia da singularidade dos documentos eletrónicos, seja mediante convenções prévias entre elas, seja com recurso a normas aprovadas por associações e acordos modelo. Fica garantida a validade e eficácia jurídica dos documentos eletrónicos emitidos no âmbito dos contratos de transporte de mercadorias.

O regime criado pela LMCE não garante, porém, a segurança ao adquirente, da prevalência do seu direito e da correspondente proteção jurídica, no caso de outra pessoa se apresentar com documento eletrónico idêntico, que cumpra os mesmos requisitos, e reivindicar os direitos sobre as mercadorias, invocando a singularidade do documento que apresenta. Neste caso, não existirá nenhuma presunção nem ficção legal que distinga um documento do outro. O aplicador da lei terá que analisar, em face das circunstâncias específicas do caso, nomeadamente da participação das outras partes no negócio, dos métodos utilizados de garantia de singularidade, e da existência de uma

eventual convenção prévia específica ou genérica, qual dos dois documentos e direitos prevalecem. Não existe, porém, uma segurança de elevado nível, como aquela que é conferida pela visualização tangível e material dos documentos em papel, que é acessível a qualquer pessoa, porque não é suscetível de ser replicada para os documentos eletrónicos.

A LMCE estabelece apenas um quadro legal mínimo para a utilização dos meios eletrónicos para a elaboração e comunicação, de documentos com relevância jurídica.

Em conclusão, podemos dizer que a LMCE não resolve o problema da singularidade dos documentos eletrónicos, porque não cria instrumentos legais para a garantir. Porém, a LMCE, regula, pela primeira vez, a admissibilidade, com relevância jurídica, dos conhecimentos de embarque eletrónicos e a sua transmissibilidade como títulos de propriedade das mercadorias, bem como de outros títulos transmissíveis, e como instrumento probatório desses direitos, mediante a sua mera posse.

O Regulamento EIDAS viria disponibilizar novos instrumentos jurídicos suscetíveis de aumentarem a segurança dos documentos eletrónicos e a sua capacidade de constituírem títulos transmissíveis. Os selos temporais e os serviços de envio registado representam um importante avanço jurídico para a possibilidade de um maior controlo acerca da singularidade dos documentos. Os primeiros permitem determinar com rigor a data e a hora de emissão dos documentos, e se é verdade que não impedem que o mesmo emitente de um título emita outro, de seguida, também é certo que se trata de um importante instrumento de segurança.

Os serviços de envio eletrónico registado proporcionam também as condições para que um mesmo documento possa circular entre vários agentes económicos. A certificação da data do envio, bem como das partes e da integridade dos conteúdos, são também importantes instrumentos de segurança para a circulação eletrónica de títulos transmissíveis.

Apesar disso, não existe ainda um regime legal específico para esses títulos, pelo que se trata de um domínio onde ainda existem lacunas relevantes e se quanto à integridade o suporte eletrónico é o mais avançado, no que respeita à singularidade não é assim, dado que não existem, pelo menos até agora, instrumentos técnicos suficientemente eficazes para responderem à necessidade de se assegurar a singularidade dos documentos.

3. Arquivo e conservação de documentos e comunicações eletrónicas

Os documentos eletrónicos são mais vulneráveis aos riscos de fraude e de perda do que os documentos em papel, pelo que é necessária a existência de normas que regulem a sua conservação e arquivo.

Nas relações administrativas são frequentes as obrigações legais de as empresas guardarem em arquivo a sua contabilidade e os documentos de suporte, para efeitos de controlo pelos acionistas, pelas autoridades fiscais e aduaneiras, bem como para proteção dos seus credores.

Do mesmo modo, a conservação dos documentos integrantes do chamado processo administrativo, é um instrumento fundamental para que a ação dos órgãos da administração pública possa ser sindicada pelos tribunais. A existência de um processo administrativo é um direito dos administrados, mas a conservação e o arquivo dos documentos que suportam direitos e obrigações é essencial para a sua efetividade, e muitas vezes para a sua validade.[942]

Ora, os documentos em suporte eletrónico são mais vulneráveis à passagem do tempo do que os documentos em suporte de papel, pelas seguintes razões:

i) Quanto à sua disponibilidade. Enquanto a leitura e a análise de um documento em papel é imediata, isso não acontece com os documentos eletrónicos, cujo acesso depende da disponibilidade de três fatores essenciais:

   a. Um equipamento (o designado *hardware*, v.g. um computador) que disponibilize num *écran* o documento legível. A evolução tecnológica altera constantemente a configuração dos equipamentos e a sua própria estrutura. No passado essas máquinas estavam equipadas com funcionalidades que foram eliminadas por se terem tornado tecnologicamente ultrapassadas, tendo também sido abandonadas, por exemplo os leitores de disquetes, de CD, de fitas

[942] Em sede administrativa, a informatização crescente de tarefas, formalidades e diligências dos órgãos das administrações públicas conduziram, com alguma frequência, à desestruturação do chamado processo administrativo. No contexto em que todo o procedimento administrativo era instruído em papel, era relativamente fácil congregar no processo todos os documentos gerados, e essa disciplina estava incorporada nos procedimentos dos serviços da administração pública. Com a informatização, muitas diligências passaram a ser efetuadas de forma desmaterializada, e muitas vezes automatizada, pelo que, para os fins específicos da eficácia na tramitação dos procedimentos, se tornou supérfluo o seu registo em papel. Parece-nos, pois, relevante a existência de uma regulamentação legal dos procedimentos administrativos eletrónicos e da sua documentação.

magnéticas, etç. Um dos pressupostos de arquivo dos documentos eletrónicos é o de garantir que sejam suscetíveis de serem lidos por equipamentos, independentemente da data em que isso venha a ser necessário;

b. Um suporte magnético onde esteja gravado o documento, que seja acessível, utilizável e suscetível de ser lido com a tecnologia disponível das máquinas antes referidas. A evolução tecnológica muda também os suportes magnéticos, não se utilizando já os antigos cartões perfurados, as bandas magnéticas, as disquetes, etc.;

c. Um sistema informático (o designado *software*) que, operando no equipamento referido anteriormente, disponibilize o documento para leitura pelo entendimento humano. Os sistemas informáticos de produção e de leitura de documentos podem deixar de ser produzidos ou ser substituídos por novas versões, em face da inovação tecnológica, o que pode tornar os documentos elaborados no passado insuscetíveis de serem disponibilizados. Pode existir o suporte magnético onde estão gravados os dados que constituem o documento eletrónico, mas não existir o programa informático que faz a conversão e permite a disponibilização pelo computador para consulta pelas entidades que dele necessitam.

ii) Outra causa da vulnerabilidade dos documentos eletrónicos é a facilidade da sua alteração ou eliminação. A integridade é essencial à confiança jurídica, sendo que o regime da sua conservação e arquivo adquire particular relevo, em especial com a criação de normas e que haverão de garantir a durabilidade no tempo do seu conteúdo, tal como foi gerado, comunicado ou recebido;

iii) A garantia da segurança no que respeita às datas e horas, bem como aos locais em que os documentos eletrónicos foram gerados, comunicados ou recebidos. Os referenciais de tempo e lugar são determinantes da conformação dos direitos e das obrigações deles emergentes, nomeadamente no que respeita à lei aplicável e à data da constituição dos correspondentes vínculos jurídicos. Dada a vulnerabilidade dos documentos eletrónicos e a facilidade como que o seu conteúdo pode

ser alterado ao longo do tempo, a segurança quanto à integridade e inalterabilidade destes elementos adquire natural relevo.

iv) O próprio conceito de documento. A necessidade de um regime jurídico do arquivo dos documentos eletrónicos é também importante para a definição do próprio conceito de documento eletrónico. Muitas mensagens eletrónicas são apenas impulsos transmitidos entre computadores para serem tecnicamente eficazes, ou seja, para produzirem efeitos informáticos. Os computadores e os sistemas informáticos operam mediante impulsos eletrónicos de receção e resposta e mediante a produção de uma consequência sempre que existe uma causa, não sendo necessário para o seu funcionamento que fique registo do conteúdo das mensagens transmitidas. Quando recebe um impulso (causa ou *input*), o sistema informático produz uma consequência (efeito ou *output*) e esse procedimento é mecânico, automático e imediato. Para os efeitos de funcionamento do sistema não é necessária a geração de um documento que evidencie essas interações, nem o seu conteúdo, nem a sua data e lugar. Apesar disso, muitas dessas interações são verdadeiros documentos, e são-no sempre que se produzem efeitos jurídicos a partir delas. Porém, para que deles fique constância, é necessário que o sistema informático produza esse documento com todos os elementos jurídicos relevantes para a apreciação dos seus contornos e dos seus efeitos jurídicos.[943] Mas a produção desse documento é um ato exterior ao funcionamento do sistema e deve ser um dos elementos essenciais da programação do sistema informático e do seu funcionamento. Para que como documentos possa a sua eficácia perdurar no futuro com segurança jurídica, é necessário que sejam autonomizados como entidades próprias e guardados em arquivo, com o mesmo conteúdo, autenticação e forma com que produziram os efeitos jurídicos quando foram emitidos e fizeram operar os sistemas informáticos;

[943] Muitos sistemas informáticos guardam registo destes acontecimentos nos designados *logs*, mas trata-se apenas de controlos técnicos que rastreiam as interações dos sistemas, que não possuem formato de documento. A lei deveria exigir não só os casos em que é obrigatória a conversão desses *logs*, mas também as situações em que os sistemas geram documentos.

v) Finalmente a intervenção de entidades terceiras que prestem serviços de confiança jurídica nas transações eletrónicas. Nos documentos em suporte de papel, a intervenção de notários na emissão de documentos, na sua autenticação ou no reconhecimento de assinaturas, confere uma confiança e segurança jurídica acrescida. Esses serviços de confiança podem ser relativos, tanto ao próprio conteúdo dos documentos, incluindo as declarações negociais, como à identidade das partes e ao tempo e lugar da prática dos atos. Nos documentos em suporte eletrónico a necessidade de intervenção de entidades terceiras que prestem serviços de confiança é ainda maior, dada a vulnerabilidade dos documentos, especialmente no que respeita às garantias da integridade, da originalidade e dos referenciais de data, hora e lugar da produção, comunicação ou receção dos documentos eletrónicos, bem como no que respeita à própria identidade das partes intervenientes e à segurança quanto à sua participação pessoal, exclusiva e direta nos respetivos documentos.

A LMCE vem responder a estas questões, estabelecendo, de forma inovadora, um conjunto de requisitos fundamentais de arquivo dos documentos eletrónicos. Trata-se do primeiro corpo de normas com relevo jurídico, reguladoras desta matéria. Essas normas traduzem-se em dois princípios gerais e um específico de arquivo e conservação. Os princípios gerais são os seguintes:[944]

i) O princípio da acessibilidade para ulterior consulta. Trata-se de um requisito evidente, mas bem se compreende a sua consagração legal, dado o conjunto de instrumentos técnicos e lógicos cuja disponibilidade é indispensável para se poder aceder aos próprios documentos.[945] Este princípio tem carácter genérico, englobando a inteligibilidade e a suscetibilidade de análise e tratamento, bem como a disponibilidade de

[944] Seguimos o artigo 10.º da LMCE, sob o título de "Conservação das mensagens eletrónicas". "Guide to Enactment LMCE (1996)", pág.s 7 e 8.

[945] Ponderou-se a inserção na LMCE, dos conceitos de legibilidade, inteligibilidade, interpretabilidade, durabilidade e inalterabilidade, mas entendeu-se ser mais abrangente e objetiva a utilização do conceito de *"acessível para posterior consulta"*. *"The use of the word "accessible" was meant to imply that information in the form of computer data should be readable and interpretable, (...). It was also stated that the word "usable" was not intended to cover only human use but also computer processing. As to the notion of "subsequent reference", it should be made clear that it had been preferred to such notions as "durability" or "non-alterability", which would have established too harsh standards, and to such notions as "readability" or "intelligibility", which might constitute too subjective criteria"*. "A/CN.9/407", par. 56.

acesso e os meios correspondentes, porque é um pressuposto essencial da própria existência jurídica dos documentos eletrónicos. Esta disponibilidade para consulta não se refere apenas à consulta por humanos, e inclui a possibilidade de os respetivos dados serem recebidos ou tratados por outros sistemas informáticos;[946]

ii) O princípio da integridade. Este princípio corresponde à necessidade de proteger os documentos eletrónicos contra a sua maior vulnerabilidade e a da facilidade com que podem ser alterados sem que essa alteração deixe vestígio. A LMCE estabelece que o sistema de arquivo deve assegurar a conservação dos documentos *"no estado em que foram gerados, comunicados ou recebidos"*. Essa garantia pode ser assegurada mediante uma reprodução direta e imediata do próprio conteúdo das mensagens, ou então mediante um formato próprio, quando for possível demonstrar especificamente que esse formato *"reproduz com exatidão a informação gerada, enviada ou recebida"*.[947] A LMCE não especificou como se garante a efetividade deste princípio, pelo que ficaram sem definição legislativa as questões relativas às regras de segurança quanto ao modo de arquivo e de conservação dos documentos.[948] Porém, se essa lacuna pode ser

[946] A LMCE não especifica sobre quem recai a obrigação de garantir a verificação dos pressupostos da acessibilidade, mas será da responsabilidade de quem efetua esse arquivo, sendo indispensável para que se cumpram os requisitos de arquivo e conservação. Trata-se, por exemplo, dos casos em que as leis tributárias obrigam as empresas e os sujeitos passivos de impostos a guardar os documentos referentes a despesas ou os que são necessários ao exercício de direitos de natureza tributária, como é o caso do direito à dedução em sede do IVA e o correspondente direito a reembolso quando se cumpram os pressupostos legais. Nesses casos a verificação dos requisitos de arquivo é um pressuposto essencial para a própria validade desses documentos eletrónicos e para que os direitos correspondentes possam ser exercidos.

[947] Esta formulação pode parecer ambígua. Por um lado exige-se que o documento seja conservado no formato em que foi gerado, numa formulação rígida e fechada. Por outro lado, logo de seguida, parece que se abre a possibilidade de uma maior maleabilidade, bastando-se a lei com a suscetibilidade de o documento ser reproduzível com exatidão. O que se pretende é manter rigor no que respeita à integridade dos documentos, mas sem prejuízo das técnicas próprias de gravação e de arquivo através dos meios eletrónicos. Para efeitos de arquivo, os documentos necessitam de ser codificados e comprimidos, sendo depois, quando a sua consulta é necessária, descomprimidos e descodificados. Essas operações técnicas têm a sua especificidade e podem produzir ligeiras modificações, embora meramente instrumentais nos documentos, sem alterar o seu conteúdo. É por essa razão que a LMCE adota esta formulação. Como se refere nas notas explicativas, *"It would not be appropriate to require that information should be stored unaltered, since usually messages are decoded, compressed or converted in order to be stored".* "Guide to Enactment LMCE (1996)", pág. 47.

[948] Nos trabalhos preparatórios identificara-se um conjunto de questões que se colocam nesta matéria, como sejam as relevantes ao modo de arquivo dos documentos, às medidas de segurança contra a alteração dos documentos arquivados, à manutenção dos sistemas de arquivo e aos métodos de autenticação. *"The following factors were mentioned as suitable for inclusion in the uniform rules:*

> superada mediante uma previsão legal que consagre a sua validade como elemento de prova em tribunal e perante a administração pública, já não o será no que respeita ao cumprimento de obrigações legais de arquivo pelas empresas, quando a lei assim o estabeleça, nomeadamente para fins tributários, como antes se referiu. Nos casos em que a lei estabelece a obrigação de as empresas guardarem a sua contabilidade e os respetivos documentos de suporte, esse requisito não estará cumprido se não se verificarem reunidos todos os pressupostos de segurança na sua conservação, não se podendo aplicar aqui qualquer margem de apreciação, porque a lei também não a prevê para estas situações. É por essa razão que não tiveram sucesso, em termos de produção de legislação interna dos estados, as normas de arquivo dos documentos eletrónicos da LMCE.[949]

A LMCE consagra também a possibilidade de a conservação e o arquivo dos documentos eletrónicos serem efetuados por entidades terceiras que sejam prestadores de serviços, sempre que se cumpram, naturalmente, os requisitos legais que antes enunciámos. A intervenção de entidades especializadas na prestação de serviços de confiança e de segurança jurídica adquiriu uma importância crescente, dada a qualidade especializada dos serviços que prestam, bem como pelo facto de, sendo entidades terceiras, poderem ter um papel importante no que respeita à prova produzida em face dos respetivos documentos.

A Diretiva 1999/93/CE não contém qualquer norma relativa ao arquivo e à preservação dos documentos eletrónicos e das respetivas garantias de autenticidade e de

---

method of recording data; adequacy of measures protecting against alteration of data; proper maintenance of data carriers; and methods used for authentication of EDI messages.". "A/CN.9/373", par. 102. Reconhecida esta necessidade de regulamentação específica, dada a relevância dos sistemas de arquivo em matéria de segurança jurídica dos documentos eletrónicos, não foi dado esse passo, porque naquele contexto não existiam ainda disponíveis instrumentos tecnológicos capazes de corresponder a essas necessidades.

[949] A regulamentação legal do regime de arquivo dos documentos eletrónicos é um instrumento fundamental para a desmaterialização dos arquivos, tanto das empresas como das administrações públicas. Os custos dos arquivos em papel são agravados pelo facto de atualmente muitas empresas e entidades públicas operarem em simultâneo com documentos eletrónicos e documentos em papel, sendo certo que para cumprirem obrigações legais, nomeadamente de contabilização e arquivo para efeitos tributários, e mesmo que para efeitos da organização interna das empresas, necessitam de converter em papel, para efeitos de arquivo, documentos que estão em suporte eletrónico. Essa necessidade de diminuir os custos de armazenamento era uma das preocupações que estava presentes nos trabalhos preparatórios da elaboração da LMCE, como se reconhece no seguinte trecho: *"The prevailing view, however, was that it would be desirable to have a such rule, which should be restricted to validating storage of records in electronic or similar form, since the rule would increase opportunities for reducing the cost of storage of records"*. "A/CN.9/373", par. 124.

integridade. E esse facto era identificado como uma das causas que impediu o crescimento da utilização das assinaturas eletrónicas.[950] Em 2012, um documento da CE vem conferir a este problema uma importância maior. O objetivo do documento é o de criar condições para que os dados eletrónicos das administrações públicas possam ser disponibilizados e partilhados, sempre que não estejam sujeitos a um qualquer regime de sigilo ou de reserva, mas sempre no contexto geral de um pressuposto fundamental para isso, que é o da existência de um regime de arquivo e de preservação que seja regulado em termos legislativos.[951] E a necessidade de preservar no tempo os registos dos documentos, bem como a tecnologia que permita a sua leitura, e a verificação da sua autenticidade e integridade, são importantes constrangimentos.[952]

O Regulamento EIDAS veio revelar a importância deste problema e prever a existência de um novo serviço de confiança, no artigo 34.º, que é o serviço qualificado de preservação de assinaturas eletrónicas qualificadas. Trata-se de um serviço destinado a preservar a tecnologia das assinaturas eletrónicas para além do prazo da sua validade tecnológica, permitindo assim prolongar no tempo os seus efeitos de autenticação sobre os documentos eletrónicos. Este serviço aplica-se também aos selos eletrónicos, nos termos do artigo 40.º. Por outro lado as previsões relativas aos institutos dos selos temporais e dos selos eletrónicos são importantes instrumento para que no futuro venha a existir um regime jurídico do arquivo dos documentos eletrónicos, em especial no domínio administrativo, como analisaremos no último capítulo do nosso trabalho.

---

950 *"Outra razão prática para a relutância na implantação das aplicações de assinatura eletrónica é o facto de o arquivamento dos documentos com assinatura eletrónica ser considerado demasiado complexo e incerto"*. COM(2006) 120 final, pág. 8.

951 O documento começa por se referir aos dados eletrónicos com *"uma moeda de inovação"* e como a *"seiva da economia do conhecimento"*, seguindo o relatório "Digital Britain" do governo inglês, de 2009, e estabelece o objetivo da*"introdução do princípio de que todas as informações públicas não expressamente abrangidas por uma das excepções são reutilizáveis para fins comerciais e não comerciais"*. COM(2011) 882 final, pág. 9. O acesso a este tipo de dados em arquivo desenvolve-se em duas dimensões: Por um lado a possibilidade de os documentos das administrações públicas serem reutilizados em procedimentos administrativos diferentes, incluindo por outros órgãos, o que implica um sistema de arquivo com garantias de autenticidade e de integridade, bem como de partilha e de acesso, que poderá, ou não, depender de indicação dos interessados. Por outro lado a disponibilização do acesso a dados constantes das bases de dados das administrações públicas que sirvam para a realização de estudos e investigações, sendo citados com exemplo os estudos sobre o tráfego urbano *("o processamento dos padrões de consumo de energia com vista a melhorar a eficiência energética ou dos dados referentes à poluição na gestão do tráfego"*), bem como a investigação científica sobre saúde pública (*"Os progressos a nível da genómica, da descoberta de drogas e do diagnóstico e tratamento de doenças graves como o cancro ou a insuficiência cardíaca dependem cada vez mais de técnicas sofisticadas de recolha e análise de dados"*). COM(2011) 882 final, pág. 3.

952 Como se refere no relatório que vimos citando, a necessidade de garantir a legibilidade e os restantes atributos dos documentos eletrónicos, *"exige tecnologia e procedimentos onerosos e complexos para assegurar a legibilidade e a verificação de que tais períodos são respeitados"*. COM(2011) 882 final, pág. 8.

O regime jurídico da conservação e do arquivo de documentos eletrónicos necessita ainda de ser desenvolvido.[953]

4. A admissibilidade de prova mediante documentos eletrónicos

4.1. Problemática

A eficácia probatória autónoma dos suportes eletrónicos, para fins judiciais ou administrativos é essencial à sua utilização no tráfego jurídico. E a primeira preocupação dos organismos internacionais na criação de um regime jurídico dos meios eletrónicos centrou-se eliminação dos entraves legais a essa admissibilidade.[954]

A função dos meios eletrónicos nas relações jurídicas é idêntica à do papel. São suportes de consignação da informação que deles consta, o que permite a sua transmissão e acessibilidade a terceiros, sendo que é essa informação que é fonte de relevância e de efeitos jurídicos.[955] A função dos suportes documentais, tanto eletrónicos como físicos (como é o caso do papel) é apenas instrumental, sem qualquer diferença entre eles, mas a sua relevância é determinante como instrumento de durabilidade das relações emergentes dos elementos informativos que deles constam, e como forma de fazer prevalecer no futuro os respetivos efeitos.

Esta identidade de funções do papel e dos suportes eletrónicos não permite, porém, que se apliquem a estes, sem mais, os regimes de prova que a lei estabelece para o papel, porque os suportes eletrónicos levantam problemas próprios em matéria

---

[953] A Comissão Europeia aprovou, por Decisão da Comissão, de 7 de julho de 2014, que alterou o Regulamento Interno (2004/563/CE Euratom), o regime dos documentos eletrónicos internos da Comissão, que inclui um conjunto de normas relativas ao arquivo eletrónico desses documentos.

[954] Como refere o Professor Pacheco de Andrade, "*a possibilidade ou impossibilidade de prova das transacções electrónicas assume-se como factor crucial para o próprio desenvolvimento do comércio electrónico*". Andrade, F. C. P. (2003*). Contratação Electrónica e Recurso a Sistemas Multi-Agentes: questões de representação e responsabilidade*. http://wiki.di.uminho.pt/twiki/pub/Research/Doutoramentos/SDDI2005/FranciscoAndrade.pdf. A via mais imediata era a da equiparação dos documentos eletrónicos aos documentos em papel, apesar da diferença estrutural entre os dois tipos de suporte: *"Because of its physical characteristics, the traditional paper document is accepted as evidence. It is durable, and changes or additions will normally be clearly visible. The electronic document is quite different. It takes the form of a magnetic medium whose data content can be changed at any time. Changes or additions will not appear as such"*. A/CN.9/WG.IV/WP.53, pág. 380.

[955] Tanto o papel como os suportes eletrónicos são apenas meios de transmissão, quer no tempo (preservação) quer no espaço, de informação. *"The paper and the data communication Iinks are only media for carrying information"*. A/CN.9/WG.IV/WP.53, pág. 380.

probatória, que não são resolúveis com a aplicação das previsões legais existentes para o papel, nomeadamente os seguintes: [956]

ii) Os problemas da integridade e da autenticidade dos documentos cujo controlo é mais difícil nos documentos eletrónicos do que no papel, dada a facilidade com que podem ser alterados sem deixar vestígio. Esse problema respeita não só aos documentos eletrónicos, como também àqueles que resultam da digitalização de documentos em papel. Esta transição implica a perda das garantias de autenticidade dos documentos em papel, a partir do momento em que os dados são transpostos para o computador podem ser alterados.[957] Os sistemas informáticos possuem capacidades de alteração dos documentos praticamente impercetíveis, sendo que essa facilidade não existe quando o documento está apenas registado no papel.[958]

A garantia da autenticidade é mesmo uma das primeiras causas da necessidade de legislar a relevância probatória dos suportes eletrónicos, nas operações bancárias, onde se verificaram as primeiras situações de fraude mediante o designado roubo de identidade, em que uma pessoa, com intuitos fraudulentos, utiliza os dados de outra pessoa, simulando ser ela. Nesses casos, a não exigência legal da autenticação das comunicações eletrónicas é suscetível de deixar desprotegida a vítima destas situações, nomeadamente perante as entidades bancárias.[959]

---

[956] *"There is a widely felt sense of insecurity over the perceived inadequacies in the law governing the use of computer records as evidence. This sense of insecurity may be in its own right an inhibition to the development of new patterns of trade documentation based on computers"*. "A/CN.9/265", par. 77.

[957] Essa vulnerabilidade era um importante motivo de preocupação, como se denota da seguinte transcrição: *"Unauthorized alterations of records, which are facilitated by remote access to the computers storing the records, are of serious concern to the enterprises whose records have been a1tered, and raise many legal questions in regard to civil and criminal liability for those acts and for their consequences. More serious problems for the legal acceptability of computer records are raised by the possibility that the enterprise itself might deliberately alter its records, since this possibility casts doubt on the credibility a. evidence of all computer stored records"*. "A/CN.9/265", par. 24.

[958] *"Firstly, data capture does not allow for testing whether the paper document had been altered as to content or authentication prior to its transformation into the new form for storage. Secondly, the content of the-original paper record may not have been accurately captured and transformed into a computer record"*. "A/CN.9/265", par. 45.

[959] O Relatório do Secretário-Geral chama a atenção para esses casos que desprotegeriam os clientes das entidades bancárias. *"It would be a practical impossibility for the customer to raise such doubts about the bank's computer system or procedures"*. "A/CN.9/266/Add.2", pág. 29. Particularmente nos sistemas de "Common Law", era muito difícil aos clientes individuais das entidades bancárias, assumirem o ónus da prova do deficiente funcionamento dos sistemas, o que deixava muito desprotegidos os clientes das entidades bancárias, que não possuíam qualquer meio de, por si mesmos, demonstrarem, que os sistemas informáticos dos bancos não funcionaram adequadamente.

iii) A questão da própria natureza dos documentos e dos registos eletrónicos, que na sua essência são apenas dados binários em suporte digital. A resposta a este problema foi dada com a exigência da sua legibilidade como pressuposto da sua validade probatória.[960] Essa exigência é um dos pressupostos essenciais da própria validade dos registos eletrónicos.[961]

iv) A segurança quanto ao arquivo dos documentos é muito importante, como referimos no capítulo anterior;

v) A segurança quanto à transmissão e comunicação dos dados e dos documentos, nomeadamente os instrumentos probatórios da sua efetiva emissão, receção, bem como as respetivas datas e lugares;

vi) A acessibilidade aos documentos é, naturalmente, um requisito essencial para a sua validade como elemento de prova. Este requisito é específico dos documentos eletrónicos, em que o imediatismo sensorial que é próprio do papel não é possível, uma vez que o acesso ao seu conteúdo tem que ser mediado por um suporte magnético onde esteja gravado, uma máquina, e um sistema informático que através dela o abra e o disponibilize para leitura ou análise. Sem esse requisito não podemos dizer que exista sequer documento.[962]

vii) Do mesmo modo, levantam-se problemas no que respeita ao valor probatório dos documentos eletrónicos em países estrangeiros. Essa matéria é particularmente relevante neste domínio, onde muitas transações são efetuadas à distância.[963]

---

[960] A versão final do Guia Jurídico da Transferência Eletrónica de Fundos, de 1987, reconhece um princípio de não discriminando dos documentos só pelo facto de estarem em forma eletrónica, com a única condição de serem legíveis e compreensíveis. "*The rules of evidence must give bank records kept in computer readable form or produced from computer-based entries the same legal value as records kept in paper-based form*". A/CN.9/221, pág. 116.

[961] A questão da legibilidade limita a equiparação dos documentos eletrónicos aos documentos em papel, deixando, porém, de fora, outros tipos de suportes eletrónicos, como por exemplo os filmes e as gravações sonoras. *"The record as stored in a computer in electronic form cannot be read or interpreted by a human being. Therefore, it cannot be presented to a tribunal unless it takes on a visual form, either on a visual display unit which the tribunal can see or on a print-out. According to the replies to the questionnaire, both means of presenting tbe data to the court are in use"*. "A/CN.9/265", par. 47.

[962] Um documento eletrónico só pode ser suscetível de valor jurídico caso seja legível, naturalmente. *"A suggestion was made that the proposed provision should make it clear that computer-generated evidence, in order to be presented in evidence, had to be in a "tangible" or "human-readable" form"*. "A/CN.9/373", par. 98. E embora este requisito não conste do artigo 10.º da LMCE, ele está implícito no conceito de acessibilidade do artigo 9.º.

[963] *"There does not as yet appear to be any experience whether computer records created in one country will be usable as evidence in the courts of another country on the same conditions as computer records*

A procura de caminhos de reconhecimento do valor probatório dos documentos eletrónicos era exigida pelas vantagens da sua utilização pelas empresas,[964] mas a falta de garantias jurídicas da validade e eficácia probatória desses documentos era um fator de insegurança.[965] Por essa razão várias iniciativas foram adotadas no domínio jurídico, em ordem à superação do problema, nomeadamente as seguintes:

i) O Conselho de Cooperação Aduaneira que emitiu a recomendação de 16 de junho de 1981 onde exorta os Estados Membros a aceitarem a comunicação eletrónica das declarações aduaneiras de bens no trânsito internacional, e que consagre e regule o valor probatório dos documentos e das comunicações eletrónicas;

ii) O Working Party on Facilitation of International Trade Procedures recomendou a admissibilidade como meio legal de prova dos registos informáticos guardados nas bases de dados dos computadores, nomeadamente as comunicações eletrónicas entre as empresas e as administrações aduaneiras, em especial as entregas das respetivas declarações relativas às mercadorias que sejam objeto de tratamento aduaneiro;[966]

iii) A aprovação, em 1981, pelo Conselho da Europa, da recomendação para os países membros equiparem na lei os documentos eletrónicos aos documentos em papel, para efeitos probatórios, dispensando as empresas da necessidade de manterem arquivos em papel.[967] Propunha ainda uma presunção legal de que as reproduções dos documentos

---

created in the second country. Any difficulties in this regard would be of serious concern for international electronic funds transfers.". "A/CN.9/266/Add.2", pág. 16.

[964] Essa maior eficiência tornou irresistível a expansão da utilização das novas tecnologias: *"The decreasing cost of telecommunications and the increasing cost on ground and air transportation has made it less expensive for banks to transmit large numbers of funds transfer instructions of large and small value in a batch mode by telecommunications, particularly when lower tariffs are offered during the night and other periods of under-utilization"*. "A/CN.9/250 and Add.1 to 4", pág. 128.

[965] Esta problemática é refletida pela UNCITRAL logo em 1982, nomeadamente no seguinte trecho: *"there remains a hesitance in some countries to admit computer records as evidence before courts and arbitral tribunals. It is thought that the current state of techniques in the matter of recordings on computers does not give sufficient guarantees against falsification"*. A/CN.9/221, pág. 20.

[966] O Conselho de Cooperação Aduaneira recomenda expressamente que os estados membros façam *"a study of changes which are necessary to national laws to admit as evidence information stored on computer"*. A/CN.9/221, pág. 22.

[967] Recommendation No. R (81) 20, of the Committee of Ministers to Member States on the Harmonization of Laws Relating to the Requirement of Written Proof And to the Admissibility of Reproductions of Documents And Recordings on Computers. (Adopted by the Committee of Ministers on 11 December 1981 at the 341st meeting of the Ministers' Deputies), disponível em https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=600958&SecMode=1&DocId=674076&Usage=2 (última consulta em 19/6/2015).

eletrónicos sejam cópias fiéis dos originais, salvo prova em contrário.[968] Essa equiparação pressupunha garantidas prévias de segurança, que naquela época não existiam ainda;[969]

iv) A UNCITRAL reconheceu, no relatório do Secretário-Geral, de 17/5/1981, a necessidade de normas jurídicas que, aproveitando os progressos da tecnologia, previssem em que termos os documentos eletrónicos podem ter valor jurídico, nomeadamente para efeitos probatórios em processos judiciais;[970]

v) O relatório do Secretário-Geral, de 30/4/1985, acerca do projeto de Guia Jurídico da Transferência Eletrónica de Fundos, considerou não existirem normas específicas acerca do valor probatório dos documentos eletrónicos, mas que esse facto não os excluía como elementos de prova. Esse relatório, que é um importante documento na história do direito das novas tecnologias, separa três tipos de regimes jurídicos então vigentes:[971]

   a. Os sistemas processuais da "*Common Law*", caraterizados pelo paradigma da oralidade e do contraditório, e onde a prova testemunhal direta prevalece sobre as restantes.[972] Nestes sistemas não é aceite a prova indireta (*hearsay evidence)* por exemplo, os factos que uma testemunha conhece de outra pessoa, de um livro ou

[968] *Idem*, pág. 22. No texto original: *"be presumed to be a correct and accurate reproduction of the original document or recording of the information it relates to, unless the contrary is proven"*.

[969] O objetivo era proporcionar às empresas a possibilidade de copiarem para suporte eletrónico a documentação e dispensá-las de guardarem cópias dos originais em papel (como se diz na nota justificativa da recomendação, *"increasingly, use is being made in business of processes of document reproduction by microfilming and of techniques for recording of information on computers, the originals, if they exist, being destroyed to save storage space and cost"*). A recomendação pretendia que se estabelecesse uma presunção de que as cópias microfilmadas possuem o mesmo valor probatório dos originais em papel, mesmo que estes tivessem sido destruídos. Essa presunção dependia, porém, da verificação de um conjunto de pressupostos, por exemplo as garantias de preservação das cópias microfilmadas contra qualquer alteração (alínea d) do artigo 3.º), a garantia de reprodução da imagem, de forma legível, bem como sem cortes nem eliminações (n.º1 e 2 do artigo 3.º), a garantia da adequada arquitetura e segurança dos sistemas informáticos de gravação, de armazenamento e de reprodução (artigo 5.º). Trata-se, naturalmente, de importantes instrumentos jurídicos de segurança, mas que, naquela época, não podiam ser acompanhados dos meios tecnológicos que os assegurassem.

[970] A/CN.9/221, pág. 24.

[971] "A/CN.9/265", parte II, par. 27 e seguintes.

[972] São enunciados como integrando este grupo de países *"Australia (some jurisdictions), Philippines, United Kingdom, United States)"*. "A/CN.9/265", pág. 26.

de um documento.[973]. Esta regra tem, porém, exceções, em especial para o que interessa à nossa investigação, a aceitação como prova dos documentos comerciais produzidos no âmbito normal da atividade empresarial.[974] Daqui resulta ser admissível, em princípio, a prova mediante registos em suporte eletrónico, quando se reportem a atos normais da atividade comercial. Alguns países anglo-saxónicos estabeleceram normas no sentido da aceitação da prova mediante registos em suporte eletrónico, mas condicionada à prévia demonstração do adequado funcionamento e segurança do sistema informático que os gerou;[975]

b. Os sistemas abertos de prova, que aceitam todos os elementos probatórios que as partes entendam relevantes para a apreciação do litígio. Nestes sistemas a prova mediante registos eletrónicos é normalmente aceite, sem prejuízo da sua impugnação;[976]
c. Os sistemas de enunciação taxativa dos elementos de prova, cuja maioria dos países havia efetuado, ou estava em curso de efetuar, ajustamentos legislativos no sentido de incluir os registos e documentos eletrónicos como meios de prova.[977]

---

973 *"What he knows through a secondary source, e.g. another person, a book or a record of an event, is denominated 'hearsay evidence', and, in principle, the tribunal cannot receive it as evidence"*. "A/CN.9/265", par. 31.

974 *"A business record created in the ordinary course of commercial activity may be received as evidence even though there may be no individual who can testify from personal knowledge and memory as to the particular record in question"*. "A/CN.9/265", par. 32.

975 "*In common law countries it is the usual rule that computer records can be admitted as evidence only if the proponent of the record establishes certain facts about the record and the computer system. The most important is that the system has been properly designed and sufficiently well-managed so that the possibility that the data stored in the record is incorrect is reduced to a minimum*.". "A/CN.9/266/Add.2" pág. 15.

976 São enunciados como exemplo: *"Austria, Colombia, Czechoslovakia, Denmark, Finland, Germany, Federal Republic of, Honduras, Japan, Mexico, Norway, Portugal, Sweden, Yugoslavia, Zambia"*. "A/CN.9/265", pág. 26.

977 A UNCITRAL refere os casos de *"Burma, Chile, Dominican Republic (...) Luxembourg, Senegal, Venezuela"*. "A/CN.9/265", pág. 27. Também em França, a *Loi du 12 juillet 1980*, relativa à prova dos atos jurídicos, veio prever o reconhecimento jurídico dos novos meios de prova, em especial das fotografias e das microfilmagens dos documentos em papel, que a doutrina logo haveria de interpretar como englobando também a admissibilidade dos documentos eletrónicos. Cf. "A/CN.9/350", par. 57. Do mesmo modo no Luxemburgo, a partir de 1986 passou a existir legislação expressa a admitir a prova por meios eletrónicos. Essa legislação, pelo seu caráter percursor, era citada no relatório TEDIS, nos seguintes termos: *"According to the terms of revised art. 1348 of the Luxembourg Civil Code cited above, these reproductions and recordings have the same probative value as the written documents of a private agreement of which they are, unless proved otherwise, presumed to be faithful reproductions or recordings, in the case where the originals have been destroyed on a regular basis and where they comply with the terms set out in the Grand Ducal Regulation of 22 December 1986, in accordance with*

No contexto tecnológico anterior às redes fechadas, entendia-se que a legislação internacional, apesar de não prever a prova por documentos eletrónicos, também não a impedia, e que, não existindo obstáculos legais à sua validade, não seria necessária qualquer recomendação no sentido de se legislar nessa matéria.[978]

Mas a emergência das redes eletrónicas, primeiro fechadas e depois abertas, logo desvelaria as insuficiências desse entendimento.

O modo de conferir autenticidade até então existente, era o da assinatura manual autógrafa, e essa era uma forma de autenticação típica do papel. Todas as normas até então existentes, relativas à assinatura, referiam-se à assinatura em papel, autógrafa e manuscrita. Nesse contexto, não havia forma de assinar um documento eletrónico, com o conceito de assinatura que então existia, ou seja, com uma assinatura manuscrita, colocada num suporte de papel. Essa operação não podia ser realizada nos registos em suporte eletrónico.[979]

Os atributos antes referidos são essenciais para que os documentos eletrónicos produzam prova perante as entidades judiciais e administrativas, bem como perante terceiros. E se na esfera do procedimento administrativo é possível que a entidade competente aceite a informação constante de suportes eletrónicos, dado o interesse primordial da informação, mais do que da forma, para a finalidade do procedimento, em sede de processo judicial as exigências de forma prescritas na lei devem sempre ser respeitadas.[980]

A necessidade de regular a admissibilidade dos documentos eletrónicos como meio de prova, intensificou-se com a generalização da utilização do EDI nas transações

---

arts. 1348 of the Civil Code and 11 of the Commercial Code described above". "TEDIS Report", pág. 180.

978 Esse foi o entendimento expresso pela UNCITRAL, no Relatório do Secretàtio-Geral de fevereiro de 1985: *"In most legal systems there are no major obstacles to the use of computer records as evidence. Therefore where a document is required primarily to facilitate subsequent proof of the existence of the transaction and its terms, a document in computer-readable form would often be sufficient"*. A desnecessidade de recomendar a adoção de alterações legislativas específicas acerca da prova mediante registos eletrónicos está também sublinhada no seguinte trecho: *"Almost all of the countries that replied to the questionnaire appeared to have legal rules which were at least adequate to permit the use of computer records as evidence and to permit the court to make the evaluation necessary to determine the proper weight to be given to the-data or document"*. E, em consequência, *"it seems-neither advisable nor necessary to attempt to unify the rules of evidence regarding the use of computer records in international .trade"*. "A/CN.9/265", par.s 60, 75 e 77.

979 *"A more serious legal obstacle to the use of computers and computer-to-computer telecommunications in international trade arises out of requirements that documents be signed or that documents be in paper-based form"*. "A/CN.9/265", par. 79.

980 *"In the administrative sphere, the focus tended to be on the gathering of information and greater discretion on the part of the administrative authority, with generally less emphasis than in the sphere of judicial or arbitration proceedings on evidentiary rules and procedures"*. "A/CN.9/WG.IV/WP.55", par. 37.

comerciais entre as empresas. Essa necessidade foi sendo suprida pelo trabalho das organizações internacionais, na elaboração de acordos-quadro ou de códigos de conduta, onde recomendavam aos seus associados a salvaguarda da eficácia dos documentos eletrónicos mediante uma de duas vias possíveis. [981] Por um lado a inclusão, nos contratos celebrados entre as partes, de normas que estabelecessem a equiparação das mensagens eletrónicas a documentos escritos.[982] Por outro lado a inclusão de cláusulas contratuais de renúncia mútua entre as partes, à impugnação da validade jurídica dos contratos celebrados através de EDI, com fundamento no seu suporte eletrónico, bem como do valor probatório dos respetivos documentos.[983] Estes acordos, pela sua diversidade, desempenharam um papel importante na sedimentação da necessidade de se conceber um regime de referência que, sendo tendencialmente uniformizador, pudesse ser um fator de simplificação e de eficiência, desafio que a UNCITRAL assumiu.[984]

4.2. As soluções legislativas

Nos trabalhos de conceção da LMCE assumiu-se que a relevância jurídica dos documentos e das comunicações eletrónicas para efeitos de prova dependia da consignação em lei dos seguintes pressupostos fundamentais:[985]

---

[981] São referidos em especial o Acordo TEDIS, o Acordo EDICC, o Acordo da American Bar Association (ABA) e o acordo SITPROSA. "A/CN.9/350", par.s 73 a 76 e 82. Esses acordos modelo estabeleciam em geral, que nenhuma das partes deveria impugnar nenhum ato ou contrato com o fundamento de que todas ou alguma das suas cláusulas constasse em suporte eletrónico ou que alguma das relações jurídicas a ele submetidas tivesse sido estabelecida por meios eletrónicos. Como exemplo citamos o caso o artigo 10.1 do Acordo TEDIS: *"The parties ... expressly waive any rights to bring an action declaring the invalidity of a transaction concluded between themselves on the sole ground that the transaction arises from the operation of an information system"*. *Idem*, par. 78.

[982] *"EDI messages were defined as written documents by mutual agreement of the parties"*. "A/CN.9/360", par. 40.

[983] *"The second approach relied upon a mutual renunciation by the parties of any rights or claims to contest the validity or enforceability of an EDI transaction under possible provisions of locally applicable law relating to whether certain agreements should be in writing or manually signed to be binding upon the parties"*. "A/CN.9/360", par. 40.

[984] *"The variety of contractual arrangements has sometimes been described as hindering the development of a satisfactory legal framework for the business use of EDI" ... "Another conclusion from the preliminary studies is that such a basic framework can, to a certain extent, be created by contractual arrangements between parties to an EDI relationship"*. "A/CN.9/350", par. 109.

[985] Esse reconhecimento é expresso em vários documentos dos trabalhos preparatórios, nomeadamente o seguinte:*"It was, however, considered useful to include in the uniform rules factors or guidelines to be taken into account in evaluating computer-generated evidence. The purpose of these factors or guidelines would be to assist the trier of fact in the taking of evidence and to increase the level of certainty in the use of EDI records, without thereby eliminating the principle that it was up to the trier of fact to evaluate evidence taking into account all relevant circumstances. The following factors were mentioned as suitable*

i) O estabelecimento de requisitos legais para o arquivo;

ii) A consignação de regras legais que assegurassem a manutenção dos suportes dos dados, bem como dos sistemas que proporcionam a sua disponibilização para serem lidos pelo entendimento humano;

iii) A criação de medidas jurídicas que assegurassem a integridade;

iv) O estabelecimento de métodos de autenticação que assegurassem a sua origem.

A LMCE estabelece um conjunto de normas tendentes a alcançar essa uniformização internacional e a promover a incorporação no direito interno de cada país, da relevância probatória dos documentos eletrónicos.[986] Podemos agrupar as medidas legislativas adotadas, nos seguintes termos:

i) O estabelecimento de uma norma geral de equivalência funcional dos documentos eletrónicos aos documentos em papel, traduzida no princípio da não discriminação dos documentos, só pelo facto de se apresentarem em suporte eletrónico. Esta regra está consignada na parte inicial do n.º 1 do art.º 9.º, que prevê o afastamento da aplicação de qualquer norma que estabeleça a discriminação negativa dos documentos só pelo facto de se apresentarem em suporte eletrónico;[987]

ii) O estabelecimento de normas de equivalência entre os documentos em papel e os documentos eletrónicos, nomeadamente a consideração do carácter escrito destes, a possibilidade de serem considerados originais e os requisitos da sua autenticidade;

v) O princípio de que todos os documentos em suporte eletrónico gozam da força probatória que lhes é devida, na parte inicial do n.º 2 do art.º 9.º e a densificação desse princípio, graduando-o em função da valoração que desses critérios fará cada aplicador da lei ou cada

---

for inclusion in the uniform rules: method of recording data; adequacy of measures protecting against alteration of data; proper maintenance of data carriers; and methods used for authentication of EDI messages". "A/CN.9/373", par. 102.

986 *"The Working Group considered the question of the manner in which assistance could be given to States in removing obstacles to the use of computer records for evidentiary purposes".* "A/CN.9/360", par. 50.

987 O n.º 1 do artigo 9.º da LMCE tem a seguinte redação: *"(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence: (a) on the sole ground that it is a data message; or, (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form".* "Guide to Enactment LMCE (1996)", pág. 7.

julgador, em função dos casos concretos.[988] Esses requisitos de que depende a avaliação da força probatória dos documentos eletrónicos referem-se à fiabilidade dos métodos quanto à forma como cada documento é:

a. Gerado, arquivado e comunicado;
b. Conservada a sua integridade;
c. Identifica e autentica o seu autor ou emitente.[989]

Ao apreciar um documento eletrónico, deve a entidade competente avaliar do cumprimento destes requisitos, e da sua verificação ou não, dependerá a sua força probatória.

A LMCE prevê apenas que a força probatória dos documentos eletrónicos dependa da verificação destes atributos, sem especificar em que termos essa verificação se impõe ao julgador ou às partes competentes ou interessadas. Trata-se, assim, de uma formulação aberta, que deixa a essas entidades margem de apreciação, que deverá, naturalmente, depender das próprias circunstâncias de cada caso. Essa maleabilidade justificava-se pela diversidade de regimes de prova existentes nos diversos países.[990] Foi assumido que, sendo o interesse mais elevado da LMCE, a eliminação de barreiras à utilização dos meios eletrónicos como meio de prova, o alcance desse objetivo não exigiria o estabelecimento de um regime completo e fechado dos documentos

[988] A configuração do regime de prova dos documentos eletrónicos consta do artigo 9.º da LMCE, sob o título *"Admissibilidade e força probatória das mensagens eletrónicas"*, cujo n.º 2 tem a seguinte redação: *"(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor"*. "Guide to Enactment LMCE (1996)", pág. 7.

[989] A parte final do n.º 2 do artigo 9.º da LMCE estabelece ainda a possibilidade de na valorização da força probatória dos documentos eletrónicos, o aplicador da lei, se socorrer de qualquer outro facto relevante ("*any other relevant factor"*). Esta norma reforça a flexibilidade da solução adotada, permitindo que a fiabilidade quanto à mensagem eletrónica, quanto ao seu ao autor e quanto à sua conservação e arquivo, sejam avaliadas pelo aplicador, não apenas em face dos referenciais tecnológicos de segurança, nomeadamente a autenticação e a integridade, mas também mediante outros meios possíveis, sem excluir nenhum, por exemplo a prova testemunhal. Essa possibilidade, que a LMCE admite, foi considerada nos trabalhos preparatórios, como resulta do seguinte trecho de um dos documentos *"As regards the issues of evidence, it was also agreed that the probative value of a message might result not only from compliance with a given method of authentication but also from other elements (e.g., testimonial evidence)"*. "A/CN.9/373", par. 71.

[990] *"It was generally considered that it was neither possible nor desirable to establish detailed statutory rules for weighing the probative value of EDI records. It was considered most appropriate to leave the question of weight of evidence to the discretion of the trier of fact"*. "A/CN.9/373", par. 102.

eletrónicos. Bastaria, numa primeira fase o estabelecimento de um conjunto de normas que pudessem ser ajustadas e não colidir com o direito interno de cada Estado.[991]

Mediante a verificação dos atributos de fiabilidade antes referidos, a LMCE conferia aos documentos eletrónicos o mesmo valor probatório dos documentos autenticados em papel, representando o mais elevado nível de eficácia probatória. Não se deu, porém, o passo de proporcionar aos agentes económicos a mesma segurança apriorística que a autenticação em papel, nomeadamente mediante reconhecimento notarial lhes proporciona, porque não havia na época soluções tecnológicas que o suportassem.

Os atributos essenciais para a equivalência plena dos documentos eletrónicos aos restantes documentos são os mesmos da assinatura eletrónica, pelo que só com a criação de um regime das assinaturas eletrónicas essa equiparação pôde passar a ser plena.

A Diretiva 1999/93/CE centrou nas assinaturas, e não na equivalência dos documentos, o objeto da proteção enquanto instrumento de prova, em face da adoção de um conceito de assinatura, que a LMCE não possuía.[992] O art.º 5.º estabelece o princípio geral da não discriminação no n.º 2, mas acrescenta uma estatuição imperativa, no n.º 1, no sentido da qual os Estados Membros estabelecerão a obrigatoriedade da relevância probatória das assinaturas eletrónicas qualificadas. Esse propósito era assumido como um dos principais objetivos da diretiva.[993] Apesar disso, a diretiva deixa para os Estados Membros a regulação da força probatória dos documentos eletrónicos (parte final do artigo 1.º) e não adota um conceito de documento eletrónico.

Com a Diretiva fica assegurada a idoneidade probatória das assinaturas e, por essa via, dos documentos assinados em suporte eletrónico quando assinados, sendo que

---

991 *"It was a generally held view that, in view of the significant diversity in national legal approaches to questions of evidence, it would not be advisable to attempt to enunciate detailed models for statutory provisions. Rather, it would be preferable to recommend that, to the degree possible, obstacles to the admission of EDI evidence should be removed"*. "A/CN.9/360", par. 50.

992 Esta mudança é importante, porque, a adoção de um conceito de assinatura eletrónica, bem como do seu regime jurídico, criou as condições para a emergência do próprio conceito de documento eletrónico e da consagração legal da prova mediante documentos eletrónicos. Como escreve Bazin, referindo-se às assinaturas manuscritas, a assinatura é a pedra angular da prova documental. *"From a legal point of view, the signature is the cornerstone of the legal evidence system"*. Bazin, Philippe; *op. cit*, pág. 180.

993 Ele é expresso no par. 21 dos considerandos prévios, nos seguintes termos: *"Para contribuir para uma aceitação generalizada dos métodos de reconhecimento das assinaturas eletrónicas, deve garantir-se que estas possam ser utilizadas como elementos de prova para efeitos processuais perante as jurisdições de todos os Estados-Membros"*.

as assinaturas eletrónicas qualificadas são equiparadas às assinaturas manuais reconhecidas por força da lei.[994]

A lei portuguesa da assinatura eletrónica (Decreto-Lei n.º 290-D/99, de 2/8) e particularmente minuciosa, e mesmo inovadora, relativamente à Diretiva. E porque esse regime ainda está em vigor no nosso direito interno, a par do Regulamento EIDAS, passamos a analisá-lo.

4.3. O regime vigente em Portugal da prova por documentos eletrónicos

A base do regime probatório dos suportes eletrónicos assenta no conceito de documento eletrónico, que a lei define e ao qual atribui relevância jurídica, habilitando-o com meio de prova. Sobre essa consagração, constrói-se a sua eficácia probatória, fazendo-a depender do tipo de assinatura eletrónico que o autentica. Justifica-se que analisemos em separado o regime jurídico do documento eletrónico para efeitos probatórios e o regime da assinatura eletrónica para os mesmos efeitos.

4.3.1. - O documento eletrónico como base probatória

O conceito de documento eletrónico da lei portuguesa (Decreto-Lei n.º 290-D/99, de 2/8) assume uma definição inovadora, dado que não se limita à equiparação do documento eletrónico ao de papel, mas vai mais longe e abrange todos os tipos de documentos eletrónicos. Na verdade, essa definição centra sobre os dados, e não sobre a

[994] A eficácia probatória das assinaturas eletrónicas não é superior à das assinaturas manuscritas, pelo que o regime da diretiva não interfere com o regime da eficácia da prova documental, limitando-se, de acordo com o princípio da equivalência funcional, a conferir igual eficácia aos documentos eletrónicos e aos de papel. Não concordamos com o entendimento de Ormazábal Sanchez, de que seria relativamente indiferente o efeito jurídico das assinaturas qualificadas, se não se alterasse o regime da prova documental. Sánchez, O.G. (2010); op cit, pág. 247. E este princípio funciona nos dois sentidos, não criando nenhum regime de prevalência relativamente aos documentos eletrónicos. Com defende Alberto Olmeda, *"la inclusión en la categoría de documento electrónico no dota a la manifestación de voluntad que en el mismo se contiene de unas reglas adicionales de validez"*. Olmeda, A.P. (2007). *La Actividad Administrativa Efectuada por Medios Electrónicos – A Propósito de la Ley de Acceso Electrónico a las Administraciones Públicas*, Thomson, Aranzadi. Pamplona., pag. 169. Concordamos com Clara Carron, quando afirma que *"la fuerza probatória de un escrito realizado en soporte electrónico es idêntica a la que se otorga al realizado en soporte en papel"*. E mais adiante, referindo-se à assinatura qualificada, *"estos certificados ofrecen a los partícipes del processo, asi como a los justiciables en general, la garantía de que, cuando intercambien datos entre si, lo podrán hacer de forma segura"*. Carron, Clara Fernandéz; op. cit, pag. 495 e 496.

sua legibilidade ou suscetibilidade de representação escrita a essência da definição.[995] O documento eletrónico é um conjunto de dados, e embora se estabeleça que se trata de uma elaboração resultante de um processamento de dados, e não apenas de um conjunto de dados, a definição é suficientemente abrangente para incluir qualquer documento eletrónico.[996]

Embora esta definição seja abrangente, e mesmo inovadora, é ainda problemática, dado que é pressuposto da definição de documento eletrónico, que se trate de um documento e, por outro lado, que tenha sido elaborado mediante processamento de dados. O primeiro requisito é relativamente redundante, porque não define a lei o que entende por documento. Diz-se apenas que um documento eletrónico é um documento, mas nada se diz acerca do que é exatamente um documento.[997] Utilizamos, para efeitos interpretativos e de aplicação, o conceito de documento do artigo 362.º do Código Civil, que o define como *"qualquer objeto elaborado pelo homem com o fim de reproduzir ou representar uma pessoa, coisa ou facto"*.

Daqui resultam dois problemas, sendo o primeiro o facto de os documentos eletrónicos serem estruturalmente diferentes dos documentos em papel. Na verdade, os documentos em papel cumprem os requisitos da representação de acordo com a teoria da representação, dando testemunho fáctico de realidades que lhes são exteriores, tal como a testemunha transmite conhecimento da observação factual. Nesses casos o documento é um veículo que "*predispõe uma representação permanente do facto, cristaliza um facto transeunte, projetando-o para o futuro*".[998] Mas o documento, além de representação é também veículo, que transporta no tempo e no espaço, essa representação.[999] Ora, os dados eletrónicos são suscetíveis de cumprir essas funções,

---

[995] A definição consta da alínea a) do artigo 2.º, cuja redação é a seguinte: *"«Documento electrónico» o documento elaborado mediante processamento electrónico de dados*".

[996] É também nessa linha que o artigo 4.º do Código dos Valores Mobiliários estabelece que se consideram cumpridas ou verificadas as exigências legais de forma escrita, "*ainda que o suporte em papel ou a assinatura sejam substituídos por outro suporte ou por outro meio de identificação que assegurem níveis equivalentes de inteligibilidade, de durabilidade e de autenticidade*". Ou seja, para os requisitos de documento escrito já não interessa o suporte em que se encontram gravados.

[997] Apesar de a norma pretender definir o conceito de documento eletrónico, como observam de forma pertinente Manuel Lopes Rocha et al, "*não se define aqui o que seja documento*". Defendem, porém, os autores, resultar daqui que "*a base essencial do conceito de documento eletrónico seja a mesma do conceito genérico de documento, particularmente quando referida aos documentos escritos*". Rocha, M. L.; Correia, M. P.; Rodrigues, M. F.; Andrade, M. A.; Amorim, P. P.; Carreiro, H. J.; Cabrita, L. (2008). Leis da Sociedade da Informação. Comércio Eletrónico. Coimbra Editora, Coimbra, págs. 30 e 31.

[998] Trata-se de uma especificação expressiva de Luís de Sousa. Sousa, L. F. P. (2017). Op. cit., pág. 10. O Autor critica a teoria de representação e entende que documento cumpre também a função de veículo, de acordo com a teoria da complexidade documental.

[999] O caráter limitado do conceito de documento resulta do facto de ter sido construído a partir do paradigma do documento em papel, dado ser esse, praticamente, o único que era utilizado como suporte

mas não só. Na verdade, a abrangência das operações desenvolvidas pelos sistemas informáticos, tornam os dados nos próprios factos, dada a magnitude dos factos que cada vez mais são operados pelos sistemas informáticos. É o caso, por exemplo, das notificações eletrónicas, da contagem de prazos de forma automatizada pelos sistemas informáticos. Nesses casos, e em muitos outros, são os dados que operam os factos, por exemplo a notificação efetuada por meios eletrónicos ou a própria identificação e autenticação eletrónicas, em que os dados representam um facto e são, eles próprios um meio de representação desse facto. Os dados que operam esses factos devem também eles ser considerados como documentos.

Por outro lado, a definição pressupõe que se trate um objeto, sendo que este conceito dificilmente se aplica aos documentos eletrónicos, que antes se trata de sequências digitais, de "*construções lógicas*".[1000]

Finalmente a definição do Código Civil trata os documentos como objetos elaborados pelo homem, o que é também suscetível de ser problemático, dado que os dados eletrónicos, podendo ser gerados por operações diretamente determinadas pelo homem, podem ser também gerado automaticamente pelos sistemas informáticos.[1001]

---

de negócios e atos jurídicos. Como se refere nos comentários à Lei do Comércio Eletrónico do G.P.L.P., "*A forma escrita, quando foi introduzida no direito estava claramente associada ao seu, até aqui, suporte por excelência: o papel. O papel deixou de ser o único suporte*". Gabinete de Política Legislativa e de Planeamento do Ministério da Justiça. (2005). Lei do Comércio Eletrónico Anotada". Coimbra Editora, página 103.

[1000] Seguindo a definição de Luís de Sousa, "*Mais do que uma entidade física, o documento eletrónico constitui uma entidade lógica (…) produto de vários elementos (software, hardware, suporte de gravação e metadados, sendo que nem todos são visíveis para o utilizador), unidos entre si por um nexo lógico e operacional*". Sousa, L. F. P. (2017). Op. cit., pág. 29 e 30. Não acompanhamos porém, o entendimento de David Silva Ramalho de que a "*prova digital*" se destaca pela "*sua imaterialidade ou invisibilidade*". Ramalho, D. S. (2017). Op. cit., págs. 104 e 105. Na verdade os dados em suporte eletrónico, sendo constituídos por impulsos elétricos, possuem um suporte material, apesar de a sua construção possuir um caráter de composição lógica. E não é pelo facto de, como o Autor sustenta, "*se abrirmos fisicamente um computador, não encontraremos no seu interior documentos escritos, sons ou filmes sensorialmente apreensíveis*" (*Ibidem*), que podemos extrair a conclusão acerca do caráter imaterial dos documentos eletrónicos. Do mesmo modo Gustavo Aboso defende a imaterialidade dos documentos eletrónicos, ("*falta la corporeidade en el sentido clásico de la definición de documento*"). Aboso, G. E. (2017). Op. cit, pág. 385. Porém uma coisa é a imaterialidade e outra é a sua visibilidade e imediatez da sua observação. O documento eletrónico é, tal como outro tipo de documento, suscetível de apreciação sensorial e capaz de transportar elementos de prova. Voltando a Aboso, "*el documento es un objeto sensorial y perceptible del mundo real*". Ibidem, pág. 387.

[1001] Apesar disso a doutrina interpreta de forma abrangente o conceito de documento do Código Civil. Nesse sentido Gonçalves Sampaio entende que a prova documental não abrange apenas os documentos escritos, mas "*todos os objetos materiais destinados a fornecer ao juíz a representação de um facto*". Sampaio, J. M. G. (2010). *A Prova por Documentos Particulares. Na Doutrina, na Legislação e na Jurisprudência. 3.ª Edição Atualizada e Ampliada*. Edições almedina, S. A. Coimbra, pág. 69. É também nesse sentido abrangente que aponta o Acórdão do Tribunal Supremo espanhol, de 5/2/88, que considera "*debe primar un concepto amplio del documento, identificándolo como qualquiera cosaa muebles aptas para la incorporación de senhales expressivas de um determinado significado*". Citado em Bennasar, A.

Além destes problemas que advêm do recurso à definição de documento do Código Civil a definição da alínea a) do artigo 2.º do Decreto-Lei n.º 290-D/99, de 2/8 contém ainda o problema de a classificar como uma elaboração resultante de um processamento de dados. E se assim pode ser em muitos casos, noutros o que se trata é que os sistemas informáticos operam, eles próprios, os dados, e nesses casos o que é necessários provar, mediante dados, são os próprios processamentos efetuados e não o seu resultado. Tudo isto porque nos sistemas informáticos, os dados não são apenas suportes, como o é o papel para os documentos tradicionais. São também os próprios processamentos em si mesmos.

É por essa razão que o Regulamento EIDAS adota um conceito mais abrangente de documento eletrónico, centrado de forma mais intensa nos dados em formato eletrónico, considerando que cumpre os requisitos da definição "*qualquer conteúdo armazenado em formato eletrónico*" (n.º 35 do artigo 3.º), sem se especificar de que tipo de conteúdo se trata.[1002]. Desta forma, sempre que existam dados que possam ser suscetíveis de efeitos jurídicos, cumpre-se o conceito de documento eletrónico.[1003] E esses dados podem consistir em declarações negociais, declarações de ciência, factos jurídicos, como sejam comunicações ou acontecimentos registados em

---

J. (2010). *La Validez del Documento Electrónico y su Eficácia en Sede Procesal*. Lex Nova. Valladolid, pág. 69.

[1002] Este conceito é também mais abrangente do que aquele que consta artigo 26.º do Decreto-Lei n.º 7/2004, de 7/7, que estabelece que se entendem como escritas as declarações em suporte eletrónico, quando cumpram as "*garantias de fidedignidade, inteligibilidade e conservação*". Na verdade, o que é relevante é que os dados em suporte eletrónico cumprem os requisitos de gravação e do armazenamento da informação, bastando isso para que se cumpra a função de veículo de transmissão de informação. E como referem Rocha e Al "*a mera circunstância de um texto estar acessível ao leitor apenas num monitor de um computador (…) não retira a esse texto o caráter de um escrito*". Rocha, M. L.; et Al. (2008). Op cit. págs. 45.

[1003] Não acompanhamos, nesta parte, o entendimento de Luís de Sousa, de que esta "*definição legal descreve o documento eletrónico por referência ao 'conteúdo' e não ao 'continente'*". Sousa, L. F. P. (2017). Op. cit., pág. 36. Na verdade, em nossa opinião ocorre o contrário, porque do que se trata é dar relevo ao caráter eletrónico da gravação, ou seja, aos dados, independentemente do seu conteúdo. É claro que esses dados necessitam de formar um conteúdo suscetível de relevância jurídica, e para que se trate de um meio de prova, é necessário que se verifique a sua capacidade de preservação da prova, mas o que é determinante é que essa preservação seja mantida por meios eletrónicos, assentes em dados. O Autor sustenta o seu entendimento no facto de "*ao contrário do documento analógico, o documento eletrónico não está adstrito a um corpo físico, podendo ser transferido entre vários tipos de suporte sem que perca a sua capacidade representantiva*". Mas também aqui não podemos estar de acordo. Na verdade o que carateriza o documento eletrónico é exatamente o seu suporte. E quando esse suporte muda, deixa de ser um documento eletrónico, o que ocorre, por exemplo quando é impresso em papel. Os documentos eletrónicos só podem ter como suporte os dados em base eletrónica e jamais outro tipo qualquer de suporte, sob pena de deixarem se ser documentos eletrónicos, e por essa razão é o suporte que define a sua natureza. E como a definição do regulamento EIDAS não acrescenta qualquer outro requisito em termos de conteúdo à definição, eletrónico é qualquer gravação suportada em dados, ou seja, eletrónica. Aliás é o próprio Autor que mais adiante reconhece que "*o câmbio de suporte (eletrónico-papel ou papel-eletrónico) provoca a perda da assinatura aposta no original)*". *Ibidem*, pág. 42.

suporte eletrónico ou operações realizadas pelos sistemas informáticos, como ainda produtos informáticos, como é o caso dos próprios sistemas informáticos.[1004]

O documento eletrónico é sempre suportado em dados digitais, sendo o suporte que define a sua natureza. Por essa razão deixa de ser eletrónico o documento quando é impresso ou muda de suporte, perdendo também, em consequência todas as garantias de confiança, nomeadamente a assinatura eletrónica.[1005]

Estabelecido assim o conceito de documento, o artigo 46.º consagra também o princípio da equivalência funcional e a garantia de que não podem ser negados efeitos jurídicos em razão do seu suporte eletrónico. Fica assim consagrada a idoneidade legal dos documentos eletrónicos, com este conceito amplo, para serem utilizados como meios de prova.

Em face da diferente delimitação do conceito de documento eletrónico, somos de parecer que o que consta do Regulamento EIDAS se sobrepõe ao do Decreto-Lei n.º 290-D/99, de 2/8. O alargamento do conceito de documento é relevante, porque abrange atos jurídicos que nos suportes eletrónicos seriam normalmente não documentados, ou mesmo verbais, porque as partes entenderam essa documentação desnecessária. É que, nas relações estabelecidas por meios eletrónicos não existem declarações verbais e todas são sustentadas em dados, pelo que, potencialmente todas podem ser documentadas.[1006]

[1004] O artigo 1.º da Convenção do Conselho da Europa sobre a Cibercrime define dados informáticos como "*any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*". Disponível em http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (última consulta em 6/7/2017). Na mesma linha, Venâncio entende que "*el concepto de datos informáticos cubre cualquier tipo de datos grabados en formato digital, independentemente de su contenido inteligible, incluindo programas de computador*". Venâncio, P. D. (2015). Delitos Contra la Integridad de los Datos Informáticos y Sistemas Informáticos en el Convénio del Consejo de Europa Sobre la Ciberdelincuencia". *Fodertics 3.0. Estúdios Sobre Nuevas Tecnologias e Justícia*. Editorial Comares. Granada, pág. 198.

[1005] Não acompanhamos, por essa razão, alguns entendimentos da doutrina acerca da existência de uma eventual categoria de documentos informáticos, que abrangeria também os documentos eletrónicos impressos ou que mudam de suporte. Rocha e Al defendem que "*documentos eletrónicos em sentido amplo, ou simplesmente documentos informáticos*" são "*fixados em qualquer suporte material gerado por um equipamento periférico ligado ao computador, seja uma impressora, …*" Rocha, M. L.; et Al. (2008). Op cit. págs. 33. Do mesmo modo Pupo Correia, refere-se aos "documentos electrónicos em sentido amplo", que ele designa de "documentos informáticos", e que seriam documentos elaborados em computador, mas impressos. Correia, M. P. (2000). Op. cit., pág. 125. Mas os documentos em papel são sempre em papel, independentemente da forma como foram gerados, porque o que os carateriza é o suporte, e nada os distingue dos restantes documentos em papel por esse facto. Para que os documentos sejam eletrónicos, necessitam se estar suportados em dados digitais.

[1006] Benjamim Rodrigues distingue três tipos de dados eletrónicos, os "*'dados de tráfego', 'dados de base' e 'dados de conteúdo'*", definindo os primeiros como "*relacionados com uma comunicação*", os segundos como os "*dados pessoais*" e os terceiros como "*aqueles que respeitam ao conteúdo de uma comunicação ou uma mensagem*". Rodrigues, B. S. (2009). Op. cit., pág. 674. O autor assume o caráter abrangente do conceito de documento eletrónico, do Scientific Working Group, como "*qualquer*

Mantém-se, porém, a equiparação dos documentos eletrónicos a documento em forma escrita nos casos em que o seu conteúdo seja suscetível de representação como declaração escrita, que consta do n.º 1 do artigo 3.º do Decreto-Lei n.º 290-D/99, de 2/8.[1007] Extraímos essa conclusão pelo facto de se tratar de uma norma interna destinada a conferir valor probatório aos documentos eletrónicos, bem como pelo facto de o n.º 3 do artigo 2.º do Regulamento EIDAS excluir a sua aplicação a matéria processual. Esta equiparação transporta, porém, para o universo significativo do conceito de documentos escrito, a generalidade da informação suportada em base eletrónica, dada a sua abrangência, porque toda ela é suportada em dados e também pelo facto de ser suscetivel de representação como declaração escrita, na sua generalidade.[1008]

Estabelecida a abrangência do conceito de documento a todos os conteúdos eletrónicos a sua habilitação legal para que possam ser objeto de relevância jurídica, bem como a sua equiparação a documentos escritos nos casos antes referidos, a eficácia probatória será graduada em função do grau de confiança nas assinaturas eletrónicas que os autenticarem.

4.3.2. – A eficácia probatória da assinatura eletrónica

---

informação com valor probatório que se encontra armazenda ou é transmitida sob a forma binária". Ibidem, pág. 722.

[1007] A capacidade de os documentos eletrónicos conterem declarações de qualquer natureza, capazes de serem suscetíveis de representação escrita é muito vasta, não só porque nas transações eletrónicas todas as operações ficam registadas em forma de dados e são suscetíveis de significado, como também porque todas elas correspondem a um comportamento humano, de forma mediata ou imediata. Por essa razão, pela via desta equiparação, o conceito de documento escrito subjacente ao Código Civil, passa a acolher uma quantidade muito mais elevada de declarações. Como refere Vadell, "*Cuando se trata de pruebas electrónicas que sobrepasan el tradicional concepto de documento, por mucho que hubiera expandido su contenido, y que tienen entidade por si mismas, nos encontramos con que la própia Ley de Enjuiciamiento Civil estabelece de manera expressa como debe procederse a essa valoración*". Vadell, L. M. B. (2015). *La Valoración de la Prueba Electrónica. Fodertics 3.0. Estúdios Sobre Nuevas Tecnologias e Justícia*. Editorial Comares. Granada, pág. 81.

[1008] O caráter limitado do conceito de documento resultava do facto de ter sido construído a partir do paradigma do documento em papel, dado ser esse, praticamente, o único que era utilizado como suporte de negócios e atos jurídicos. Como se refere nos comentários à Lei do Comércio Eletrónico do G.P.L.P., "*A forma escrita, quando foi introduzida no direito estava claramente associada ao seu, até aqui, suporte por excelência: o papel. O papel deixou de ser o único suporte*". Mas, como se refere no mesmo texto, "Na prática não existe qualquer diferença entre escrever manualmente uma palavra ou pressionar as teclas correspondentes ao teclado de um computador". Gabinete de Política Legislativa e de Planeamento do Ministério da Justiça. (2005). Lei do Comércio Eletrónico Anotada". Coimbra Editora, página 103. E como invoca com pertinência Miguel Pupo Correia, "*uma declaração tradutora de um dado conteúdo do pensamento humano, exteriorizado através de uma palavra de um determinado idioma, expressas em sinais adequados – máxime, entre nós, em carateres alfabéticos e numéricos – sobre um determinado suporte que permita a sua visualização*", deve também entender-se como documento escrito. Correia, M. P. (1999). *Comércio Eletrónico: Forma e Segurança. As Telecomunicações e o Direito da Sociedade da Comunicação*. Coimbra, página 235.

Sobre esta base abrangente do conceito, recorta-se a definição da sua eficácia probatória. Essa eficácia probatória está diretamente dependente do grau de confiança que cada um dos tipos de assinatura eletrónica proporciona, dado que é essa função de serviço de confiança que melhor a define.[1009] Analisamos, de seguida, os efeitos probatórios que cada um dos tipos de assinatura proporciona aos documentos eletrónicos.

4.3.2.1. – Das assinaturas eletrónicas qualificadas

Estas assinaturas eletrónicas garantem a mais elevada eficácia probatória aos documentos por elas assinados. O n.º 2 do artigo 25.º do Regulamento EIDAS determina que elas possuem o mesmo efeito das assinaturas manuscritas. Esta equiparação é acrescida de um conjunto de garantias de segurança, que o Regulamento acrescenta a este tipo de assinaturas:

i) A presunção de que elas garantem a identificação do signatário com o mais elevado grau de confiança,

ii) A presunção de que estão associadas de modo único ao signatário,

iii) A presunção de que, com elevado nível de confiança, só o signatário podia ter assinado o documento, dado que o dispositivo de criação de assinatura estava sob o seu controlo exclusivo e é um dispositivo qualificado;

iv) A integridade dos dados,

Todas as presunções enunciadas são reforçadas pelo facto de se tratar de assinaturas eletrónicas avançadas (do artigo 26.º), se baseiam em certificados qualificados, foram criadas por dispositivos qualificados, gerados por prestadores qualificados de serviços de confiança, que também criaram os certificados.

A equiparação legal, acompanhada das presunções antes referidas, que resultam diretamente dos pressupostos legais que estão estabelecidos no Regulamento

[1009] Trata-se, como refere Luís de Sousa, do princípio da simetria da função probatória, segundo o qual a eficácia probatória de um meio de prova depende do grau de segurança, ou de confiança de que é merecedor esse meio. Aplicado aos documentos eletrónicos, essa segurança advém da sua assinatura: *"A força probatória do documento eletrónico radica, numa primeira vertente, nas garantias que o mesmo oferece quanto à sua proveniência (identidade do autor) e inalterabilidade do seu conteúdo (integridade)"*. Sousa, L. F. P. (2017). Op. cit., pág. 63.

EIDAS para que as assinaturas possam ser classificadas como qualificadas, conferem um elevado nível de confiança às assinaturas eletrónicas qualificadas. Inclui-se nos respetivos pressupostos de confiança o controlo regular e permanente das entidades de supervisão sobre os prestadores qualificados, a fim de garantirem o cumprimento daqueles pressupostos, bem como a necessidade de um reconhecimento prévio desse estatuto. É destas garantias e presunções legais que advém a elevada eficácia probatória das assinaturas eletrónicas qualificadas.

Analisemos agora o seu efeito no direito interno português. Sobre a base abrangente do conceito de documento eletrónico do EIDAS, opera a segmentação efetuada pelo artigo 3.º Decreto-Lei n.º 290-D/99, de 2/8, entre o documento eletrónico e escrito e os restantes documentos eletrónicos.

O n.º 1 deste artigo 3.º considera como escritos os documentos eletrónicos cujo conteúdo seja suscetível de representação como declaração escrita. E embora na sua generalidade os documentos eletrónicos pudessem ser considerados escritos, porque assentam na linguagem binária e na gravação em tabelas em suporte eletrónicos de dígitos de zero e um, devemos interpretar o conceito de escrita por reporte ao Código Civil. O n.º 1 do artigo 374.º refere-se ao conteúdo dos documentos particulares como sendo formada pela "*letra e a assinatura*".[1010]

Para isso o artigo 3.º estabelece, no n.º 1, uma equivalência dos documentos eletrónicos aos documentos escritos, nos casos em que o seu conteúdo seja suscetível de representação como declaração escrita.

Nos casos em que assim não seja, estabelece-se também uma equiparação dos documentos eletrónicos, conforme os casos, a gravações sonoras e de imagens, às reproduções mecânicas que, nos termos do artigo 368.º do Código Civil constituem prova documental. Esta última equiparação tem, porém, a insuficiência da dificuldade de nela se incluírem os programas informáticos.

[1010] Luís de Sousa reflete acerca da natureza escrita dos documentos eletrónicos e conclui que se trata de uma terceira categoria de documentos, entre os documentos escritos e os orais. "*A forma eletrónica não é apenas uma nova técnica para escrever, mas integra, de pleno, uma nova forma, a par da oral e da escrita tradicionais*". Sousa, L. F. P. (2017). Op. cit., pág. 29. Com já referimos, o conceito de documento eletrónico é substancialmente diferente do de documento em papel, mas isso não significa que tenhamos necessidade de criar uma nova categoria de documentos. Nos suportes eletrónicos não existe oralidade e todas interações estabelecidas são suportadas em dados, sendo que os dados são sempre escritos em tabelas. E por essa razão seria sempre possível afirmar o caráter escrito da generalidade dos documentos eletrónicos, sem prejuízo, naturalmente, da equiparação que é efetuada no n.º 2 do artigo 3.º do Decreto-Lei n.º 290-D/99, de 2/8.

A equivalência efetuada pelo n.º 1 do artigo 3.º a que nos vimos a referir, não significa que esta norma limite os documentos eletrónicos a documentos escritos. Ela pretende apenas segmentar, de entre o género dos documentos eletrónicos, uma espécie que pode integrar o conceito dos documentos escritos do Código Civil e beneficiar do respetivo regime probatório. Em simultâneo habilita os meios eletrónicos a poderem cumprir os requisitos de documentação em forma escrita dos negócios ou factos jurídicos, nos casos em que a lei a exija. Assim, sempre que a lei exija forma escrita, passa a poder entender-se que os documentos eletrónicos são hábeis para cumprir esse requisito legal. E o n.º 1 do artigo 3.º é ainda mais abrangente e estabelece que cumpre o requisito de forma escrita qualquer documento eletrónico cujo conteúdo seja suscetível de representação como forma escrita.

4.3.2.1.1. – Documentos eletrónicos em forma escrita

O segmento dos documentos eletrónicos equiparados a documentos em forma escrita, que sejam autenticados como assinatura eletrónica qualificada, possui a força probatória prevista no artigo 376.º do Código Civil, ou seja, fazem prova plena em juízo ou no procedimento administrativo. Esta eficácia probatória vai muito para além da equiparação da assinatura eletrónica à assinatura manuscrita do n.º 2 do artigo 25.º do Regulamento EIDAS, dado que o Código Civil não confere esta eficácia a todos os documentos escritos.

O Código Civil só atribui forma probatória plena ao núcleo de documentos particulares escritos cuja autoria seja reconhecida. E só se considera reconhecida a autoria aos documentos que cumpram um dos seguintes requisitos, nos termos do artigo 374.º e 375.º:

i) Sejam reconhecidas presencialmente a letra ou a assinatura, nos termos do artigo 375.º do Código Civil;
ii) Sejam reconhecidas pela parte contra quem o documento é apresentado, como verdadeiras a letra e a assinatura;
iii) Não sejam impugnadas, a letra e a assinatura, pela parte contra quem o documento é apresentado.[1011]

[1011] Segundo Pires de Lima e Antunes Varela o reconhecimento pela parte contra quem os documentos são apresentados pode ser expresso ou tácito, ocorrendo este último caso quando não seja impugnada a

O universo de documentos escritos e assinados a que o artigo 376.º do Código Civil atribui força probatória plena, limita-se apenas àqueles que, cumprindo um dos requisitos anteriormente referidos, sejam considerados documentos cuja autoria seja considerada reconhecida. Assim, não integram essa categoria, os documentos que não tendo assinatura reconhecida presencialmente por notário, sejam impugnadas pela parte contra quem são apresentados. Ou seja, para a generalidade dos documentos assinados, caso a parte contra quem são apresentados impugne a sua letra ou a assinatura, a lei não considera que esteja reconhecida a autoria.[1012]

Ora, por efeito do n.º 1 do artigo 3.º do Decreto-Lei n.º 290-D/99, de 2/8, os documentos eletrónicos autenticados com assinatura eletrónica qualificada entram diretamente para o segmento de documentos com autoria reconhecida, pelo que possuem força probatória plena, reconhecida diretamente pela lei, nos termos do n.º 1 do artigo 376.º do Código Civil. Nestes casos, a impugnação da veracidade da letra ou da assinatura, pela parte contra quem o documento foi apresentado, não possui o efeito previsto na parte fina do n.º 2 do artigo 374.º do Código Civil, que seria a devolução à parte que apresenta o documento assinado, do ónus da prova da validade da assinatura.[1013]

Faz sentido que assim seja, dadas as garantias que o regime jurídico atual das assinaturas eletrónicas qualificadas constante do Regulamento EIDAS, tanto pelos

---

assinatura nem a letra. Lima, F.A.P., Varela, J.M.A. (1984). *Código Civil Anotado, Volume I, 3.ª Edição Revista e Actualizada*. Coimbra Editora. Coimbra, página 329.

[1012] Este é o sistema da generalidade dos países da *civil law*, ao contrário dos países da *common law*, onde o ónus da prova incumbe a quem apresenta o documento. O regime espanhol é idêntico ao português, seguindo a doutrina dominante entendimento idêntico ao nosso. "*Cuando un documento electrónico está firmado electrónicamente, su valor probatório dependerá si es (i) electrónica o (ii) electrónica avanzada. En el primer de los casos, el valor probatório de la firma será el que acuerdem las partes y en el segundo tendrá idéntico valor que documento público o privado com firmas certificadas*". Bessio, I. P. (2015). "Prueba Documental Electrónica en el Processo Jurisdicional: Estamos Listos?". Fodertics 3.0. Estúdios Sobre Nuevas Tecnologias e Justícia. Editorial Comares. Granada, págs. 124 e 125

[1013] Não é este o entendimento de Luís de Sousa, que defende a aplicação aos documentos eletrónicos com assinatura eletrónica qualificada, o mesmo regime dos documentos escritos particulares, ou seja, que caso a parte contra quem é apresentado o documento impugne a assinatura se aplica o n.º 2 do artigo 374.º do Código Civil. O problema desta interpretação é que ela opera no pressuposto de que o n.º 2 do artigo 3.º do Decreto-Lei n.º 290-D/99, de 2/8, efetua uma remissão para o artigo 374.º do Código Civil, quando a verdade é que essa remissão é feita para o artigo 376.º, ou seja, para os documentos cuja autoria esteja já reconhecida, e não apenas para os documentos particulares escritos. Esta interpretação conduziria ao resultado problemático de, em caso de impugnação, obrigar a parte que apresenta o documento autenticado com assinatura eletrónica qualificada, a provar a autenticidade da assinatura, com todas as dificuldades daí advenientes e frustrando o efeito de segurança que estas assinaturas pretendem produzir. Para contornar esta dificuldade o Autor defende a necessidade de a parte que invoca um documento com este tipo de assinatura, apresentar à partida prova dela e da identidade do seu autor e que, nesse caso, se ela fosse impugnada, o juíz teria que assumir uma presunção de cumprimento dos requisitos de assinatura qualificada. O problema dessa interpretação é que ela não é conforme ao disposto no n.º 2 do artigo 374.º do Código Civil, para o qual o Autor entende que a lei remete. Luís de Sousa. Sousa, L. F. P. (2017). *Op. cit*., pág. 74.

requisitos substanciais, como formais, dos quais depende essa classificação, que incluem, recordemos, um regime de reconhecimento de natureza pública e um controlo público permanente da verificação desses pressupostos. Na verdade a lei confere aos documentos eletrónicos autenticados com assinatura eletrónica qualificada a mesma força probatória dos documentos com assinatura reconhecida presencialmente por notário.[1014] Em ambos os casos existe, aliás, um regime de controlo de caráter público.[1015]

Este regime também faz sentido por outra razão. É que é muito difícil a prova da autenticidade da assinatura eletrónica, dado o seu caráter tecnológico complexo, ao contrário da assinatura manuscrita, cuja prova de genuinidade ou falsidade se pode fazer por análise grafológica. Fazer impender sobre quem apresenta um documento eletrónico com assinatura eletrónica, o ónus da prova da genuinidade desta, colocaria as assinaturas eletrónicas num plano de inferioridade relativamente às assinaturas manuscritas, pelas dificuldades de prova que envolve. E, face das garantias de segurança com que a lei atual rodeia as assinaturas eletrónicas qualificadas, dispensa-se essa prova à parte que invoca o documento assinado, colocando-se sobre a parte que impugna a assinatura o ónus da prova.[1016] Pode ser naturalmente impugnada, mesmo assim, a assinatura, mas sê-lo-á nos termos do artigo 347.º do Código Civil que faz recair o ónus da prova sobre quem invocar a falta ou vício da assinatura.

A força probatória das assinaturas eletrónicas qualificadas aplica-se, de forma correspondente, do nosso ponto de vista, aos selos eletrónicos qualificados emitidos pelas pessoas coletivas para autenticarem documentos eletrónicos por elas emitidos

---

[1014] Em sentido idêntico ao nosso, Susana Larisma "*O documento electrónico cujo conteúdo satisfaça a exigência legal de forma escrita e a que seja aposta uma assinatura electrónica qualificada emitida por uma entidade certificadora credenciada tem a força probatória de documento particular assinado, (…), o que significa que "(...) faz prova plena quanto às declarações atribuídas ao seu autor*". O documento é, assim, equiparado a um original". Larisma, S. (2004) "Contratação Electrónica". O Comércio Electrónico em Portugal. O Quadro Legal e o Negócio. https://www.anacom.pt/streaming/manual_comercio_elec.pdf?contentId=178219&field=ATTACHED_FILE, (última consulta efetuada em 6/7/2017), pág. 165.

[1015] No mesmo sentido deste nosso entendimento se pronuncia Gonçalves Sampaio: Quando autenticado com assinatura eletrónica qualificada, o "*documento eletrónico faz prova plena quanto às declarações atribuídas ao seu autor*". Naturalmente que isso não impede que a parte contra quem é apresentado o documento possa impugnar a assinatura, mas nesse caso caber-lhe-á o ónus da prova daquilo que invoca. "*sem prejuízo de poder ser arguida e provada a sua falsidade*". Sampaio, J. M. G. (2010). *Op. Cit.*, págs. 259 e 160.

[1016] No mesmo sentido deste nosso entendimento pronuncia-se Afonso Patrão: *"a agregação de uma assinatura electrónica qualificada certificada por entidade credenciada confere ao documento electrónico a força jurídica de um documento particular dotado de assinatura reconhecida por entidade com funções notariais, fazendo prova plena quanto às declarações atribuídas ao seu autor"*. O Autor acrescenta que essa assinatura se *"equipara à assinatura autógrafa reconhecida presencialmente*". Patrão, A. (2012). Op. cit., pág. 55.

Extraímos esta conclusão, não só pelo efeito de presunção de autenticidade e de integridade estabelecido no n.º 2 do artigo 35.º do Regulamento EIDAS, como também pela identidade do regime que lhes é aplicável, com o das assinaturas eletrónicas qualificadas, constante dos artigos 38.º a 40.º do Regulamento. Assim, embora o n.º 2 do artigo 3.º do Decreto-Lei n.º 290-D/99, de 2/8 não enuncie os selos eletrónicos no seu âmbito de previsão, o que se compreende porque quando entrou em vigor não existia essa espécie jurídica, a sua identidade com as assinaturas eletrónicas, permite que seja feita uma integração por mera interpretação extensiva.

4.3.2.1.2. – Documentos eletrónicos não considerados em forma escrita

Quando os documentos eletrónicos não se puderem considerar documento escrito, o n.º 3 do art.º 3.º do mesmo decreto-lei, atribui-lhe a força probatória que o art.º 368.º do Código Civil estabelece para as reproduções fotográficas, fonográficas, cinematográficas ou outras reproduções mecânicas. Neste caso, em termos literais o regime não é tão favorável, dado que o regime do Código Civil não prevê a assinatura destes tipos de documentos. Essa falta de previsão faz todo o sentido para os documentos que não estejam gravados em forma eletrónica. Na verdade, tanto as fotografias como os filmes, as gravações de música, suportados em fitas magnéticas ou em papel, não podiam ou não faria sentido serem assinados, pelo que não se justificava a previsão legal da sua assinatura.

Mas as coisas já não são assim nos casos em que, como ocorre atualmente de forma generalizada, esses conteúdos podem ser gravados em suporte eletrónico. Nesses casos a assinatura pode garantir, como é próprio das assinaturas, a sua autenticidade, integridade e a identificação do respetivo titular.

A questão que aqui se coloca é a de saber se é possível aplicar a estas assinaturas, quando qualificadas, o mesmo regime que o Código Civil prevê para os documentos escritos, ou seja, a consideração desses documentos como suscetíveis de fazer prova plena quanto à identidade do signatário, bem como à integridade e autenticidade.

Do nosso ponto de vista não, porque o regime do artigo 368.º do Código Civil não o prevê e estabelece que basta a impugnação da exatidão do conteúdo desses documentos, pela parte contra quem são apresentados, para que eles deixem de

beneficiar da força probatória máxima, de fazerem prova plena que a lei lhe atribui caso não sejam impugnados.

Assim, caso não exista impugnação, eles constituem prova plena quanto ao seu conteúdo, mas caso o sejam, perdem essa eficácia probatória. E perdendo essa eficácia, pode o juiz valorar livremente o seu efeito probatório, aplicando-se o previsto no n.º 1 do artigo 342.º do Código Civil, que faz pender o ónus da prova para a parte que apresentar o documento.

Nos casos em que esses documentos sejam assinados com assinatura eletrónica qualificada, não se lhes aplica a qualificação como documentos com autoria reconhecida prevista no n.º 1 do artigo 376.º do Código Civil.

Naturalmente que nos casos em que esses documentos eletrónicos estejam assinados com assinatura eletrónica qualificada, se lhe aplicam as garantias que esse serviço de confiança proporciona nos termos da lei, mas essa segurança e o seu reconhecimento dependerá sempre da livre apreciação do juiz.

É necessário, porém, ter em conta que o conceito de documento eletrónico do Regulamento EIDAS, alarga substancialmente o âmbito da abrangência que constava do DL 290-D/99, de 2/8. Na verdade enquanto este fazia depender o conceito de documento eletrónico, do conceito tradicional, o Regulamento EIDAS considera como documento eletrónico qualquer conteúdo armazenado em formato eletrónico. E sendo certo que todas as transações eletrónicas são suportadas em dados, então todas elas podem, potencialmente, ser consideradas documentos eletrónicos. E por essa via, o n.º 1 do artigo 3.º do DL 290-D/99, de 2/8, incorpora no seu âmbito de previsão todos os suportes que, nos termos do Regulamento, podem ser considerados documentos eletrónicos. E também por essa via, quando assinados, podem alcanças o valor probatório do n.º 1 do artigo 376.º do Código Civil, quando assinados com assinatura eletrónica qualificada.

4.3.2.2. – Das assinaturas eletrónicas não qualificadas

Os documentos com assinatura eletrónica não qualificada não beneficiam da qualificação como documentos particulares com autoria reconhecida, pelo que se lhes aplica o regime geral dos documentos particulares.

Assim, caso a parte contra quem são apresentados reconheça a assinatura como sua, farão prova plena, como resulta do n.º 1 do artigo 374.º e do n.º 1 do artigo 376.º do Código Civil.

Do mesmo modo, caso a parte contra quem são apresentados os documentos declare que não sabe se a assinatura lhe pertence, se considera fazer prova plena, porque se considera verdadeira e, portanto, reconhecida, nos termos do n.º 2 do artigo 374.º do Código Civil.[1017]

Finalmente, nos casos em que a parte contra quem o documento assinado é apresentada impugne a assinatura, se esta for de outro tipo que não a assinatura eletrónica qualificada, fica destruída aquela força probatória plena. Essa destruição não significa, porém, que esses tipos de assinaturas eletrónicas não tenham qualquer efeito probatório. Tem-no, na verdade, mas trata-se de um efeito dependente da livre apreciação do juiz. E nessa apreciação deverá sempre o juiz ter em conta de que tipo de assinaturas eletrónicas se trata e dos pressupostos legais necessários à sua classificação.

Nessa matéria é necessário distinguir as assinaturas eletrónicas avançadas das restantes. Relativamente às primeiras, o artigo 26.º do Regulamento EIDAS estabelece um conjunto de funções que asseguram, como anteriormente referimos. Essas garantias não possuem a eficácia que é conferida pelas assinaturas eletrónicas qualificadas, em especial as que resultam do controlo prévio e sucessivo permanente das entidades de supervisão, mas o Regulamento estabelece um conjunto de garantias que não deverão deixar de ser tidas em conta pelo juiz na sua livre avaliação da sua eficácia probatória.

É verdade que as assinaturas eletrónicas avançadas não pressupõem a existência de dispositivos qualificados nem emitidos por prestadores de serviços de confiança, o mesmo se aplicando relativamente aos certificados qualificados. Apesar disso as assinaturas avançadas, pela sua eficácia, resultante da utilização da criptografia das chaves assimétricas, permitem um nível relevante de confiança, superior ao das restantes, que não deverá deixar de ser tida em conta na prudente avaliação do juiz. Esta relevância não deixará de ser tida em conta ela parte que apresenta o documento assim assinado, que depois da respetiva impugnação pela outra parte será chamada a provar a

[1017] Não acompanhamos o entendimento de Afonso Patrão, no sentido de que só possua eficácia probatória a assinatura eletrónica qualificada. "*não será uma assinatura electrónica a aposição a um documento, por via informática, do nome do pretenso autor, porquanto essa introdução não é susceptível de constituir objecto de um direito individual e exclusivo*". Patrão, A. (2012). Op. cit., pág. 52. Na verdade todas as assinaturas tem eficácia probatória, maior ou menor, sendo que, nos casos em que ela consiste na possibilidade de o juiz as apreciar livremente, não deixará essa apreciação de ter em conta, no caso das assinaturas eletrónicas avançadas o seu regime jurídico.

validade da assinatura. Neste caso, essa prova, assentará, entre outras razões, na demonstração da verificação dos pressupostos do artigo 26.º do Regulamento EIDAS.[1018]

Nos casos em que o documento esteja assinado com assinatura não avançada, aplica-se o mesmo raciocínio, mas na avaliação do seu efeito probatório não poderá o juiz considerar os efeitos da utilização da criptografia das chaves assimétricas quando ela não é utilizada.

4.3.2.3. – Das convenções de autenticação eletrónica

O n.º 4 do artigo 3.º do Decreto-Lei n.º 290-D/99, de 2/8 regula a relevância dos métodos eletrónicos de autenticação convencionados pelas partes como instrumentos de assinatura. Nesses casos aplica-se esse regime convencional de autenticação estabelecido pelas partes. O mesmo regime se aplica, nos termos da parte final desta disposição legal, sempre que a parte contra quem é apresentado o documento aceite o método de autenticação utilizado.

As convenções de autenticação são livres, mas não se podem sobrepor à força probatória que a lei estabelece para as assinaturas reconhecidas. Admite-se, assim, implicitamente, que as partes concordem em atribuir a métodos de autenticação eletrónica efeitos de mais elevada eficácia que aquela que a lei estabelece, mas não podem degradar esses efeitos legais, como aliás resulta diretamente do artigo 345.º do Código Civil. É esse o sentido da ressaltava constante do n.º 5 do artigo 3.º que vimos analisando. Por exemplo, é possível que as partes utilizem um par de chaves assimétricas para autenticarem as transações que efetuam entre si, sem certificado nem dispositivo qualificados e lhe atribuam contratualmente o efeito de uma assinatura

[1018] Divergimos, também aqui, de Afonso Patrão, que defende "*do ponto de vista estritamente positivo, não se detectam diferenças entre documentos não assinados ou dotados de assinaturas não reconhecidas, já que nenhum deles produz os efeitos probatórios qualificados*". Patrão, A. (2012). Op. cit., pág. 56. Na verdade, são relevantes para a adequada avaliação da eficácia probatória das assinaturas, não apenas as normas do Código Civil acerca da prova, mas também as que conformam a natureza das assinaturas eletrónicas, em especial das avançadas. Aliás o próprio Autor acaba por o reconhecer mais adiante: "*julgamos que a sua existência acaba por produzir uma indicação gradativa ao julgador na apreciação de documentos electrónicos subscritos, pois este tenderá a valorar mais seriamente um documento dotado de uma assinatura electrónica avançada em face dos demais, dada a individualização legislativa daquela categoria*". Ibidem, pág.58.

qualificada. Nesse caso a lei aceita a eficácia probatória daí resultante, mas apenas nas relações entre as partes da convenção.[1019]

Sempre que nesses casos seja utilizado como método de autenticação a assinatura eletrónica qualificada, o regime desta sobrepõe-se a esse regime convencional.

4.3.3. - O documento eletrónico não assinado

Os documentos eletrónicos não assinados não beneficiam dos atributos de identificação do autor ou subscritor, nem da autenticação nem da integridade. Nos termos do artigo 46.º do Regulamento EIDAS são documentos e não lhes podem ser recusados efeitos jurídicos pelo facto de estarem suportados em base eletrónica, mas não sendo assinados, não lhes podem ser reconhecidas, por si, as funções próprias das assinaturas. E nesse caso, naturalmente, que os efeitos são idênticos nos suportes eletrónicos e no papel.

Os documentos deste tipo não são idóneos para, por si mesmos, produzirem efeitos jurídicos, sem prejuízo, porém, do recurso a outros meios de prova que lhe confiram essa eficácia.[1020]

Alguns autores assimilam a este tipo de documentos aqueles em que a assinatura eletrónica tinha o certificado caducado ou revogado. Acerca deste ponto é necessário especificar que o que releva são apenas os casos em que o certificado estava nessa situação na data da assinatura, dado que, caso estivesse válido não se levanta qualquer problema. Nos casos em que o signatário assinou com um certificado suspenso ou revogado, a assinatura não será qualificada, mas esse facto não lhe retira todo e qualquer efeito, de forma automática. Desaparece apenas a qualificação, mas a assinatura pode continuar a se uma assinatura avançada, pelo que o juiz poderá apreciar livremente a sua eficácia probatória. E para isso deverá ter em conta, tanto a natureza da assinatura, como as circunstâncias que estão na base do cancelamento ou da suspensão do certificado. Assim, se se trata apenas de uma situação de caducidade, poderá a assinatura ter os efeitos de uma assinatura avançada, mas no caso em que ocorreu uma violação do acesso e ela esteve exposta a um terceiro, que teve acesso à chave privada, então os efeitos serão outros, na prudente apreciação do juiz.

[1019] No mesmo sentido Luís de Sousa. Sousa, L. F. P. (2017). *Op. cit*., pág. 54.
[1020] No mesmo sentido Luís de Sousa. Sousa, L. F. P. (2017). *Op. cit*., págs. 61 e 62.

Capítulo IV – A assinatura eletrónica na administração pública

1. - A assinatura e o documento eletrónico no procedimento administrativo

O direito das assinaturas eletrónicas teve a sua génese na documentação das transações internacionais de mercadorias, domínio onde um dos agentes intervenientes são as autoridades aduaneiras, e isso teve um impacto imediato no procedimento administrativo.

Logo no ano 1981 o CCC defendia a utilização dos suportes eletrónicos para o cumprimento das obrigações aduaneiras das empresas, sob determinadas condições.[1021] Em 1982, a maioria das declarações aduaneiras apresentadas perante as respetivas autoridades dos EUA eram já preenchidas de forma automatizada pelos computadores

[1021] Citamos de novo essa importante recomendação aos estados, no sentido de *"Allow, under conditions to be laid down by the customs authorities, declarants to use electronic or other automatic means to transmit to the Customs Goods declaration for automatic processing. Such declarations may be transmitted either by direct link between the data processing system of the Customs and those of declarants or on magnetic or other ADP media (...) Accept, under conditions, (...) that Goods Declarations which are transmitted by electronic or other means, to Customs be authenticated other than by handwritten signature "*. A/CN.9/221, pág. 21.

das empresas, e embora o suporte utilizado fosse ainda o papel, esse facto revela a importância da utilização da informática nas relações das empresas com as administrações públicas.[1022]

Apesar de a LMCE ter como âmbito de aplicação as relações comerciais entre as empresas, como estabelece no seu art.º 1.º, dela constam normas que preveem a utilização dos meios eletrónicos nos chamados conhecimentos de embarque, que sendo títulos de transporte de mercadorias, são também documentos aduaneiros.[1023] A relevância jurídica desses documentos assentava no modelo das convenções prévias de autenticação estabelecidas com as autoridades aduaneiras, semelhantes àquelas que eram estabelecidas com outros agentes económicos.[1024]

Já nesse período, do início da década de 1980, a Dinamarca, declarava que as suas autoridades aduaneiras aceitavam a entrega de documentos em suporte eletrónico nos procedimentos administrativos aduaneiros, embora dependendo de autorização prévia dos órgãos competentes e ao cumprimento de um conjunto de requisitos.[1025]

A utilização de meios eletrónicos era também já referenciada para os casos de declarações para efeitos fiscais ao nível dos diversos impostos.[1026] Também nestes casos a modalidade de entrega era através de suportes físicos dos quais constavam gravados os documentos que cumpriam as respetivas obrigações fiscais.[1027] [1028]

[1022] É verdade que não se trata ainda de declarações apresentadas em suportes eletrónicos, mas esses documentos eram elaborados em local fisicamente distante daquele onde depois eram impressos e assinados. *"… The United States reported that a 1982 survey showed that 60 per cent of the goods declarations submitted to the customs authorities in that country were prepared on computer"*. "A/CN.9/265", par. 18. Como se refere mais adiante no mesmo parágrafo do documento que estamos a citar, *"These documents would seem to have the same physical and legal characteristics as similar documents prepared on a typewriter"*.

[1023] Prevê-se que a norma do artigo 1.º não impeça a sua utilização dos suportes eletrónicos nas relações com as administrações públicas: *"For example, while the focus of the Model Law is not on the relationships between users of electronic commerce and public authorities, the Model Law is not intended to be inapplicable to such relationships"*. "Guide to Enactment LMCE (1996)", par. 26.

[1024] *"Two parties who anticipate communicating frequently by computer-to-computer telecommunications may agree in writing beforehand on the form of the communications and the means to be used to authenticate the documents. Such an agreement may also be required by an administrative organ of the State before it will accept documents in electronic form, whether by telecommunications or computer memory device"*. "A/CN.9/265", par. 54.

[1025] *"Denmark stated that before being permitted to submit information to the customs authorities by means of magnetic tapes or diskettes, the consignee must obtain an authorization from the authorities"*. "A/CN.9/265", pág. 16.

[1026] *"The most commonly reported were tax declarations of various types, including goods declarations to the customs authorities"*. "A/CN.9/265", par. 70.

[1027] *"In order to transmit any document in computer-readable form from one entity to another either by physical exchange of computer memory devices or by telecommunications, both parties must have compatible equipment capable of sending and receiving data in that form"*. "A/CN.9/265", par. 71.

[1028] Em Portugal a possibilidade de entrega de declarações em suporte eletrónico para efeitos fiscais foi disponibilizada pela primeira vez em 1997, tendo passado a ser obrigatória a entrega das declarações periódicas do IVA a partir de 2003, pela Portaria n.º 375/2003, de 10/5.

O CCC publicou, em março de 1990, um projeto de guia sobre acordos de utilização de comunicações EDI entre as empresas e as administrações aduaneiras.[1029] Esse protocolo ainda hoje é utilizado nos procedimentos aduaneiros de exportação e de importação de mercadorias.

A expansão da utilização dos suportes eletrónicos nas operações das empresas forçou que ela se generalizasse rapidamente nas administrações públicas. Foram adotados procedimentos administrativos desmaterializados e muitas vezes automatizados, sem que estivessem previstos na lei os instrumentos jurídicos necessários nomeadamente no que respeita à segurança jurídica.[1030]

Esta generalização levou a UNCITRAL a considerar a utilização dos meios eletrónicos nas relações administrativas, um dos temas principais de análise no âmbito da preparação da LMCE. Nos trabalhos preparatórios foram identificados quatro pontos de especial relevo no que respeita a esta matéria:

i) A questão da autenticação das mensagens recebidas e enviadas pelas administrações públicas.[1031] Esta é uma questão essencial que afeta não só a segurança jurídica, mas também a própria validade dos atos praticados, uma vez que as comunicações que utilizam a Internet ou outras redes são efetuadas entre máquinas e era necessário que essas comunicações vinculem de forma segura as pessoas que são partes nas relações administrativas;[1032]

ii) A questão da admissibilidade dos documentos eletrónicos como elementos de prova;

iii) A possibilidade de a organização contabilística e os elementos de suporte serem mantidos apenas em suporte informático e eletrónico,

[1029] Esse foi um dos pontos de partida para a análise que neste domínio se iniciou no seio da UNCITRAL: "A/CN.9/350", par. 64.

[1030] Uma das causas da urgência na aprovação da LMCE era a necessidade de criar instrumentos legais que legitimassem a utilização dos meios eletrónicos pelas administrações públicas. *"In some countries, in the absence of legislative modernization to keep pace with clear legislative authority (...) regulatory decisions at lower levels and ad hoc arrangements entered into between companies and administrative authorities were used to facilitate the use of EDI"*. "A/CN.9/360", par. 70.

[1031] A questão foi abordada com profundidade em 1992: *"It was in the public interest that authentication and verification procedures were used since authenticated and verified messages could be relied upon by the user in its dealings with tax, customs or other authorities"*. "A/CN.9/360", par. 114.

[1032] Como afirma um especialista de segurança na Internet, Dan Kaminsky, *"Na Internet não há nomes de pessoas, tal como não há nomes no telefone. Quando necessitamos de telefonar a alguém, marcamos um número. Mas os números na Internet são as direcções IP, que mudam continuamente"*. Dan Kaminsky, Op. cit.

para efeitos de auditoria e de controlo, nomeadamente pelas autoridades tributárias, bem como para controlo dos acionistas e credores;[1033]

iv) A possibilidade de entrega de declarações para fins tributários, às respetivas administrações fiscais, por meios eletrónicos. Também este foi um domínio em que as administrações públicas desde logo iniciaram a utilização das comunicações eletrónicas como forma de aumentarem a sua eficiência, dados os custos elevados que a receção e tratamento destas declarações em papel envolviam.[1034]

Foram ponderadas várias possibilidades no que respeita à promoção da utilização de comunicações e de documentos eletrónicos, mas a UNCITRAL decidiu não fazer recomendações aos países no sentido de alterarem a sua legislação interna para, com isso, viabilizar a utilização dos registos e das comunicações eletrónicas no cumprimento daquelas obrigações.[1035]

Concluiu-se que a LMCE não deveria conter normas específicas para as relações administrativas, mas houve também acordo no sentido de que não deveria excluir as administrações públicas da sua aplicação, pelo que as normas dela constante se poderiam aplicar normalmente aos procedimentos administrativos.[1036] São exemplo disso a vontade expressa nos comentários ao projeto de disposição legal sobre a conservação e arquivo das mensagens de dados, onde se refere claramente a intenção da sua aplicação aos documentos com relevância tributária.[1037]

[1033] A necessidade de as empresas manterem em arquivo em suporte de papel, as faturas relativas às aquisições que efetuavam, era identificado como um dos problemas de resolução prioritária *"The obligations imposed with regard to the keeping and perpetuation of accounting and/or tax records are so full of loopholes and so widely divergent that we consider priority action even going beyond the simple TEDIS Programme absolutely must be envisaged here. Indeed, what is the point of being able to transmit invoices electronically if writing remains a mandatory requirement in the destination Member State on the grounds that the expenditure to which it relates must be evidenced by a written paper document in order to be deductible?".* "TEDIS Report", pág. 306.

[1034] No Estudo Preliminar, elaborado em 1990, são referenciados os seguintes três tópicos como de maior relevo: *"Evidence in court, with the same evidentiary value as that of the original documents they purport to reproduce; - The extent to which accounting records can be held electronically and the conditions under which one could be allowed to store the documents or information on which such accounting was based exclusively on computer; - The possibility of allowing tax or customs declarations to be submitted by electronic means"*. "A/CN.9/333", par. 17.

[1035] Esse entendimento vem expresso, nomeadamente, na seguinte asserção dos documentos preparatórios: *"recommending changes in administrative rules at the national level would not be an appropriate focus of work by the Commission"*. "A/CN.9/373", par. 46.

[1036] *" while the uniform rules should not expressly deal with the situations where a form requirement was prescribed by an administration for reasons of public policy, the sphere of relationships between EDI users and public authorities should not be excluded from the scope of the uniform rules"*. "A/CN.9/373", par. 48.

[1037] Essa disposição era o então artigo 9.º que, na versão final da LMCE passou a ser o artigo 10.º: *"Article 9 establishes a set of supplementary rules for existing requirements regarding the storage of*

Mas é necessário distinguir os casos em que, no âmbito dos procedimentos administrativos, a lei exige o formalismo de que os documentos de suporte ao exercício de direitos ou ao cumprimento de obrigações estejam suportados em papel, daqueles em que essa exigência não existe.[1038] Os procedimentos administrativos são essencialmente instâncias de receção e tratamento de informação, nos quais, com frequência, é mais importante o conteúdo da informação do que a forma como ela se apresenta. Nesses casos é possível que, havendo acordo entre o órgão competente da administração para o procedimento e os particulares, os dados de informação que estes apresentem sejam suportados em forma eletrónica e não em papel.[1039]

Essa possibilidade abrangia, naturalmente, as diversas formas de entrega de documentos em suporte eletrónico, quer as comunicações por EDI ou a entrega de suportes magnéticos, como os CD, disquete ou banda magnética, quer outros meios de comunicação que se viessem a desenvolver. Do mesmo modo, são frequentes as situações em que os formulários e o modo de entrega da informação, no seio dos procedimentos administrativos, sejam estabelecidos através de regulamentos administrativos, pelo que se considerava que nada impedia que a administração pública ajustasse esses regulamentos à utilização dos suportes eletrónicos nas comunicações.[1040]

Esta possibilidade não existia no caso dos documentos entregues para servir como prova nos processos judiciais e a entrega de dados formais à administração pública.[1041] Relativamente a estes últimos, a sua admissibilidade dependia da inexistência de entraves na própria legislação processual.

---

information (e.g. for accounting or tax purposes) that may constitute obstacles to the development of modem trade". "A/CN.9/WG.IV/WP.64", par. 81.

[1038] Esta distinção é um dos pressupostos que esteve na base da LMCE. *"there were instances in which administrative and regulatory statutes (e.g, tax and securities laws) imposed particular requirements that had potential evidentiary implications. Among the requirements of this type that were most prevalent were obligations imposed on commercial entities to maintain business records for accounting and tax purposes"*. "A/CN.9/360", par. 47.

[1039] Essa possibilidade era considerada um pressuposto natural nos trabalhos de conceção da LMCE: *"It could be expected that such an agreement would be sufficient to allow the use of the record of the EDI message as evidence. A similar agreement may be also required by an administrative organ of the State before it will accept documents in electronic form, whether by telecommunication or by manual transmission of a computer memory device such as a diskette or magnetic tape"*. "A/CN.9/333", par. 157.

[1040] Essa possibilidade já era admitida em alguns países, desde que garantidos alguns princípios, como a inteligibilidade dos documentos e a sua inalterabilidade, garantindo-se, desta forma, os princípios de não repúdio, tanto pelos particulares como pelos órgãos administrativos com competência para os procedimentos. *"In some countries the use of EDI for such purposes was expressly sanctioned, subject to conditions such as the intelligibility and unalterability of electronic records"*. "A/CN.9/360", par. 47.

[1041] *"In most countries a distinction had to be drawn between the admissibility of electronic evidence in judicial proceedings and the acceptance and use of such evidence by administrative authorities. The applicable rules and approaches employed in the two types of fora tended to differ. In the administrative sphere, the focus tended to be on the gathering of information and greater discretion on the part of the*

Nos trabalhos de elaboração da Diretiva 1999/93/CE foi logo reconhecida a necessidade da generalização da utilização das tecnologias eletrónicas na administração pública.[1042] E essa necessidade viria a ser reafirmada sucessivamente, quando se tornava mais claro que a utilização destas tecnologias eram um fator de eficiência e qualidade do serviço prestado.[1043]

A Diretiva assume a utilização da assinatura eletrónica na administração pública como um pressuposto, prevendo apenas que cada estado membro possa sujeitar a sua utilização no sector público a requisitos adicionais, desde que sejam objetivos, transparentes, proporcionados e não discriminatórios.[1044] Um exemplo desses requisitos adicionais era já a utilização dos selos temporais, dada a importância da determinação dos prazos nos procedimentos administrativos e a garantia, para os particulares, de ser demonstrável a data de entrega de petições ou de cumprimento de obrigações. Esse requisito consta, por exemplo, da lei espanhola de assinatura eletrónica de 1999.[1045] A lei de 2003 manteve esta previsão, acrescentando a estatuição da possibilidade de emissão de certificados de assinatura eletrónica para os próprios serviços da administração pública e a sua correspondente utilização nos procedimentos administrativos.[1046]

Em Portugal, a lei da assinatura eletrónica de 1999 previa também a sua utilização no procedimento administrativo, estabelecendo apenas como requisito adicional que se tratasse de assinaturas eletrónicas qualificadas cujos certificados tenham sido emitidos ao abrigo do Sistema de Certificação Central do Estado e que identificassem claramente o órgão da administração pública onde decorre o procedimento e o respetivo titular que praticou o ato.[1047],[1048]

---

administrative authority, with generally less emphasis than in the judicial sphere on evidentiary rules and procedure". "A/CN.9/360", par. 47.

[1042] O Comité Económico e Social Europeu reconheceu, pela primeira vez em 1998, que *"no mais breve prazo possível, as administrações públicas devem ser capazes de fornecer e aceitar documentação eletrónica"*; 98/C 157/01, JOCE, 25.5.98. par. 6.10.

[1043] Alguns anos mais tarde, o mesmo Comité, num parecer de 2012 sobre o mercado digital, escreve que *"O CESE considera que as administrações públicas deverão estar acessíveis em linha a breve trecho"*. 2012/C 229/01; JOCE, 31/7/2012, par. 4.4.2.

[1044] Trata-se do n.º 7 do artigo 3.º da Diretiva 1999/93/CE, de 12/12/99. Do mesmo modo, no preâmbulo escreve-se que *"As assinaturas eletrónicas serão utilizadas no sector público no âmbito das administrações nacionais e comunitárias e nas comunicações entre essas administrações, assim como com os cidadãos e os operadores económicos, por exemplo em contratos públicos, em matéria de sistemas de fiscalidade, de segurança social, de saúde e judiciário"*.

[1045] Artigo 5.º do Real Decreto-Ley 14/99, de 17/9.

[1046] Artigo 4.º, n.ºs 3 e 6 do artigo 7.º e n.º 1 do artigo 13.º da *"Ley 59/2003, de 19 de diciembre, de firma electrónica"*.

[1047] Artigo 5.º do DL n.º 190-D/99, de 2/8.

Mais tarde, já em 2010, no âmbito da Agenda Digital Europeia, assumia-se a ambição de a administração pública disponibilizar todos os seus serviços nas redes abertas, com o objetivo de aumentar a participação dos cidadãos e de promover a generalização da utilização das tecnologias eletrónicas.[1049]

O Regulamento EIDAS veio criar o quadro legal necessário para a plena utilização pelas administrações públicas, dos Estados Membros da UE, das tecnologias eletrónicas no procedimento administrativo. Mais do que isso, assume-se o papel liderante do Estado e dos organismos administrativos na criação de um "*mercado único digital*", aproveitando as oportunidades de crescimento económico disponibilizadas pelas tecnologias eletrónicas.[1050] O Regulamento EIDAS vem criar dois sistemas de interoperabilidade no espaço de toda a UE, por um lado no domínio da identificação eletrónica e por outro no domínio dos chamados serviços de confiança que inclui as assinaturas eletrónicas. O primeiro destina-se a garantir a utilização dos serviços eletrónicos das administrações de todos os Estados Membros pelos cidadãos europeus, com apenas um meio de identificação eletrónica e o segundo a permitir o reconhecimento mútuo e automáticos das assinaturas eletrónicas e dos restantes serviços de confiança eletrónica em toda a UE. Também aqui se estabelece um princípio da liderança das administrações públicas, em especial nos artigos 27.º e 27.º, alargando-se a interoperabilidade às assinaturas não qualificadas, bem como aos selos eletrónicos.

Tanto o regime da identificação eletrónica como dos serviços de confiança têm o efeito de abrir os sistemas das administrações públicas à interação eletrónica com os cidadãos e as empresas. E mesmo nos casso em que esses sistemas não exijam a autenticação da identidade eletrónica com meios de identificação com níveis de garantia elevados, o Regulamento obriga a que os Estados aceitem que os cidadãos e toda a

---

[1048] Ém Portugal, a utilização das tecnologias de informação e das redes abertas nos procedimentos administrativos remonta ao ano de 1997, quando o Ministro das Finanças, Professor Doutor Sousa Franco assinou o despacho n.º 10.854/97 (2.ª série), com data de 30/10/97, estabelecendo a possibilidade e a validade do envio através da Internet, das declarações de IRS e IVA, bem como da declaração modelo 10, de remunerações pagas pelas entidades patronais. O despacho previa que o sistema de autenticação do envio desses documentos consistia na utilização de uma senha de autenticação. O despacho foi publicado no Diário da República, II série, de 11/11/97, pág. 13892. Mais tarde, em 2003, passou a ser obrigatória a entrega eletrónica.

[1049] Esse objetivo é descrito da seguinte forma: *"Os governos europeus estão empenhados em, até 2015, disponibilizar generalizadamente serviços de administração pública em linha centrados no utilizador, personalizados e multiplataforma"*. Por outro lado, *"Os serviços de administração pública em linha constituem um meio eficaz e económico para melhor servir todos os cidadãos e empresas e promover uma governação participativa, aberta e transparente"*. "COM(2010)245 final", par. 2.7.4, pág. 36

[1050] Em conformidade com as conclusões do Conselho Europeu de 4/2/2011 e de 23/10/2011. A Agenda Digital para a Europa era apresentada como uma das principais medidas de resposta à chamada crise das dívidas públicas, que provocou uma crise na construção europeia, na sequência da grande recessão iniciada em 2007 com a crise do *subprime* nos EUA.

União Europeia possam a eles aceder eletronicamente com os mesmos meios. Do mesmo modo, a autenticação dos documentos e dos dados eletrónicos com assinaturas eletrónicas ou selos eletrónicos pode ser efetuada sem necessidade de exigência do nível de garantia mais elevado das assinaturas eletrónicas qualificadas, quando os sistemas informáticos utilizados pelas administrações públicas utilizem apenas assinaturas eletrónicas avançadas. Assim, a utilização dos serviços eletrónicos disponibilizados pelas administrações públicas fica disponível a todos cidadãos e empresas da União Europeia, com os mesmos instrumentos de identificação e de autenticação que se exigem aos cidadãos de cada Estado, sem requisitos adicionais de segurança para a sua utilização transnacional.

O CPA de 1991 não continha normas acerca da utilização das tecnologias eletrónicas nos procedimentos, mas o novo Código, de 2015 vem consagrar, pela primeira vez, um importante conjunto de normas, nomeadamente as seguintes:

i) Um conjunto de princípios da administração pública eletrónica, destacando-se o dever de os respetivos órgãos utilizarem meios eletrónicos como forma de promover a prossecução dos três objetivos fundamentais da eficiência, da transparência e da participação dos cidadãos (n.º 1 do art.º 13.º do CPA). O princípio da transparência é especificado mediante a criação de uma nova obrigação, de os órgãos da administração pública competentes para o procedimento, disponibilizarem aos interessados todas as fases da sua tramitação na Internet.[1051]

ii) A instituição da obrigação de os serviços utilizarem, no procedimento administrativo, as tecnologias eletrónicas (n.º 4 do art.º 14.º do CPA). Esta obrigação é densificada no art.º 61.º do CPA, que estabelece especificamente que no procedimento "*devem ser preferencialmente utilizados meios eletrónicos*". Esta preferência justifica-se pelas

[1051] Essa obrigação dos serviços da administração é um importante instrumento de transparência e de participação dos cidadãos no procedimento administrativo, e conta do n.º 4 do artigo 82.º, especificando o n.º 2 que a informação a disponibilizar, mediante autenticação prévia do interessado, consiste na seguinte. *"a indicação do serviço onde o procedimento se encontra, os atos e diligências praticados, as deficiências a suprir pelos interessados, as decisões adotadas e quaisquer outros elementos solicitados"*. Consagra-se, na última parte desta norma, a possibilidade de os interessado solicitarem a disponibilização de informação do procedimento através da Internet, podendo este ser um canal de comunicação continuada das partes no procedimento.

faculdades que a utilização destes meios proporciona, de eficiência, transparência e comodidade para os cidadãos;[1052]

iii) A previsão da utilização da assinatura eletrónica como forma de garantir a autenticidade dos documentos, estabelecendo-se que na decisão final deve ser aposta a assinatura eletrónica do autor do ato, ou outro meio de autenticação do titular do órgão, remetendo o CPA para norma regulamentar a criar, a especificação deste meio (art.º 94.º, n,º 1 do CPA);[1053]

iv) O direito de os cidadãos entregarem o requerimento inicial do procedimento por via eletrónica, consignado na alínea d) do n.º 1 do art.º 104.º do CPA. Este direito é uma emanação do direito mais amplo, de que os cidadãos são sujeitos ativos e a administração pública sujeito passivo, se relacionarem por via eletrónica com os serviços públicos;

v) A previsão da utilização dos meios eletrónicos como instrumento de comunicação e de notificação no procedimento administrativo (art.º 63.º e alínea c) do n.º 1 do art.º 112.º.

Podemos classificar estas normas do CPA, relativas à utilização dos meios eletrónicos no procedimento administrativo, como sendo de dois tipos. Por um lado normas de promoção dessa utilização, que poderíamos designar de programáticas, revelando um certo voluntarismo e otimismo do legislador no que respeita ao efeito dessa utilização para os fins do procedimento. Por outro lado, normas de segurança destinadas a garantir a validade e a eficácia jurídicas da utilização desses meios e a conferir aos agentes económicos e aos cidadãos confiança jurídica nessa utilização, sendo, porém, estas mais escassas, limitando-se à que anteriormente referimos no ponto iii). Analisamos, no ponto 1 do Capítulo V, já de seguida, os problemas e dificuldades que subsistem nesta matéria.

[1052] A utilização das tecnologias no procedimento administrativo estava já prevista de forma generalizada na Lei Geral Tributária (LGT), que previa no seu artigo 60.º-A a sua utilização. Essa norma foi introduzida em 2011 e veio conferir enquadramento jurídico à utilização dessas tecnologias que já estava generalizada na administração tributária. A norma legitima, sem induzir nem obrigar essa utilização, mas obriga a administração tributária a possuir um serviço na Internet. Por outro lado, a norma é também imperativa no que respeita À obrigação de a administração tributária disponibilizar nesse serviço a prestação do mesmo tipo de serviços que presta nas suas unidades orgânicas físicas. Pires, J.M.F., Bulcão, G., Vidal, J.R. e Menezes, M.J. (2015), *Lei Geral Tributária Comentada e Anotada*. Livraria Almedina. Coimbra., pág.s 633 a 638.

[1053] Por exemplo, nos casos em que os interessados apresentam requerimentos em serviços periféricos desconcentrados, mas dirigidos aos órgãos centrais, o envio por via eletrónica para estes, que está previsto no nº 3 do artigo 103.º do CPA, deve ser efetuado com observância da garantia de autenticidade do documento enviado, mediante assinatura eletrónica do serviço que procede à sua expedição.

2. O efeito da assinatura eletrónica e do documento eletrónico no procedimento administrativo

A utilização das tecnologias eletrónicas pelos serviços da administração pública iniciou-se pelas tarefas instrumentais e de rotina, com escassa relevância jurídica, mas rapidamente se expandiu ao próprio procedimento administrativo e às relações estabelecidas com os cidadãos.[1054] Essa utilização cresceu rapidamente, como resposta a uma necessidade de aumento da eficácia dos órgãos da administração pública ao crescimento acelerado das solicitações dos cidadãos nas últimas décadas do século XX, à medida do crescimento do estado social de direito.

O crescimento da procura havia aumentado a lentidão das administrações públicas na apreciação e decisão dos procedimentos administrativos degradando a qualidade e a capacidade de resposta dos órgãos da administração. A utilização das tecnologias eletrónicas assumiu-se como o instrumento para aumentar a rapidez das decisões, a sua qualidade, previsibilidade e transparência, e esses são importantes interesses protegidos pelo Direito Administrativo.[1055]

As administrações públicas são, essencialmente, sistemas de receção, produção, tratamento e gestão de informação e, por isso, a sua atividade é, em grande parte, suscetível de ser digitalizada e informatizada.[1056]

[1054] Como afirma com propriedade Davara Rodriguez *"não se deve falar da alegada falta de garantias com a introdução das novas tecnologias, quando é precisamente a excessiva burocratização e a lentidão dos procedimentos que está a causar uma insegurança e impossibilidade de defesa que faz aumentar a falta de confiança dos administrados na própria administração"*. Rodriguez, M.A.D. (2004*). Manual de Derecho Informático.* Thomson – Aranzadi. Navarra.. 396.

[1055] Assim o postula também Margariños: *"Os instrumentos tecnológicos emergentes possibilitam dar um maior grau de segurança, incluindo com maior grau de certeza, ao exercício correcto dos poderes da administração pública à salvaguarda da plena integridade dos direitos e das liberdades individuais"*, e mais adiante: *"O uso da informática possibilita que a actividade da administração pública seja mais transparente e por isso, ao poderem ser conhecidos os defeitos, tornando-os mais suscetíveis de crítica e censura, dos cidadãos, e impedindo que as más práticas administrativas fiquem impunes".* Rodriguez-Margariños, F.G. (2008), Op. Cit, pág. 50.

[1056] São relevantes, nesta matéria, as inovações introduzidas no processo de execução fiscal pelo DL n.º 53-A/2006, de 29/12, que vieram regular a utilização da assinatura eletrónica na emissão de certidões de dívida, passando estas a ser assim um documento eletrónico (nºs 3 e 4 do artigo 163.º do Código de Procedimento e de Processo Tributário – CPPT), bem como pela DL n.º 238/2006, de 20/12, que vieram alterar o regime da competência territorial em matéria de execução fiscal, permitindo ao órgão da instauração efetuar todos os atos de execução no território nacional, sem necessidade de emitir carta precatória (n.º 2 do artigo 185.º e n.º 5 do artigo 187.º do CPPT). É ainda relevante a nova redação dos n.ºs 4 e 5 do artigo 191.º do CPPT, que prevê a emissão eletrónica de citação em execução fiscal,

O paradigma de funcionamento da administração pública é o procedimento administrativo e a sua instrução compõe-se, essencialmente, de um conjunto de suportes de informação constantes de requerimentos, documentos e comunicações, trocados entre os particulares e os órgãos da administração em ambos os sentidos, entre vários órgãos da administração, bem como com outras entidades terceiras. Do mesmo modo, as decisões proferidas constam de documentos que, por sua vez são comunicados aos interessados ou a terceiros. Os dados, a informação, os suportes documentais e as comunicações são a base material de operação dos procedimentos administrativos, os mesmos que as tecnologias de informação vieram transformar.

São também eles, os dados, o objeto de aplicação da assinatura eletrónica como instrumento de identificação e de autenticação dos respetivos sujeitos. A assinatura eletrónica veio permitir a manutenção da autenticidade e da integridade dos dados dos procedimentos administrativos, apesar da sua digitalização e desmaterialização, bem como dos arquivos dos respetivos processos, e ainda a utilização segura da Internet e de qualquer rede eletrónica como um instrumento de comunicação.[1057]

As administrações públicas estão também sujeitas aos princípios eficiência, economicidade e celeridade previsto no n.º 1 do art.º 5.º do CPA, sem prejuízo, naturalmente, do interesse público, princípios idênticos àqueles que impeliram as empresas privadas a adotar as tecnologias eletrónicas no desenvolvimento da sua atividade.

Do mesmo modo, o acesso dos cidadãos aos serviços da administração pública passa a poder ser efetuado de forma imediata e em qualquer local, quebrando-se assim os constrangimentos resultantes da distância física. Esse acesso, quando efetuado através da Internet, pode ocorrer a qualquer hora do dia e em todos os dias da semana,

---

mediante assinatura eletrónica qualificada do titular do órgão de execução fiscal, que foi introduzida pela Lei n.º 67-A/2007, de 31/12, bem como o regime de penhora imóveis por comunicação eletrónica, constante do artigo 231.º do CPPT, dando sequência a idêntico regime do artigo 838.º do Código de Processo Civil. É também relevante referir, a Portaria n.º 331-B/2009, de 30/3, que veio prever a utilização das comunicações eletrónicas mediante assinatura eletrónica no âmbito da ação executiva.

[1057] A utilização da Internet para a realização de operações transacionais, com relevância jurídica pelas administrações públicas, só ocorreu numa segunda fase, e depois da disponibilização de meios de assinatura eletrónica, nomeadamente da tecnologia das palavras passe, dada a sua insegurança no estádio anterior. *"A Internet, como rede aberta, é intrinsecamente insegura, pelo que as Administrações Públicas devem garantir a segurança nas suas relações com os cidadãos, bem como a privacidade da infinita quantidade de dados de carácter pessoal que possuem nos seus arquivos."* Pozo, J.D.S. e Sonseca, M.A.M. (2004). Empleo de la Firma Electrónica en el Seno de las Administraciones Públicas: Derecho Comparado. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.pág. 45.

eliminando-se assim os constrangimentos próprios do horário de funcionamento dos serviços.

Além da facilidade do acesso, a digitalização dos procedimentos e dos processos permite que aumente a participação dos cidadãos na formação da vontade da administração pública e na determinação do interesse público em cada procedimento. A facilidade das comunicações permite ainda a interação mútua entre os cidadãos e a administração, e o estabelecimento de relações permanentes e prolongadas no tempo, mais do que esporádicas, entre os cidadãos e as suas administrações. Através da Internet os cidadãos podem acompanhar a marcha do procedimento em que são interessados e controlar também a própria atividade da administração.

Tal como na atividade económica as redes abertas alteraram o conceito de mercado como uma instância delimitada em termos físicos e temporais, também nas relações administrativas se eliminaram os constrangimentos de espaço e de tempo.[1058] Essa mudança altera os conceitos de competência territorial, de descentralização e de desconcentração administrativa.[1059] A administração fica mais próxima dos cidadãos com a disponibilização dos seus serviços na Internet e nos restantes suportes eletrónicos, alterando-se o paradigma de uma presença exclusivamente física, em instalações só abertas em períodos temporais limitados. Esse efeito está a produz importantes alterações no atual paradigma de uma administração pública distribuída pelo território segundo o modelo clássico de ocupação territorial e organizada por competências em função das circunscrições territoriais e da proximidade física com os cidadãos.[1060]

No interior dos serviços das administrações públicas, as tecnologias eletrónicas permitem a completa desmaterialização dos processos administrativo e da tramitação de todo o procedimento. Essa desmaterialização, associada à utilização das comunicações eletrónicas entre os órgãos das administrações públicas e no seio de cada um deles, permite o trabalho em rede.

[1058] Como refere Benjamim da Silva Rodrigues, "*Os sistemas e as redes informáticas fazem (des)aparecer o tempo e o espaço*". Rodrigues, B. S. (2009). Op. cit., pág. 66.

[1059] Como refere com propriedade Olmeda, a utilização das tecnologias eletrónicas no procedimento administrativo veio colocar em crise o papel da competência territorial, dado que a prática dos atos se torna possível em lugares diferentes daqueles onde está localizado fisicamente o órgão competente. O território deixa assim de ser limite, pelo que os órgão passam a poder aceder e a ser acedidos pela generalidade dos cidadãos e, por outro lado, a atividade administrativa passa a poder ser feita nas redes abertas. Olmeda, A.P. (2007), op. cit.; pag. 52 e 53.

[1060] É particularmente simbólica nesta matéria, a eliminação da competência territorial das Conservatórias do Registo Predial a partir de 1/1/2009, operada pelo DL n.º 116/2008, de 4/7, com a introdução do artigo 6.º-A ao DL n.º 519-F2/79, de 29/12.

O trabalho em rede permite que os serviços e as equipas de trabalho que os compõem estejam em comunicação permanente independentemente do local onde estão fisicamente instalados. Isso permite que a organização dos serviços da administração seja cada vez mais indiferente à sua localização física, eliminando-se os constrangimentos de espaço e de tempo. Assim, os procedimentos podem ser instruídos e decididos por equipas de trabalho dos órgãos da administração pública que não estão necessariamente próximas fisicamente, pelo que esses órgãos não necessitam mais estar organizados em serviços fisicamente localizados e juntos. Na organização interna dos serviços, a possibilidade de se fazer uma distribuição que seja independente dos constrangimentos de localização dos serviços, aumenta as possibilidades de uma especialização de funções, o que poderá, também, aumentar a qualidade e a rapidez do trabalho dos serviços. Esse facto permite uma maior especialização em função dos tipos de procedimento e do conhecimento que lhes está associado, e já não apenas uma especialização por áreas territoriais, que no passado repetiam em cada circunscrição o mesmo tipo de conhecimento procedimental e substancial de todas as outras. Trata-se, provavelmente, de um novo paradigma de administração pública, que as tecnologias eletrónicas estão a permitir fundar, com maior qualidade nos serviços prestados aos cidadãos e maior rapidez nas respostas às demandas destes.

Também nas relações entre órgãos da administração pública, as possibilidades de comunicação de documentos eletrónicos com segurança aumentaram a celeridade dos procedimentos, pela possibilidade de os documentos de suporte dos procedimentos, nomeadamente certidões, declarações ou cópias de documentos arquivados noutros serviços públicos, serem obtidos mediante ligação eletrónica em rede entre os serviços das administrações públicas, dispensando-se os interessados de serem eles a obter esses documentos e entregá-los nos serviços competentes.[1061] [1062]

[1061] Em Portugal, esta interoperabilidade converteu-se num direito dos cidadãos à dispensa de apresentarem documentos em órgãos da administração pública quando eles estejam disponíveis noutro órgão. Esse direito depende da autorização do próprio cidadão, que habilita um órgão a obter de outro um documento que lá se encontra disponível e foi finalmente consagrado em lei pelo DL n.º 73/2014, de 13/5, que aditou o artigo 28.º-A ao DL n.º 135/99, de 22/4.

[1062] O CPA já prevê que o ónus dos factos cabe aos interessados no procedimento que os tiverem invocado (n.º 1 do artigo 88.º), mas isso não prevalece sobre a obrigação que impende sobre o órgão da administração competente para o procedimento, de ser ele a promover oficiosamente às averiguações necessárias à apreciação e decisão dos procedimento, como determina o n.º 1 do artigo 87.º, consagrando assim o princípio do inquisitório. Amaral, D.F., Caupers, J.; Claro, J.M., Raposo, J., Garcia, M.G.D; Vieira, P.S., Silva, V.P. (2005). *Código do Procedimento Administrativo Anotado, com Legislação Complementar*. 5.ª Edição", Livraria Almedina. Coimbra., pág. 175. Do mesmo modo, Esteves de Oliveira, Pedro Gonçalves e Pacheco de Amorim, afirmam que impende sobre o órgão competente para a decisão, *"o dever oficioso de verificar a suficiência dos pressupostos da actuação administrativa. Esse*

Essa atividade de veículo de comunicação entre serviços públicos que tradicionalmente era efetuada pelos cidadãos interessados nos procedimentos administrativos passa a ser efetuada por transmissão direta e digital da informação diretamente entre os serviços.[1063] Essa transmissão é mais rápida, porque é imediata, eliminando aos cidadãos os encargos inerentes ao procedimento e tornando a marcha deste mais rápida e também mais económica, porque elimina também os custos de atendimento e de execução de tarefas manuais.

A informação assim obtida, de forma digital e imediata, pode ser facilmente integrada nos procedimentos administrativos em curso, de modo a que a fase decisória destes seja alcançada com maior rapidez. Mas a digitalização e a transmissão digital permitem ainda que os sistemas informáticos validem a qualidade da informação e automatizem a sua obtenção, de forma que poderão existir procedimentos administrativos em que a instrução fique concluída com grande rapidez e se possa disponibilizar aos cidadãos interessados o resultado produzido pela informação obtida para que estes possam pronunciar-se em audição prévia.

Esta possibilidade de tornar praticamente instantâneos e automáticos os atos de obtenção de informação e de documentação no âmbito da instrução do procedimento administrativo pode também conduzir a que ocorram casos de procedimentos vinculados que sejam suscetíveis de automatização e, nesse caso, de produção da decisão de forma muito rápida e em alguns casos instantânea, sem prejuízo dos direitos de participação dos cidadãos na decisão do procedimento.[1064] Muitos dos procedimentos

---

dever de (conhecimento e) averiguação oficiosa e obrigatória dos factos e interesses relevantes no procedimento constitui a vertente material ou 'de conhecimento' do princípio do inquisitório." Oliveira, M.E., Gonçalves, P.C. e Amorim, J. P. (2006) *Código do Procedimento Administrativo Comentado*; 2.ª Edição, Livraria Almedina. Coimbra, pág. 419.

[1063] Cabe referir, acerca deste princípio de simplificação e racionalização, as importantes alterações introduzidas no Código do Registo Predial pelo DL n.º 116/2008, de 4/7, que vieram consagrar o direito de os cidadãos exigirem às Conservatórias do Registo Predial que sejam estas a obter os documentos necessários ao registo, quando esses documentos se encontrem disponíveis noutros serviços da administração pública. Do mesmo modo, quando para o ato de registo são necessárias certidões emitidas por outras Conservatórias, a sua obtenção passou a ser obrigação daquela que é competente para o registo, deixando de ser possível a exigência dessas certidões aos interessados no registo (cf. Nova redação do artigo 42.º do Código do Registo Predial e dos n.ºs 2, 5 e 6 do artigo 43.º do mesmo Código). É ainda muito importante o exemplo de interoperabilidade entre organismos públicos e privados, dado que, com o aditamento do artigo 8.º-B ao mesmo Código, as entidades que titulam atos de transmissão de imóveis (mediante escritura pública, autenticação de documentos particulares ou outros factos jurídicos sujeitos a registo - Notários, Advogados, Solicitadores, Câmaras de Comércio), passam a ser elas também obrigatoriamente, sujeita à obrigação de registar esses mesmos atos. Essa obrigação de registo deve ser cumprida através de pedido efetuado por via digital, como determina o novo artigo 42.º-A do mesmo Código.

[1064] Numa descrição sintética da evolução do impacto que a Internet está a produzir na economia e na Administração Pública, Friedman transcreve uma descrição de um responsável pela IBM, nos seguintes

em que os órgãos da administração não possuem margem de discricionariedade, e em que os atos da instrução estão tipificados na lei, poderão ser integralmente automatizados e desmaterializados, podendo os sistemas informáticos proporcionar a geração de uma decisão típica com carácter imediato, que poderá ser depois ajustada, confirmada ou alterada pelo órgão competente para a decisão, depois de se garantir a participação dos interessados no procedimento.[1065]

Nestes casos de procedimentos administrativos em que se trate da prática de atos vinculados, sem margem de discricionariedade dos órgãos da administração pública, a rapidez na sua conclusão é muito importante, em especial quando se trate de reconhecimento de direitos dos cidadãos, cumprindo-se assim com maior efetividade o princípio da eficiência, economicidade e celeridade previsto no n.º 1 do art.º 5.º do CPA.[1066]

As mudanças que antes enunciámos tornaram-se possíveis pela segurança proporcionada pela assinatura eletrónica, mas também pelo facto de as relações administrativas terem estado presentes desde muito cedo nos trabalhos da sua conceção. Mas existe ainda um longo caminho a percorrer no que respeita a utilização dos suportes eletrónicos nas administrações públicas, como veremos no próximo capítulo, nomeadamente a regulação dos próprios procedimentos eletrónicos automatizados e o regime de partilha de informação entre os diversos órgãos da administração pública.

---

termos: *"Está a surgir todo um novo conjunto de padrões com vista a permitir a sistematização do fluxo de trabalho. Trata-se de padrões para que o meio empresarial funcione em conjunto. A título de exemplo, quando recorre a uma hipoteca, seja para a transferência da propriedade de um imóvel ou compra de uma casa, ocorrem literalmente dúzias de processos e fluxos de dados entre muitas empresas. Um banco poderá tratar de garantir a aprovação do processo, verificar o seu crédito, fixar-lhe as taxas de juro e gerir a transferência – após o que o crédito é 'vendido' quase imediatamente a outro banco (...). O nível seguinte será automatizar todos estes processos para que fluam em conjunto"*. Friedman, T.L. (2005). Op cit., pág. 93.

[1065] William Eggers descreve o investimento que foi efetuado na utilização das novas tecnologias pela administração do estado norte-americano da Florida, sob o lema *"eliminate what you can, digitalize what you can't"* (elimina tudo o que puderes e digitaliza o que não puderes eliminar) e analisa, particularmente o programa de eliminação e de reengenharia dos procedimentos de emissão de licenças para o exercício de determinadas atividades, e os interessados passaram a poder obter diretamente essa licenças através da Internet. O sistema informático faz imediatamente um conjunto de validações críticas, mediante cruzamentos de dados e emite a licença. A atividade não automatizada dos órgãos da administração pública passou, nestes casos, para uma função de controlo e fiscalização *a posteriori,* da verificação e manutenção dos requisitos do licenciamento. Eggers, W.D. (2005). *Governing 2.0 - Using Technology to Improve Education, Cut Red Tape, Reduce Gridlock, and Enhance Democracy*. Roman & Littlefield Publishers, Inc. Maryland, pág.s 119 e 120.

[1066] Como afirmam o Professor Doutor Freitas do Amaral e os restantes Autores do "CPA Anotado, trata-se de um princípio *"que obriga a uma renovação permanente das estruturas e dos métodos de funcionamento da Administração Pública"*. Amaral, D.F., Caupers, J.; Claro, J.M., Raposo, J., Garcia, M.G.D; Vieira, P.S., Silva, V.P. (2005). *Op.cit*., pág. 23.

Capítulo V – Problemas jurídicos da assinatura eletrónica

A investigação cujos resultados expusemos até aqui revela o processo de formação do corpo de conceitos e normas jurídicas que sustentam o direito dos suportes eletrónicos, mas revela também o longo percurso que está por fazer, as lacunas legais, os fatores de insegurança e as perspetival de evolução futura. Neste capítulo pretendemos dedicar-nos a enunciar as lacunas mais importantes, que serão também as possíveis vias de desenvolvimento do direito dos suportes eletrónicos e da assinatura eletrónica.

1. O procedimento administrativo e os serviços de confiança eletrónica

Os procedimentos administrativos são, na sua generalidade, instâncias de recolha e de tratamento de informação, operando sobre ela as decisões proferidas e a sua execução. Um procedimento administrativo é, na verdade, um sistema de tratamento de informação relevante para a decisão, existindo muitos casos de procedimentos que se

repetem de forma sistemática, porque a instrução e a decisão é de natureza vinculada. Nesses casos, os atos de instrução desenvolvidos pelos serviços estão sistematizados, mesmo nos casos em que a sua tramitação é manual. Na verdade, todos os procedimentos administrativos são geridos e tramitados segundo protocolos internos dos serviços que definem o modo de realização dos atos de cada tipo de procedimento, para além, naturalmente, da sua conformação legal.

Tanto o caráter sistemático dos procedimentos como a base informacional sobre que assentam, facilitaram a generalização da utilização das tecnologias eletrónicas no procedimento administrativo. Esse facto alterou o paradigma de tramitação dos procedimentos, que de uma base de papel passaram a ser suportados em dados e em procedimentos de natureza eletrónica. Analisamos, nos pontos seguintes, os problemas que subsistem neste domínio.

1.1. - O procedimento administrativo eletrónico

O procedimento administrativo é uma conquista civilizacional do estado de direito, pela sistematização e disciplina da ação da administração, libertando-a do arbítrio e do seu caráter errático.[1067] O direito ao procedimento é uma das mais importantes garantias dos administrados.[1068] É o procedimento que garante a legalidade material da atividade dos órgãos da administração, a sua racionalidade e a sua sindicabilidade, em especial quando se trate de procedimentos através dos quais a administração pública pratica atos de autoridade.[1069] A importância do procedimento administrativo na realização do direito e dos fins de interesse pública da ação da administração tem ganho importância crescente e isso revela-se pela consolidação dos

[1067] Wolf, Bachof e Stober falam de uma "*severidade da forma*", correspondendo "*às exigências da segurança jurídica e da consequência lógica*". Wolf, H.; Bachof, O; Stober, R. (2006*). Direito Administrativo, Volume* I. Fundação Caloust Gulbenkian. Lisboa, pág. 448.

[1068] Citando Paniagua, "*el procedimento administrativo debe entenderse como garantia para los ciudadanos y los operadores jurídicos en general. La administración pública cobra transparência …*". Paniagua, E. L., (2010). Fundamentos de Derecho Administrativo. Del Derecho del poder al Derecho de los ciudadanos. 2.ª edición. Colex Editorial. Universidad Nacional de Educación a Distância. Madrid, página 305.

[1069] Como nos ensina o Professor Freitas do Amaral, um dos objetivos do procedimento é "*esclarecer melhor a vontade da Administração, de modo a que sejam sempre tomadas decisões justas (quanto ao próprio 'procedimento' e não apenas quanto ao 'produto final') úteis e oportunas*", acrescentando que as formalidades do procedimento se destinam a "*esclarecer a vontade da Administração, em ordem a ser tomada uma decisão justa, útil e oportuna*". Amaral, D. F. (2001). *Curso de Direito Administrativo, Volume II*. Edições Almedina, Coimbra, páginas 292 e 293.

chamados direitos procedimentais dos administrados, nomeadamente o direito à participação, o direito à fundamentação, à notificação dos atos procedimentais, etç.[1070]

A efetividade dos direitos procedimentais dos cidadãos depende do modo como o procedimento é conduzido pelo órgão competente e pelos agentes a quem incumbe a prática dos atos e das formalidades que o compõem, bem como pelos formalismos envolvidos na sua prática.[1071] A forma é essencial à realização dos direitos.[1072]

Ora, os formalismos procedimentais consolidaram-se no pressuposto de que o procedimento segue a forma escrita e é documentado em suporte de papel. A documentação dos atos e das diligências procedimentais é determinante do cumprimento das normas legais e do respeito pelos direitos dos cidadãos. Os órgãos que dirigem o procedimento, os agentes que executam as diligências procedimentais, por um lado, e a sua documentação pelo outro, são a base da garantia da efetividade dos direitos procedimentais dos cidadãos.

1.1.1. - O procedimento administrativo automatizado

A utilização dos suportes eletrónicos no procedimento administrativo conduziu a que partes significativas da sua gestão e tramitação tenham sido automatizadas.[1073]

[1070] Como referimo na nossa *Lei Geral Tributária Comentada e Anotada*, a propósito do procedimento administrativo tributário, "*esses direitos procedimentais são tão importantes como os direitos substanciais na relação jurídica tributária, porque são eles que garantem a legitimidade da ação da administração e o respeito pelo Estado de Direito*". Pires, J.M.F., Bulcão, G., Vidal, J.R. e Menezes, M.J. (2015), *op cit*, pág. 561. O Professor Vasco Pereira da Silva, na esteira de Vieira de Andrade, classifica mesmo os direitos procedimentais dos cidadãos como direitos subjetivos, que são, em alguns casos, direitos constitucionais, como é o caso do direito à audiência prévia, o direito à fundamentação, o direito de acesso aos arquivos, o direito à informação acerca do andamento do processo e o direito à notificação. Silva, V. M. P. D. P. (2003). *Em Busca do Acto Administrativo Perdido (reimpressão)*. Livraria Almedina. Coimbra, página 439.

[1071] A importância do procedimento como garantia dos cidadãos é, entre outros, enfatizada por Maurer, "*mediante la determinación y la observância de normas procedimentales se garantiza la obtención de decisiones materialmente adecuadas e irreprochables*". E mais adiante, "*las decisiones estatales deben estar en consonância con los derechos fundamentales, sino que también el procedimento administrativo y el subsiguiente sistema de garantías judiciales deben configurarse y desarrollarse de tal modo que asseguren una adecuada realización de las posiciones jurídicas garantizadas por los derechos fundamentales individuales*". Maurer, H. (2011). *Derecho Administrativo. Parte General*. Marcial Pons. Ediciones Jurídicas y Sociales, S.A. Madrid, pág. 479.

[1072] Na lição de Maria da Glória Garcia, "*o princípio da legalidade administrativa e a dimensão garantística do direito, sobre o qual aquele princípio se estrutura, ganham uma nova consistência e a ação estadual fundada na lei adquire, por força desta, legitimidade material*". Garcia, M.G.F.P.D. (1994). Da Justiça Administrativa em Portugal. Sua Origem e Evolução. Universidade Católica Editora. Lisboa, pág.s 608 e 609.

[1073] Na doutrina americana utiliza-se o conceito de governo eletrónico, ou *e-Government*, na sequência da publicação do *e-government Act*, projetado por Al Gore e depois promulgado em 2002 pelo Presidente Bush. O conceito abrange as dimensões interna, de utilização das tecnologias eletrónicas no trabalho

Casos existem, e serão cada vez mais, em que todo o procedimento estará automatizado, nomeadamente naqueles que são de decisão vinculada, em que não cabe margem de discricionariedade à entidade competente para a decisão.[1074] Nestes procedimentos, a conformação vinculada das decisões e a sua sustentação em dados que constam de registos de outros sistemas informáticos, tornam possível que a tramitação do procedimento consista, fundamentalmente, num conjunto de verificações objetivas de pressupostos, que podem ser efetuadas de forma automatizada, tornando todo o procedimento eletrónico e na prática sem intervenção humana.[1075]

Em muitos procedimentos administrativos a decisão depende de um conjunto de operações matemáticas, por exemplo, no apuramento dos impostos a pagar, mediante a liquidação, que sendo efetuada pela administração tributária, depende de uma declaração entregue pelos sujeitos passivos, da qual constam todos os dados necessários à prática do ato de liquidação, eventualmente complementados por outros dados recebidos pela administração tributária de outras entidades. Como a entrega dessas declarações é também feita, na maioria dos casos, por via eletrónica, todo o procedimento pode ser automatizado, sem necessidade de existir intervenção imediata humana na sua tramitação e na decisão final. Trata-se de um procedimento sistematizado, sendo a decisão proferida sem qualquer margem de discricionariedade, mediante um conjunto de procedimentos matemáticos, pelo que a sua automatização é possível.

Noutras situações, a instrução do procedimento e a decisão nele proferida dependem da verificação de um conjunto de pressupostos, sendo que muitos deles constam de bases de dados informatizados, e a apreciação desses pressupostos da decisão a proferir pode também ser automatizada, mediante a análise e processamento

---

interno dos órgãos administrativos e externa, de comunicação e interação com os interessados no procedimento. Nesse sentido, Gutiérrez, R.M. (2009), op. cit., pags. 202 e 203.

[1074] É o caso, por exemplo, dos procedimentos administrativos em matéria tributária, como as liquidações do IRS e do IRC, bem como da generalidade dos impostos. Do mesmo modo é do conhecimento público que outros procedimentos são automatizados, como por exemplo a colocação de professores do ensino secundário e dos alunos no ensino superior. Também o CPTA prevê duas situações de tramitação eletrónica automatizada e de processos judiciais, sendo a primeira a da distribuição do processo ao juiz e a segunda a citação das partes. No que respeita à distribuição dos processos pelos juízes, o artigo 26.º estabelece que ela é efetuada de forma automatizada e eletrónica, pelo sistema informático. Relativamente à segunda, estabelece o n.º 3 do artigo 24.º que logo que apresentada a petição inicial, a citação das entidades públicas ou dos órgãos nela indicados é efetuada automaticamente por via eletrónica, sem necessidade de despacho ou de outras diligências, salvo nos casos em que a lei estabeleça a existência de despacho liminar.

[1075] Acerca do papel dos suportes eletrónicos no procedimento administrativo, Ortega, R.R. (2007). *El Expediente Administrativo - De los Legajos a los Soportes Electrónicos*. Thomson, Aranzadi. Navarra., página 38, 39.

de dados informatizados. Nestes casos, a decisão não depende apenas de operações matemáticas, mas a verificação de pressupostos em que as possibilidades sejam passíveis de ser parametrizadas, permite também a automatização da instrução e da decisão. É o caso, por exemplo, da análise de um pedido de isenção do pagamento de determinadas taxas, por exemplo taxas moderadoras, que depende do rendimento declarado pelo requerente, da sua idade ou da sua morada.

Como os sistemas informáticos funcionam com base em silogismos construídos a partir de dados, é possível efetuar processamentos automatizados extraindo conclusões, segundo o método dedutivo, a partir da constatação de respostas positivas ou negativas em resultado da comparação de dados informatizados existentes. Por exemplo, se o rendimento é superior a determinado montante, extrai-se uma conclusão, se for inferior extrai-se outra conclusão, formando-se árvores de respostas de sim ou não, que permitem uma automatização em níveis crescentes, até que se forme a decisão do procedimento, nos casos em que não exista margem de discricionariedade na decisão.

Assim, quando os dados são iguais ou diferentes de um determinado parâmetro, a conclusão variará também em conformidade. Por exemplo, se têm direito a uma isenção de uma determinada taxa as pessoas com rendimentos inferiores a um montante fixo, o sistema informático onde está instaurado o procedimento de reconhecimento da isenção acede a um outro sistema informático onde consta o montante dos rendimentos daquele requerente. Nesse acesso o sistema compara o valor correspondente ao limiar de rendimento que confere o direito à isenção com o valor real do rendimento do requerente. Se este último for inferior, considera-se cumprido um dos requisitos para a decisão, caso contrário não.

É desta comparação mimética de dados e da obtenção de respostas de sim ou não, que os sistemas informáticos vão construindo os itinerários de decisão, compostos de condições que se verificam ou não (se A é inferior a B, então C, se não A não é inferior a B, então D. Se B é maior que D, então E, caso contrário, então F, e assim sucessivamente, mediante comparação de lógica de dados).

Um exemplo de um procedimento administrativo que pode ser completamente automatizado é o relativo ao reconhecimento da isenção do Imposto Municipal Sobre Imóveis dos prédios que estão afetos à habitação própria e permanente dos seus titulares. O artigo 46.º do Estatuto dos Benefícios Fiscais (EBF) estabelece essa isenção para os casos em que se cumpram cumulativamente os seguintes requisitos:

i) O titular tenha no prédio a sua morada permanente considerando-se que é a morada associada ao seu número de identificação fiscal (n.º 9) do artigo 46.º do EBF);

ii) O valor patrimonial tributário do prédio não seja superior a 125.000 euros;

iii) O rendimento do titular ou do seu agregado familiar não seja superior a 153.300 euros;

iv) O titular não esteja a beneficiar de idêntica isenção relativamente a outro prédio;

v) O titular não tenha, no passado, desde 2003, iniciado mais do que um período de isenção do mesmo tipo;

vi) O titular não tenha dívidas fiscais não suspensas legalmente;

vii) O titular não tenha dívidas à Segurança Social não suspensas legalmente.

A verificação de todas estas condições é suscetível de ser automatizada, dado que todas elas constam de bases de dados informatizadas.[1076] Assim, criando-se um sistema operativo em cuja programação se indique:

i) Qual a localização de cada uma das bases de dados onde cada uma daquelas condições pode ser verificada. Cada um dos tipos de dados que são necessários para a instrução do procedimento (rendimentos, valor dos prédios, cadastro dos domicílios fiscais, cadastro de outros benefícios fiscais) está localizado em bases de dados diferentes, do órgão competente para o procedimento, em serviços diferentes do mesmo órgão e, frequentemente, noutros organismos públicos;[1077]

ii) Se estabeleçam os parâmetros de comparação, as condições e as respostas, por exemplo, os limites dos valores do prédio e do

[1076] Essa automatização está agora prevista na própria lei, nos termos estabelecidos na alínea a) do n.º 6 do artigo 46.º do EBF.

[1077] Por exemplo, no caso do procedimento de liquidação do IRS, além dos elementos declarados pelos sujeitos passivos, os sistemas informáticos tratam os dados relativos aos rendimentos obtidos, que são enviados pelas entidades patronais à administração tributária, bem como os relativos a pensões que as instituições de segurança social enviam, os bancos, que enviam os dados relativos a despesas com juros para aquisição de habitação, as seguradoras, que enviam as despesas com seguros de vida e planos de reforma, as escolas, que enviam as despesas de educação, os serviços de saúde que enviam as despesas de saúde e, em geral, todas as empresas, que enviam as faturas correspondentes a despesas gerais e familiares que cada adquirente pode deduzir à coleta do IRS, etç. Cada um desses tipos de rendimentos ou despesa consta de bases de dados separadas, a que acede o sistema que efetua a instrução do procedimento de liquidação do IRS, para efetuar o apuramento do imposto a pagar.

rendimento, sendo a resposta positiva quando o valor é inferior aos parâmetros e negativa no caso inverso;

iii) Se determinem os efeitos da verificação e da não verificação de cada uma das condições, por exemplo, neste caso, basta a não verificação de uma delas para que a decisão seja de indeferimento, se todas se verificarem a decisão será de deferimento;

iv) A inserção no sistema de um conjunto de textos parametrizados para cada uma das decisões, com espaços em branco que o sistema preencherá com os dados que recolheu das diferentes bases de dados;

v) A criação de funcionalidades de envio de notificações para audição prévia e de notificação da decisão final;

vi) A criação de funcionalidades de comunicação ao sistema responsável pelo procedimento de liquidação do imposto, com a informação de que o prédio em questão está isento de imposto a fim de que este não proceda à sua liquidação.

O algoritmo de programação do sistema informático corresponde ao conjunto de diligências de instrução do procedimento, que no passado consistiam em diligências instrutórias efetuadas pelo órgão competente para a decisão. O sistema informático efetua as mesmas operações que no passado eram efetuadas manualmente pelos recursos humanos afetos à sua instrução nos serviços correspondentes aos órgãos da administração pública competentes. Cada uma dessas diligências era formalizada em documentos, sendo que em muitos casos esses documentos tinham que ser obtidos pelos requerentes noutros órgãos da administração pública e noutros casos eram obtidos oficiosamente pelo próprio órgão competente para a decisão, em especial quando se tratava de elementos nele existentes. O sistema informático fica dotado com funcionalidades próprias para obter os dados, nas bases de dados onde eles estiverem guardados e para, mediante aquele processo matemático ou dedutivo, extrair conclusão positivas ou negativas acerca dos pressupostos de instrução do procedimento.

Na instrução manual, a decisão proferida no procedimento deveria sustentar-se e reportar à informação constante desses documentos e resultava da análise que o órgão competente deles extraia. A racionalidade da decisão poderia sempre ser averiguada por comparação e análise dos documentos instrutórios e das conclusões que deles extraiam os serviços.

A informatização e a automatização dos procedimentos permitem que a verificação de todos os pressupostos da decisão final seja feita praticamente de forma instantânea, e para que o sistema informático desencadeie a notificação da decisão operada no procedimento não é indispensável qualquer intervenção manual nem intelectual do titular do órgão competente para a decisão.

Significa isto que o sistema informático é suscetível de produzir uma conclusão do procedimento com idêntico teor daquela a que conduziria uma instrução manual, porque as diligências que executa são iguais às da instrução manual, mas enquanto no procedimento manual é necessária a documentação dessas diligências para que o órgão competente forme a sua decisão com base na sua apreciação, o sistema informático não necessita deles, porque a decisão corresponde apenas a uma das muitas iterações que executa.

Daqui resultam, entre outras, três questões fundamentais, sendo uma delas a da documentação dos atos e da formação do processo administrativo, que analisamos no ponto seguinte (1.2 do presente capítulo), a outra a da natureza da "decisão" proferida pelo órgão competente, com base na execução do programa, que analisamos imediatamente e a terceira a que se refere à segurança quanto aos dados com que os sistemas informáticos operam (que analisamos no ponto 1.3 do presente capítulo). Começamos pela segunda.

1.1.2. – A programação do ato administrativo

Alguns autores falam do chamado ato administrativo eletrónico, nos casos em que o procedimento administrativo seja informatizado e a produção da decisão final seja efetuada com recurso a um sistema informático automatizado. Defende-se que um sistema informático poderia, por si, vincular um órgão da administração com os atos por si praticados, defendendo mesmo a necessidade de uma revisão do conceito de ato administrativo.[1078] Outros autores distinguem os procedimentos administrativos em que se utilizam tecnologias eletrónicas dos restantes, classificando-os com conceitos

[1078] É o caso de Francisco Úría que defende a necessidade de *"revisar integralmente da construcción tradicional de acto administrativo"*. Fernández, F.U. (2004). Efectos Jurídicos de la Firma Electrónica: La Emisión de Actos Administrativos «On Line». Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid., pág. 361.

próprios, como teleprocedimento ou ciberprocedimento.[1079] Wolf, Bachof e Stober falam de uma "*Administração Mecânica*", referindo-se ``*a sua aplicação aos procedimentos de massa aos casos em que "a aplicação do direito é um processo lógico no qual não interferem decisões de vontade precisas (...) poderá ser feita de forma igualitária através de máquinas programadas pelo ser humano*", dando como exemplo as liquidações de impostos.[1080]

Em Portugal, Pedro Gonçalves fala do "*ato administrativo informático*", como um ato de vontade determinado por sistemas informáticos "*inteligentes*", dotados de programação não "*determinista*", mas "*probabilística*" que produziriam decisões administrativas, mediante uma programação em que "*não está assegurado naturalmente o domínio do órgão sobre o processo decisório*".[1081] O Autor refere-se mesmo a uma "*delegação no computador da tarefa decisória*", acrescentando que neste caso "*a informática não apoia o processo decisório, fornece a decisão, dispensando o funcionário dessa tarefa*".[1082] Um dos casos em que isso ocorreria, seria no procedimento de liquidação de impostos pela administração tributária.

Vasco Pereira da Silva designa este fenómeno como da "*Administração através de máquinas*".[1083] Enquadra, porém, essa atividade no contexto da necessidade do respeito dos órgãos da administração pública pelos direitos substantivos e procedimentais dos cidadãos, relevando o papel do procedimento e do próprio ato administrativo nessa desiderato. Os direitos procedimentais são assumidos pelo Autor como "*manifestação de dignidade da pessoa humana ao nível do relacionamento dos particulares com a administração, a qual postula o tratamento do particular como sujeito de direitos subjetivos (substantivos e de procedimento*)". [1084] E em consequência, relevando a função garantística e de realização do direito e da justiça, do procedimento

[1079] Têm sido muito utilizados estes conceitos na doutrina jurídica. Por todos, Gutiérrez, Rubén Martínez; op. cit., pag. 228. Como refere o autor, *"actualmente existen actividades administrativas puramente mecânicas en las que la participación directa del funcionário no resulta crucial, máxime cuando existen herramientas informáticas que puden desempenhar más eficazmente dicha labor"*. Gutiérrez, R.M. (2009), Op. cit., pág. 217.
[1080] Wolf, H.; Bachof, O; Stober, R. (2006*). Op. cit*, pág. 449.
[1081] Gonçalves, P. (1997). O Acto Administrativo Electrónico. *Scientia Jurídica, Revista de Direito Comparado Português e Brasileiro, Tomo XLVI. N.º 265/267*, Universidade do Minho, pág. 73.
[1082] Gonçalves, P. (1997). Op. cit., pág. 49. O Autor acrescenta, entre outros, o inconveniente da "*espiral da automação*" dos procedimentos administrativos, pelo facto de aumentar a "*dependência da administração em relação à máquina (o uso do computador dá lugar a um funcionário dependente, não criativo)*". Idem pág. 51.
[1083] Silva, V.M.P.D.P. Op cit., pag. 481.
[1084] Ibidem. Ibidem.

administrativo, enfatiza que "*as atuações administrativas suscetíveis de afetar direitos fundamentais devem ser tomadas em resultado de um procedimento administrativo*".[1085]

No procedimento administrativo automatizado o Autor chama a atenção para os "*numerosos perigos*" da "*práticas de atos administrativos em série*" e da "*administração de massas*", defendendo a necessidade de "*regulamentação especialmente adequada às suas particularidades de procedimento e de forma*".[1086] E nessa linha defende que a programação dos sistemas informáticos que tramitam os procedimentos administrativos é juridicamente relevante e, "*na medida em que possuem um caráter geral, e abstrato e que estabelecem as regras a que fica submetida a prática futura de decisões automatizadas, devem ser considerados como regulamentos*".[1087]

Por outro lado, releva-se a necessidade de limitar a automatização aos atos de instrução que o possam ser, nomeadamente aqueles que respeitam a recolha de informação e a tarefas de execução, e não atos que "*dependem de apreciações, valorações e escolhas, que só o homem está em condições de fazer*". Conclui o Autor que a automatização deve sempre respeitar os fins do procedimento e os direitos fundamentais dos cidadãos, de modo que "*não seja suscetível de pôr em causa o conteúdo essencial desses direitos fundamentais*".[1088]

Embora não defenda uma revisão do conceito do ato administrativo o mesmo Autor entende que ele adquire "*uma novíssima e futurista função de instrumento capaz de potenciar o desenvolvimento da mecanização da administração e da sua atividade*", ao mesmo tempo que assegura a "*sua clássica função de defesa do cidadão perante a Administração Pública, atuando sob forma automatizada*".[1089]

Na mesma linha Marcelo Rebelo de Sousa, defendia a necessidade de uma revisão do CPA em face da emergência da generalização da utilização das tecnologias eletrónicas no procedimento administrativo, relevando que ele estava "*concebido para um procedimento administrativo predominantemente escrito, mas abstraindo da computorização, abstraindo da informatização*".[1090]

Não cabe no objeto da nossa investigação a reflexão acerca da natureza do ato administrativo praticado por meios eletrónicos automatizados, mas é relevante que analisemos a importância dos suportes eletrónicos utilizados no procedimento, da sua

[1085] Ibidem, página 440.
[1086] Ibidem, página 484 e 485.
[1087] Ibidem, página 485.
[1088] Ibidem, página 487.
[1089] Ibidem, página 489.
[1090] Sousa, M.R. (1992). Regime do Ato Administrativo. *Direito e Justiça,* Volume VI, Lisboa, página 40.

autenticação e da sua preservação.[1091] E para isso é necessário que se estabilize do que estamos a falar quando tratamos de analisar a utilização das tecnologias eletrónicas no procedimento administrativo.

Em primeiro lugar é necessário separar as situações em que a utilização dos sistemas informáticos é apenas parcial, e serve apenas para as tarefas instrumentais, repetitivas ou de realização de operações matemáticas, sendo que a apreciação dos factos, a sua valoração, a interação com os interessados e a decisão são praticadas por recursos humanos afetos à instrução do procedimento. A maioria das situações em que se utilizam meios eletrónicos automatizados é deste tipo.

Em segundo lugar os casos em que o procedimento é totalmente informatizado e automatizado, sendo a decisão aplicada pelo sistema informático e a sua notificação ao interessado automatizada. Trata-se, fundamentalmente, de procedimentos em massa, em que não existe discricionariedade do órgão, nem na apreciação e valoração dos factos do procedimento nem na decisão, sendo esta estritamente vinculada a um conjunto de pressupostos quantificáveis ou suscetíveis de decisão segundo um processo lógico-dedutivo. São os casos, como anteriormente referimos, da liquidação dos impostos, em algumas situações, ou dos procedimentos de reconhecimento do direito a isenção de certos tributos, quando a decisão é vinculada e assente em dados objetivos e não suscetiveis de valoração não demonstrável em termos matemáticos ou lógico-dedutivos.

No primeiro caso, a automatização de fases ou de tarefas parciais do procedimento é meramente instrumental e a decisão continua a ser praticada, como no passado, manualmente pelo titular do órgão. Em muitos procedimentos ocorre que são automatizados todos os atos de instrução, mas não o é a decisão final, porque existe um conjunto de possibilidades de decisão e não é possível a sua automatização. Por exemplo, porque existe uma margem de discricionariedade que depende de uma valoração ou avaliação não quantificável nem parametrizável, ou subjetiva, bem como nos casos em que o funcionamento automático dos sistemas informatizados não pode ir mais longe do que à identificação de um conjunto de probabilidades, que para se converterem em decisão necessitam de intervenção humana. Nestes casos, o procedimento e o ato administrativo mantêm a sua natureza.

É também neste sentido que uma alteração legislativa recente à Lei do Procedimento Administrativo alemã passou a prever-se expressamente a possibilidade

[1091] Roques-Bonnet utiliza mesmo o conceito de ato administrativo eletrónico. Roques-Bonnet, M.C. (2010). Op. Cit., pag. 551 e 552.

de completa automatização dos procedimentos administrativos, incluindo a adoção do ato administrativo. Mas essa possibilidade fica dependente de duas condições fundamentais, sendo uma a existência de habilitação legal expressa para essa automatização e a outra que se trate de procedimentos de apreciação e de decisão vinculadas, estando afastada essa automatização da produção do ato administrativo nos casos em que exista alguma margem de discricionariedade, como é o caso da liquidação dos impostos.[1092] A lei estabelece algumas cautelas, como é o caso da necessidade de o órgão efetuar o apuramento manual de um conjunto de situações, não só como forma de se garantir o domínio do conhecimento, como o controlo da adequação do funcionamento dos automatismos.

O que distingue o procedimento administrativo automatizado é a automatização integral, incluindo a aplicação da decisão final, sendo, porém, certo que, nos casos em que o interessado exerça o direito de audiência prévia, a sua análise não deverá ser automatizada, quando não possa ser apreciada naqueles termos matemáticos e lógicos.

O funcionamento dos sistemas automatizados depende da programação, dado que é esta que enforma o modo como os mecanismos automáticos operam. A programação depende da análise funcional, que é o documento que transpõe para a linguagem informática o conteúdo das normas jurídicas aplicáveis ao procedimento que o sistema informático executará.

Depois de construído o programa informático, a análise funcional fica nele materializada e ele está em condições de executar os atos e as formalidades que anteriormente eram efetuados pelos agentes do órgão da administração pública competente para o procedimento. O programa informático não se distingue, em termos de conteúdo jurídico, do conjunto de procedimentos e do conteúdo do conhecimento que os funcionários responsáveis pela realização dos atos e diligências do procedimento tinham que efetuar na sua instrução manual. São exatamente iguais, com a única diferença de o sistema informático as fazer de forma mecânica e, por isso, normalmente mais rápida.[1093]

[1092] A redação da lei é a seguinte: *"§ 35a Vollständig automatisierter Erlass eines Verwaltungsaktes. Ein Verwaltungsakt kann vollständig durch automatische Einrichtungen erlassen werden, sofern dies durch Rechtsvorschrift zugelassen ist und weder ein Ermessen noch ein Beurteilungsspielraum besteht*".

[1093] Concordamos aqui com Pedro Gonçalves, que assim considera a natureza da programação: "*Por serem preceitos regulativos fechados, absolutamente deterministas, as instruções constantes do programa informático, não são equiparáveis a instruções em sentido jurídico*". Gonçalves, P. (1997). Op. cit., pág. 61. Mas não podemos concordar que as decisões do procedimento automatizado sejam "*decisões*

O programa informático contém o modo de aplicação das normas legais que aplicáveis, a cada um dos procedimentos em concreto que forem instaurados. O programa informático consubstancia a interpretação e o modo de aplicação dessas normas a cada um daqueles casos em concreto, incluindo as normas substantivas e procedimentais, que o órgão competente para o procedimento entende aplicáveis, que que aplicaria quer no caso de o procedimento ser instruído manualmente que automaticamente. Por essa razão, não existe diferença substancial entre a instrução manual do procedimento e a sua automatização, e isso ocorre nas suas três fases mais importantes:

1.1.2.1. – A subsunção dos factos ao programa informático

Os programas informáticos não efetuam qualquer atividade de subsunção dos factos relevantes para a instrução do procedimento, nem quanto aos factos relevantes para a instauração e para a aplicação, em concreto do programa a cada procedimento, nem quanto à subsunção dos factos relevantes para a sua instrução.

Relativamente à subsunção dos factos determinantes da aplicação do programa informático, trata-se da questão de saber se a aplicação do programa a cada procedimento administrativo representa uma subsunção efetuada pelo sistema informático, dos factos determinantes da sua aplicação a cada procedimento em concreto.

Trata-se de saber o modo como se decide a aplicação a um determinado procedimento de um determinado programa informático e não de outro. Ou seja, como se efetua o diagnóstico, em função da relação jurídica subjacente ao procedimento, acerca de qual o sistema informático que efetuará as tarefas correspondentes à respetiva instrução. Mas também aqui não existe qualquer decisão que não seja imputável ao órgão da administração ou ao interessado no procedimento.

---

informáticas", dado que o caráter determinístico que o Autor assinala ao programa resulta do facto de ele ser dependente da vontade do autor do programa, que será o titular do órgão competente para a decisão. É ele que determina a vontade que a decisão revela. Aliás é o próprio Autor que o reconhece mais adiante, quando refere que "*Quando elabora o programa, mais do que 'regular' a Administração, está, pois, a 'determinar' a atuação concreta subsequente da máquina; o programa fixa, de modo definitivo, as premissas abstratas de decisão, que serão depois complementadas pelas premissas do caso concreto*". Ibidem, pág. 63. Do nosso ponto de vista, o programa não se limita a estabelecer as premissas gerais, mas desce ao pormenor de prever todas as situações que, em concreto, se possam verificar, para que o programa execute os procedimentos estritamente previstos.

Nos casos em que a iniciativa do procedimento é do interessado e a entrega do requerimento inicial é efetuada por via eletrónica, a subsunção que desencadeia a aplicação do sistema informático resultante da programação é do próprio interessado, dado que as funcionalidades de entrega pelo interessado e de receção pelo sistema fazem já parte da programação. E nos casos em que a iniciativa do procedimento é do órgão competente, é ele que decide que sistema aplicar à sua instrução e decisão. Não são os próprios programas que operam autonomamente na escolha dos procedimentos a que se aplicam em função da natureza e da iniciativa dos procedimentos, mas os interessados e os órgãos competentes.

Do mesmo modo, os factos, os dados e os elementos relevantes para a instrução são determinados minuciosamente pelo órgão competente na análise funcional, onde são assinalados ao programa informático os dados que vão ser tratados, o local onde estão disponíveis, bem como o próprio modo como esses dados vão ser comparados ou conjugados com outros. O programa efetua um conjunto de operações previamente determinadas, de modo fechado, sendo essa determinação exaustiva e sem margens para quaisquer imprevistos ou ponderações não contempladas. Caso o grau de minúcia na previsão e no tratamento não seja suficiente, o programa simplesmente não opera. Por essa razão, as análises funcionais são documentos exaustivos, que preveem todas as possibilidades e todas as consequências, no que respeita a cada uma das interações que o programa vai efetuar.

1.1.2.2. – A apreciação e qualificação dos elementos do procedimento

Outra questão que se coloca é a de saber se os programas informáticos procedem à análise, classificação, qualificação e avaliação dos factos relevantes para o procedimento, consubstanciados nos dados que tratam. A resposta é claramente negativa. Os sistemas informáticos não apreciam nem avaliam. Operam sobre dados que podem representar factos previamente determinados, de modo previamente determinado, mediante comparação e, numa estrutura dedutiva sequencial, determinística, de aplicação de uma consequência perante a constatação de um dado que serve de causa, fazem avançar o procedimento para fases subsequentes de tramitação.

É verdade que em algumas situações os programas informáticos são preparados para, em face da análise de um conjunto que dados previamente determinados na análise

funcional, gerarem como resultado um conjunto de probabilidades e eliminarem outras. Mas nesse caso trata-se apenas de programas de apoio ao órgão competente para o procedimento, cabendo a este a sua valoração. Também é verdade que em face dessas probabilidades pode o titular do órgão adotar um conjunto de critérios de decisão, que também eles podem ser parametrizáveis e quantificáveis e, por essa via, suscetíveis de automatização. Mas quando essa quantificação não é possível, não é também possível a automatização. Ela depende sempre de um algoritmo.[1094]

Os programas informáticos não apreciam factos nem os investigam. Executam apenas operações instrumentais previamente determinadas pelo órgão competente.

1.1.2.3. – A decisão final do procedimento automatizado

Ao contrário do que se possa entender, a decisão nos procedimentos administrativos nunca serão proferidas por máquinas nem por quaisquer entidades que não sejam os titulares, homens e mulheres, dos órgãos da administração pública. E por essa razão, o ato administrativo, mesmo que adotado mediante o recurso a máquinas, sejam elas de que natureza forem, depende sempre de uma apreciação, valoração, formação da vontade e da sua expressão, pelo do titular do órgão competente para a decisão.

Quando se classificam os sistemas informáticos como sistemas inteligentes, não é disso que se trata, porque a inteligência jamais será uma faculdade das máquinas nem dos sistemas. A utilização desse conceito revela apenas o voluntarismo daqueles que trabalham com instrumentos que sendo inovadores e aumentando a eficiência e a produtividade, representam um passo adiante na eficiência dos órgãos da administração pública no cumprimento da sua missão. Nesses casos, inteligência significa apenas mais eficiência, porque as máquinas não possuem intencionalidade volitiva, nem capacidade

[1094] E como refere com propriedade Pedro Gonçalves, "*essencial é que o órgão ou agente tenha um efetivo domínio sobre o sentido e o conteúdo da decisão*". Gonçalves, P. (1997). Op. cit., pág. 72. Não podemos é concordar com o Autor em designá-la como uma "*decisão informática*". Na verdade, uma decisão é sempre o produto da vontade e de um processo gnoseológico e volitivo de formação, e esse processo não é automatizável. Podemos tornar esse processo repetível, sempre que ocorram circunstâncias iguais e sejam quantificáveis, mas a vontade e o conhecimento são sempre de quem o determina e nunca da máquina que o executa. E por isso a decisão é sempre humana. Tal como numa linha de montagem industrial robotizada o conhecimento que permite o seu funcionamento é humano e nunca das máquinas, que são apenas instrumentos.

intelectiva. Não existem sistemas informáticos inteligentes, como não existem objetos nem equipamentos inteligentes.[1095]

Do que se trata é de os titulares desses órgãos serem apoiados, no exercício das suas funções, por instrumentos de trabalho que executam as suas competências funcionais. E os sistemas informáticos que operam com tecnologias eletrónicas são apenas instrumentos de trabalho, como eram a máquina calculadora ou a máquina de escrever, que passaram a efetuar com maior eficiência as tarefas anteriormente manuais.

Ao executarem a programação, esses sistemas executam a vontade do órgão da administração, pelo que o ato administrativo conserva a sua natureza de expressão da vontade da administração.

Em nosso entendimento não se pode dizer que as máquinas possuem vontade ou que a instrução do procedimento e a decisão nele proferida com recurso a programas eletrónicos esteja para além da vontade do órgão competente para a decisão, ou que essa decisão lhe seja alheia. E tal como nos procedimentos instruídos manualmente pelos funcionários por eles responsáveis a decisão expressa a vontade do órgão e não a vontade individual de quem efetua a instrução ou adota a decisão no procedimento, também nos casos em que são utilizados sistemas informáticos existe qualquer vontade das máquinas.

Os programas informáticos são apenas instrumentais e a sua operacionalidade é estritamente determinada pela programação, sem qualquer margem de imprevisão que permita a prática de atos fora dos termos estritamente previsto na programação. É por essa razão que os únicos procedimentos que são suscetíveis de automatização integral são aqueles em que a apreciação e a decisão são estritamente vinculadas. O sistema informático executa sempre a vontade do órgão, expressa nas regras funcionais que subjazem à programação. Mas não se pode utilizar o conceito de ato administrativo eletrónico, porque em nada se distingue dos restantes.

Nestes casos o que acontece é que a expressão da vontade do órgão na decisão se dilui no tempo, entre o momento da programação e o momento em que se materializa em cada caso concreto, cujos contornos e consequências foram minuciosamente previstos na programação, a expressão dessa vontade. Por essa razão, mais do que uma

[1095] Pedro Gonçalves refere, a propósito, que não se podem considerar como atos administrativos as decisões praticadas por um "*sistema inteligente*". Gonçalves, P. (1997). Op. cit., pág. 73. Mas não há sistemas inteligentes. Os sistemas informáticos podem efetuar um conjunto mais ou menos complexo de processamentos de dados, mas a inteligência será sempre de quem determina o programa e nunca do programa em si mesmo, porque esse é sempre meramente instrumental.

decidir, o programa informático, quando opera sobre o procedimento de forma integralmente automatizada, executa apenas a expressão da vontade de decisão e do seu conteúdo, do titular do órgão. E isso é assim porque o titular controla integralmente o funcionamento do programa, não só porque foi ele que o criou, mas também porque esse programa é apenas um instrumento de funcionamento do serviço. E por essa razão o funcionamento do programa é acompanhado em permanência pelo titular do órgão, sendo que esse funcionamento depende do seu controlo exclusivo.

Não sendo fonte de vontade, o sistema informático limita-se a aplicar a intenção volitiva do titular do órgão, competente para a decisão, na conclusão de cada um dos procedimentos. Essa aplicação é uma ação mecânica, determinística e sem qualquer substância intelectual.

Mas a formação da vontade é um processo que se reporta a uma relação jurídica e a um procedimento administrativo em concreto, a partir dos elementos que resultam da respetiva instrução e, por essa razão, só se pode consolidar no final do procedimento. Em condições normais isso é verdade, mas essa conclusão não impede que seja também verdade que existam casos em que a vontade se possa formar por reporte a um conjunto de fatores que sejam exatamente iguais, que conduzam sempre necessariamente ao mesmo resultado e que se repitam de forma sistemática. Existem, na verdade, muitos procedimentos administrativos que são exatamente iguais a outros, relativamente aos quais o processo de formação da vontade e os fatores que a fundam são iguais, pelo que a conclusão pretendida e desejada é sempre a mesma. Nesses casos a decisão será sempre a mesma. E se o órgão competente para a decisão pretende que seja sempre essa mesma a decisão, então o processo de formação da vontade ocorreu, da mesma forma, determinada pelo órgão competente, mas esse processo distendeu-se no tempo, entre o momento em que se formou, com base em pressupostos de facto iguais, e o momento em que o sistema informático o aplica ao caso concreto que havia sido antevisto e com os exatos contornos dessa antevisão.

Assim, o processo de formação de vontade é um *continuum*, entre o momento em que se agrupam os fatores de decisão e se determina ao sistema, caso a caso, tendo em conta minuciosamente todas as variáveis, que procedimentos são aplicáveis a cada caso, para que ele mecanicamente os aplique, e o momento que em concreto essa aplicação é efetuada. Só nesse momento a vontade do órgão se consuma em decisão, pelo que o processo de formação e de manifestação da vontade do órgão se distende no tempo, numa continuidade incindível.

Naturalmente que existe sempre um pressuposto essencial nesta construção, que é o de o titular do órgão possuir permanentemente o controlo direto e pleno sobre o sistema informático. Só assim se produz uma condição da validade do seu funcionamento, que é o de ele ser um instrumento apenas de execução, e não de formação da sua vontade, e de ele se limitar a reproduzi-la.

1.1.2.4. – A natureza regulamentar do programa informático

A doutrina tende a considerar a programação dos sistemas informáticos, baseada na sua análise funcional como tendo natureza de regulamento.[1096] Como anteriormente referimos, no ponto 1.1.2 do presente Capítulo, Vasco Pereira da Silva afirma que os programas informáticos "*possuem um caráter geral, e abstrato",* pelo que *"devem ser considerados como regulamentos*".[1097] Do mesmo modo Pedro Gonçalves considera tratar-se de um regulamento interno, acrescentando que "*embora determinando a decisão concreta, não cria qualquer regra jurídica que discipline relações entre a Administração e os particulares ou que exerça um efeito vinculativo inovador*".[1098]

O CPA de 2015 veio definir legalmente o conceito de regulamento administrativos, como normas gerais e abstratas que visem a produção de efeitos jurídicos externos, emitidas no exercício de poderes jurídico-administrativos.[1099]

As análises funcionais são instrumentos de aplicação de normas legais a cada um dos casos concretos. Elas consistem na especificação dessas normas de forma tão minuciosa que preveja todas as combinações factuais possíveis para que, perante cada caso concreto nelas previsto se aplique uma decisão também nelas prevista e determinada. O programa informático contém os mecanismos exaustivos de previsão de

[1096] Com refere Alberto Olmeda, a programação que está na base de funcionamento desses sistemas, constitui um conjunto de normas, com *"efectos generales y que se integra en el Ordenamiento Jurídico de foram estable y permanente hasta que, obviamente, sea derrogada o sustituida por outra"*. Olmeda, A.P. (2007), Op. cit. pag. 285.
[1097] Ibidem, página 485.
[1098] Gonçalves, P. (1997). Op. cit., pág. 66.
[1099] Como referem esta norma "*veio preencher uma lacuna no nosso direito administrativo*" e "*ao encontro do consenso praticamente unânime da doutrina e da jurisprudência*". Gonçalves, F.; Alves, M.J.; Vieira, V.M.F.; Gonçalves, R.M.; Correia, B. e Gonçalves, M.V. (2016). *Novo Código do Procedimento Administrativo Anotado e Comentado, 3.ª edição*. Edições Almedina, S.A. Coimbra, página 183. No entanto, como ensina Freitas do Amaral, já desde a revisão constitucional de 1982, os n.ºs 7 e 8 da Constituição, estabelecem o regime dos regulamentos, nomeadamente a dupla obrigatoriedade de lei habilitante e da menção expressa da lei que visam regulamentar. Amaral, D. F. (2001). *Curso de Direito Administrativo, Volume II*. Op. cit., página 161.

todas as situações possíveis e de todas as decisões aplicáveis em cada uma delas. Por essa razão, dificilmente se podem considerar normas legais, gerais e abstratas que complementam a lei, dado que apenas se limitam a cristalizar em linguagem informática os mecanismos necessários para a aplicação da lei nos mesmos termos em que ela seria aplicada se não existisse programa informático. Poderiam eventualmente preencher o requisito da generalidade, dado que não seriam previamente identificáveis os interessados a que se aplicam, mas mais dificilmente cumprem o requisito da abstração, dada a sua dificuldade em vincularem a própria administração e em se aplicarem de forma sistemática sem limitação temporal.[1100]

Na verdade, o programa informático é meramente instrumental, e pode conter erros ou conduzir o programa informático à produção de resultados não pretendidos, dada a diversidade de factos a que se aplica. Pode ainda conter deficiências de previsão, porque não foram contempladas todas as situações possíveis. Nesses casos, o órgão competente para o procedimento não deve ficar obrigado a aceitar o respetivo resultado, devendo antes corrigi-lo.[1101]

Do mesmo modo a análise funcional e o programa informático não são normas que tenham como destinatários os funcionários do serviço nem os eventuais interessados nos procedimentos. São definições funcionais destinadas a garantir a operacionalidade dos sistemas informáticos, de acordo com as normas legais ou regulamentares aplicáveis.

Por outro lado, a natureza das análises funcionais e dos programas informáticos será sempre muito diversa e dificilmente se poderão classificar como cumprindo os requisitos da generalidade, dado que casos poderão existir em que se criam programas para situações concretas, com destinatários claramente identificados. Existem também casos de programas temporários e de outros em que anualmente se altera a respetiva

---

[1100] Mário Aroso de Almeida refere-se à abstração como a capacidade de o regulamento não dizer "*exclusivamente respeito à produção de um único efeito jurídico, no qual se esgote, mas que seja passível de aplicação ao longo do tempo*". E mais adiante define a abstração como "*a vocação de execução permanente*", identificando-a como "*o critério verdadeiramente distintivo do ato normativo, que determina os traços essenciais do regime dos regulamentos*". Almeida. M. A. (2015). *Teoria Geral do Direito Administrativo. O Novo Regime do Código do Procedimento Administrativo, 3.ª Edição*. Edições Almedina, S.A. Coimbra, páginas 139 e 140.

[1101] E a submissão da própria Administração ao regime do regulamento é um dos efeitos da sua generalidade e abstração, como muito bem menciona Mário Aroso de Almeida: *"Isso explica que nem sequer a mesma entidade que emanou um regulamento possa afastar-se, na tomada de decisões concretas, do regime por ele instituído"*. Almeida. M. A. (2015). Op. cit., pág. 134.

programação, pelo que será difícil a sua integração na definição de regulamentos em todas as situações, bem como dos chamados atos administrativo.

A criação do programa informático não se enquadra tipicamente no exercício da competência regulamentar do órgão competente para o procedimento, dado que ele não se destina a satisfazer uma necessidade normativa, nem a especificar uma norma aberta. O fim do programa informático não é típico dos fins do regulamento, porque através dele o titular do órgão se limita a determinar a criação de um equipamento instrumental de apoio à sua função de responsável pela instauração, instrução e decisão do procedimento, sendo que essa determinação não se distingue, em termos substanciais, do modo como os procedimentos são instruídos manualmente.[1102] Na verdade, a análise funcional limita-se a transpor, para uma máquina informática, os mesmos modos de instauração, instrução e decisão dos procedimentos que são praticados na sua tramitação manual.[1103]

Por outro lado, a criação do programa informático é um ato de gestão do serviço, destinado a aumentar a eficiência do procedimento. Integra-se, por isso, nas competências do respetivo titular, de gestão do órgão competente para o procedimento. Por essa razão, não deve estar dependente de habilitação legal, como acontece com o regulamento, como estabelece o n.º 1 do artigo 136.º do CPA.[1104] [1105]

Finalmente, sendo apenas instrumentais das normas que se destinam a aplicar, os programas informáticos e as respetivas análises funcionais que estão na base da sua construção, não são fontes de direito.[1106] Na verdade a fonte de direito é a lei, limitando-se o programa informático a fazê-la operar num ambiente eletrónico, nos precisos

[1102] Nos casos em que os órgãos administrativos instauram e decidem uma quantidade elevada de procedimentos, a sua instrução é efetuada por equipas de trabalho compostas por uma multiplicidade de funcionários, e muitas vezes de serviços, sendo que, nessas situações, o titular do órgão emite instruções acerca dos procedimentos a adotar na instrução. Maurer distingue essas instruções, dos regulamentos, considerando que não se trata de normas regulamentares, pela sua falta de eficácia externa. Maurer, H. (2011). Op. cit. pág. 360

[1103] Na lição do Professor Freitas do Amaral, existe uma "*identidade material entre a lei e o regulamento – substancialmente os regulamentos são leis*", acrescentando que se distinguem "*apenas por aspetos orgânicos e formais*". Amaral, D. F. (2001). *Curso de Direito Administrativo,* Op. cit., pág. 168 e 169.

[1104] Seguindo Freitas do Amaral, "*o exercício de qualquer atividade administrativa regulamentar tem que ser precedido de uma lei habilitante*". Amaral, D. F. (2001). *Curso de Direito Administrativo,* Op. cit., pág. 182, e mesmo a previsão da admissibilidade dos regulamentos independentes, que o novo CPA consagra na parte final do n.º 2 do artigo 136.º, não dispensa a existência d elei habilitante.

[1105] Embora "*el órgano competente para la promulgación del reglamento se determina mediante la ley habilitante*", "*queda, en princípio, a la discrecionalidad de órgano competente para dictar el reglamento el hace uso de la habilitación legal*". Maurer, H. (2011). Op. cit., pág.s. 362 e 364, respetivamente.

[1106] Com refere Mário Aroso de Almeida, "*Regulamentos são atos normativos*", bem como, "*O regulamento é fonte de direito*". Almeida. M. A. (2015). Op. cit., pág. 133, 134.

termos nela estabelecidos. E em muitos casos o próprio programa informático destina-se a executar os procedimentos previstos numa norma legal de natureza regulamentar.

Embora não se integre o âmbito da nossa investigação o estudo da natureza jurídica dos programas informáticos, nem dos regulamentos, entendemos que as análises funcionais que lhe estão na base devem ser previamente aprovadas pelo titular do órgão competente para o procedimento. O programa informático é um instrumento da ação administrativa e jamais um substituto do órgão, mas se executa todos os seus atos, é necessário que exista uma garantia de que ele cumpre essa função instrumental, o que só ocorrerá se existir a certeza de que a sua ação está estritamente determinada pelo titular do procedimento.[1107]

Por outro lado a análise funcional deve ser sempre publicada, podendo ser objeto de impugnação autónoma pelos interessados. Na verdade, tendo em conta os efeitos que dela podem resultar para o universo dos possíveis interessados, será fundamental, para a defesa dos seus direitos, a possibilidade de escrutinarem a sua regularidade. Uma via possível para se alcançarem esses objetivos seria a de equiparar, para todos os efeitos, as análises funcionais a regulamentos.[1108] Essa equiparação já existe, em termos idênticos, para uma norma que equipara a regulamentos um conjunto de "*comunicações dos órgãos da administração pública*", que tenham natureza orientadora. Neste caso, afigura-se-nos que não se deveria exigir lei habilitante, até porque a utilização das tecnologias eletrónicas já é promovida genericamente pelo próprio CPA, em especial no n.º 1 do artigo 61.º e nos n.ºs 1 e 6 do artigo 14.º, sendo que este último chega a prever a existência de discriminação positiva pela utilização das

---

[1107] No mesmo sentido, Olmeda, Alberto Palomar; op. cit. pag. 289. Este Autor refere ainda que *"el procedimiento administrativo basado en médios electrónicos no tiene que suponer conceptualmente algo distinto al procedimento tradicional, sino simplemente un aprovechamiento de las ventajas que las tecnologias de la información y la comunicación presentan"*. Olmeda, A.P. (2007), Op.cit., pag. 60.

[1108] Em Espanha essa a obrigação de aprovação desses programas pela entidade competente consta do n.º 4 do artigo 45.º do Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo tendo sido regulamentadas pelo Real Decreto 263/1996, de 16/2. A mesma norma obriga a que as regras de funcionamento desses sistemas sejam publicadas. Munhoz, J.M.A., Mercado, F.G.G, Delgado, J.M.G, Espinosa, J.I.M.M, Bedoya, M.D.R.M, González, M.R., Gandasegui, F.S., Labelha, J.I.V. (2004). *Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo*. 3.ª edição, Thomson Aranzadi. Navarra, pag. 316. Do mesmo modo a Ley Geral Tributária espanhola obriga à aprovação das regras desses sistemas pelo órgão competente para a prática dos atos, no n.º 4 do artigo 96.º. O n.º 3 deste artigo prevê também a atuação automatizada da administração tributária, estabelecendo que, nesse caso, os sistemas correspondentes devem indicar quem é a entidade responsável pela prática dos atos. Boadilla, Ricardo Huesca (Coordinador) e outros; Comentarios a la Nueva Ley General Tributaria"; Thomson, Aranzadi, Navarra, 2004, pag. 643. A necessidade da publicação advém do facto de o destinatário dessas regras de programação ser a sociedade em geral e também do facto de a aprovação dessas regras se produzir à margem de qualquer pretensão formulada por qualquer cidadão interessado. Olmeda, A.P. (2007), Op. cit. Pag. 285.

tecnologias eletrónicas no procedimento. A equiparação deveria ter o objetivo finalístico de promover a publicação da análise funcional e de permitir a sua impugnação autónoma.

É verdade que com a publicação e a possibilidade de impugnação se alargam os direitos de defesa e as garantias dos interessados, mas o ganho resultante da inovação deve ser sempre repartido entre as partes do procedimento.

1.1.3. – Direitos dos interessados no procedimento eletrónico

O CPA já contém normas relevantes acerca de novos direitos dos interessados, proporcionadas pela utilização de meios eletrónicos no procedimento administrativo. É o caso do direito de acesso à informação acerca do estado do procedimento, nos termos do n.º 4 do artigo 82.º

Mas outros direitos poderiam e deveriam ser consagrados na lei, como são os seguintes:

i) O direito a consultar o processo administrativo, que poderia ser exercido por via eletrónica, obrigando-se os órgãos da administração pública a disponibilizá-lo por essa via, naturalmente mediante identificação e autenticação dos interessados. O artigo 83.º do CPA, que regula a consulta do processo, nada refere à possibilidade da sua consulta por via eletrónica, sendo que, nos casos dos procedimentos totalmente automatizados, essa consulta não só é a mais adequada como possível;[1109]

ii) Os interessados devem conhecer, com antecedência ao início do procedimento, se a sua tramitação é automatizada, devendo as respetivas especificações de funcionamento do sistema ser-lhe disponibilizadas. Essa informação deve constar também da decisão final que é notificada no final do procedimento;

[1109] Garcia Marques e Lourenço Martins consideram que "*o direito de informação dos interessados engloba ainda um 'feixe' de direitos fundamentais, de que são exemplos a consulta do processo, a transcrição de documentos, a passagem de certidões, manifestações do que sugestivamente se pode chamar um 'direito à transparência documental'*". Acrescenta que, naturalmente, esse *"acesso exercer-se-á, verbi gratia, através da consulta gratuita ao local onde se guarda o arquivo ou registo, com óbvia observância das normas e regras técnicas relativas à preservação do documento"*. Marques, G. e Martins, L. (2006). *Direito da Informática, Lições de Direito da Comunicação, 2.ª Edição Refundida e Atualizada*. Edições Almedina, S. A. Coimbra, págs. 320 e 321.

iii) Por último, a participação dos interessados no procedimento administrativo eletrónico. A Internet veio mudar o modelo de relacionamento dos cidadãos com os órgãos da administração pública. Enquanto no passado os serviços estavam tendencialmente fechados ao público e só abriam numa janela temporal pré-determinada, as redes abertas vieram possibilitar o acesso permanente aos processos e mudar o perfil do relacionamento de esporádico para permanente. Daqui resulta a possibilidade do acesso permanente ao processo pelos interessados e a possibilidade da sua participação ser também permanente.

Relevam ainda como importantes instrumentos de garantia dos direitos procedimentais dos interessados no procedimento eletrónico, as seguintes exigências que deveriam constar da lei:

i) A previsão de que não são suscetíveis de automatização as decisões proferidas em procedimentos em que a decisão não seja estritamente vinculada;[1110]

ii) O princípio da proibição da automatização da análise da audiência prévia entregue pelos interessados, a não ser nos casos em que o seu conteúdo seja suscetível de ser meramente quantitativo;

iii) A previsão de que não são suscetíveis de automatização os atos e formalidades dos procedimentos que exijam valoração não quantificável;

iv) A obrigatoriedade legal de o titular do órgão ter o controlo exclusivo da programação e do funcionamento de todos os programas informáticos do procedimento administrativo.

[1110] Afastamo-nos, neste caso, do disposto no § 35a da Lei do Procedimento Administrativo alemã, que prevendo expressamente a possibilidade de completa automatização dos procedimentos administrativos, bem como da adoção do ato administrativo, a faz depender, por um lado da existência de previsão legal expressa e, por outro lado, que se trate de procedimentos de apreciação e de decisão vinculadas, afastando a possibilidade da automatização nos casos em que exista alguma margem de discricionariedade. Do nosso ponto de vista esta última condição faz sentido, até porque não é simplesmente possível a automatização nos casos em que existe discricionariedade, a não ser quando o órgão competente estabeleça parâmetros objetivos de decisão e que isso seja possível, mas parece-nos que a necessidade de previsão legal expressa não se justificará, dado que não deve se preocupação do legislador a avaliação da adequação da automatização, mas do aplicador da lei. Binder, N. B. (2016). *Weg frei für vollautomatisierte Verwaltungsverfahren in Deutschland*. http://www.foev-speyer.de/files/de/downloads/Jusletter-IT_22.09.2016.pdf (última consulta efetuada em 2017/07/07). De qualquer forma parece-nos adequado que a lei obrigue o serviço da administração competente a efetuar um conjunto de procedimentos de forma manual, dada a importância que isso tem para que se garanta sempre o domínio do conhecimento e o controlo de qualidade da programação.

O Regulamento EIDAS não se aplica aos sistemas internos dos serviços porque em muito casos esses sistemas foram desenvolvidos e não respeitam atualmente os requisitos de confiança do regulamento. Do mesmo modo, no que respeita aos organismos públicos, é frequente os sistemas informáticos não exigirem sistemas de identificação nem serviços de confiança de mais elevado nível de garantia, é necessário que a lei estabeleça um regime de transição, limitado no tempo, que adeque esses dois tipos de sistemas a níveis mais elevados de confiança.

É também relevante que se estabeleça um regime transitório até que todos os sítios *web* dos organismos públicos sejam autenticados nos termos previstos no Regulamento EIDAS, mediante a autenticação de sítios *web*.

1.2. O processo administrativo eletrónico

A utilização das tecnologias eletrónicas no procedimento administrativo começou por ser meramente instrumental e auxiliar nas operações rotineiras e repetitivas, sem relevância jurídica, só mais tarde se generalizando e chegado à automatização em alguns casos.

Essa generalização foi quase sempre determinada pela necessidade de aumento da rapidez e da eficiência dos serviços competentes da administração pública, em especial como resposta à crescente demanda dos cidadãos. Em muitos casos essa generalização foi promovida sem se cuidar dos seus efeitos jurídicos.

Uma das consequências desse fenómeno foi a desmaterialização do processo administrativo. Dela resultou em muitos casos, uma verdadeira desestruturação do chamado processo administrativo. No contexto em que todo o procedimento administrativo era tramitado em papel, era relativamente fácil congregar no processo respetivo todos os documentos gerados, e essa disciplina estava incorporada nos procedimentos dos serviços da administração pública. Muitos atos e formalidades do procedimento passaram a ser efetuados de forma desmaterializada, e muitas vezes automatizada, pelo que se tornou supérfluo o seu registo em papel, para os fins específicos da eficácia na tramitação dos procedimentos.

Esse facto, aliado à escassez de recursos e à necessidade de urgência na conclusão dos processos, conduziu a que em muitos tipos de procedimentos, se perdesse

a ideia da importância fundamental do processo administrativo, ficando assim subtraídos ao processo elementos relevantes dos atos e das diligências efetuados.

No procedimento suportado em papel, o art.º 64.º do CPA estabelece as regras da sua organização, assegurando a sua integridade e autenticidade. Todas as diligências são documentadas, e mesmo nos casos em que são verbais, devem ser reduzidas a escrito, contendo sempre a data e o local da realização das respetivas diligências, para além dos elementos essenciais dessas diligências. Os documentos organizam-se em folhas, que por sua vez devem ser todas paginadas, de um modo que facilite a sua junção sucessiva, devendo ser todas rubricadas pelo titular do órgão responsável pelo procedimento. O n.º 2 do art.º 1.º do CPA estabelece que o processo administrativo é o conjunto de documentos, devidamente ordenados, em que se traduzem os atos e as formalidades do procedimento. É manifesta a preocupação do legislador, de garantir a ordem do processo e a sua organização, dada a sua importância para o controlo da legalidade dos atos praticados e da garantia da transparência da ação da administração pública. O direito ao procedimento assegura aos interessados o controlo da legalidade da ação administrativa e essa é, em si mesma, uma garantia contra a arbitrariedade. Por essa razão, a existência de um processo administrativo é um direito dos administrados, que se integra no direito ao procedimento, e que é essencial à garantia do respeito pelo princípio da legalidade e dos restantes princípios do procedimento, bem como dos direitos dos administrados.

Quando os órgãos da administração pública praticam os atos do procedimento em suporte eletrónico, os seus sistemas informáticos operam com dados e não com documentos. Se nos procedimentos suportados em papel os documentos são essenciais à prática dos atos, no procedimento suportado em base eletrónica, são os dados e não os documentos que são indispensáveis à produção dos atos e à conclusão dos procedimentos.

Com a possibilidade de tramitação do procedimento exclusivamente em suporte eletrónico, e do ponto de vista meramente operacional, não é necessário existirem documentos nem processo, com o sentido que o CPA lhe confere, para que todos os atos e formalidades do procedimento sejam concluídos. Bastam apenas os dados. Mesmo o requerimento inicial do interessado no procedimento, podendo ser entregue por via eletrónica no sítio institucional do serviço competente, é apenas um

conjunto de dados que logo os sistemas informáticos tratam.[1111] Do mesmo modo, toda a tramitação do procedimento pode ser desmaterializada, pelo que o procedimento passa a ser um conjunto diverso de dados que são submetidos a uma quantidade de processamentos informáticos que produzem um conjunto de resultados e proporcionam a decisão final, que em muitos casos poderá ser também ela automatizada. Nesses casos, que serão cada vez mais, não são necessários documentos para que os sistemas informáticos dos serviços da administração pública instaurem, instruam e concluam os procedimentos. E o processo, como suporte documental, deixa de ser intrinsecamente indispensável à conclusão do procedimento.

Ora os dados que são operados pelos sistemas informáticos não são suscetíveis de fornecer, por si, o conhecimento necessário para o controlo da legalidade dos atos praticados no procedimento.

Em muitos procedimentos, os dados necessários à sua tramitação são meramente quantitativos, e noutros consistem meramente em respostas de sim e não na comparação de dados com um determinado padrão de decisão. Nesses casos, inseridos que sejam os dados nos sistemas e efetuado um conjunto de verificações, que podem também ser meramente quantitativas, a produção dos atos finais nos procedimentos pode ser também automatizada.

Por outro lado, muitas vezes os dados utilizados no procedimento ou na prática do ato administrativo estão dispersos por bases de dados distintas, que umas vezes estão armazenadas nos mesmos serviços do órgão competente para a decisão e outras estão localizadas noutros serviços. Esses dados são verificados pelos programas informáticos que operam o procedimento administrativo e que a partir deles extraem os respetivos efeitos que a programação assinala, mas para que se possa apreciar a racionalidade da operação efetuada e dos efeitos extraídos é necessário que essas operações sejam

[1111] A documentação dos requerimentos, petições e outros elementos que os cidadãos entregam às administrações públicas é essencial ao exercício dos seus direitos, à sua efetividade e também à certificação do cumprimento das suas obrigações. Além da necessidade de salvaguarda dessa documentação e da integridade da sua forma e do seu conteúdo, é ainda muito importante a certificação da data e da hora da sua entrega. Essa certificação deve ser assegurada com sistemas de selos temporais, que devolvam aos interessados o documento e a certificação da data e hora da sua entrega efetiva. Nesse sentido se pronuncia Nadal, a propósito das relações administrativas: *"Un premier ejemplo concreto es el registro de entrada digital, que deberá emitir un acuse de recibo que permita verificar a posteriori que efectivamente un documento se presentó en una fecha determinada e com un contenido concreto"*. Nadal, A.G. (2009). Op. cit., pag. 55.

documentadas, reunindo-as num suporte que as torne suscetíveis de análise e de avaliação.[1112]

É necessário reconstruir a ideia de processo administrativo no paradigma eletrónico. Se ele deixou de ser intrinsecamente indispensável para a conclusão do procedimento, de um ponto de vista meramente utilitarista, pela própria natureza do funcionamento dos sistemas informáticos, é necessário que a sua existência e a sua organização seja legalmente exigida. E nesse caso é necessário partir do próprio conceito de documento, dado que, em muitos casos, é necessário definir que tipos de interações dos sistemas informáticos terão que ser documentos autónomos. A produção desses documentos, não sendo necessária à tramitação eletrónica do procedimento, terá que ser regulada por lei ou por regulamento. E essa tarefa não será fácil, dado que para os serviços administrativos basta a disponibilidade dos dados e a programação dos sistemas para que o resultado seja alcançado.

Tal como o art.º 64.º CPA exige que as diligências feitas oralmente sejam reduzidas a escrito, deveria também a lei exigir que quando as diligências sejam efetuadas por via eletrónica mediante o tratamento de dados, de cada uma das formalidades e diligências do procedimento fosse produzido um documento. Para isso, deveriam os serviços competentes identificar previamente todas as operações efetuadas pelos sistemas informáticos na tramitação dos procedimentos e formatar o conteúdo de documento que seria produzido para as evidenciar.

Exemplo de um documento que é indispensável ao procedimento é o requerimento inicial, cujo formalismo está tipificado no art.º 102.º do CPA. Existem casos em que o requerimento é efetuado mediante inserção no sítio *web* do órgão competente da administração. Para que esse órgão possa desencadear a tramitação do procedimento, necessita da disponibilidade desses dados, mas se a tramitação se efetuar de forma eletrónica e automatizada, não é necessário, para fins operacionais, o documento de onde constem estruturados, num determinado formato legível, esses

[1112] Como refere Bessio, "*En realidade la practica actual en todo el mundo es usar los registros computarizados como único suporte en muchas transacciones. Y cuando estas transacciones tienen que ser probadas en un proceso judicial pueden plantearse varios problemas: i) los datos pueden estar almacenados en diferentes sítios y es posible emplear distintas bases de datos e software; ii) la información relevante puede estar oculta o protegida, etç*". Bessio, I. P. (2015). Op. cit., pág. 122. Esta necessidade de documentação não se aplica apenas ao procedimento e ao processo administrativo, mas a todas as transações efetuadas mediante sistemas informáticos, dado que só assim o consumidor fica protegido com elementos probatórios que representem as operações que efetuou. Na verdade, nas aquisições de bens e de serviços efetuadas através de sítios *web*, o registo das transações efetuada fica na disponibilidade do titular do sítio *web*, não tendo a elas acesso o adquirente.

dados. Nesses casos perde-se a ideia de requerimento inicial, pelo que o interessado insere apenas um conjunto de dados no sistema informático. Mas é necessário que a lei exija a documentação desse requerimento, tal como é necessária a documentação de todos os atos e formalidades praticados no procedimento.

A ausência de documentação em papel dos atos de tramitação do procedimento em suporte eletrónico dificulta o acesso dos interessados ao procedimento e uma avaliação rigorosa da legalidade dos atos praticados pelos órgãos respetivos, não só porque torna muito complexa a análise dos dados que servem de base ao procedimento e à decisão, como em muitas situações pode conduzir à perda desses dados.[1113] Se para os fins operacionais do procedimento, os sistemas informáticos não utilizam documentos, mas apenas dados, a verdade é que para os fins de controlo da legalidade dos atos da administração pública, os documentos são indispensáveis, porque esse controlo é efetuado com base nos documentos. Se os dados são indispensáveis para a tramitação eletrónica do procedimento, os documentos que evidenciam a tramitação são essenciais para o controlo da legalidade e da efetividade dos direitos dos cidadãos.

Dando como exemplo um tipo de procedimento em que a generalidade dos cidadãos participa, que é o procedimento tributário de determinação e pagamento do IRS, o processo administrativo deveria ser uma unidade documental da qual constaria a declaração entregue pelos sujeitos passivos, a documentação das operações de validação efetuadas pela administração tributária, as operações de controlo, nomeadamente o confronto que é feito com outras fontes de informação (por exemplo com os documentos entregues pelas entidades patronais, demonstrando o valor do rendimento e das retenções na fonte, a documentação dos benefícios fiscais através das faturas comunicadas e das despesas de saúde, educação e habitação, etc.), as operações de apuramento do imposto a pagar ou a reembolsar, as notificações efetuadas no procedimento, a documentação dos pagamentos, etc..[1114]

[1113] Por exemplo, os artigos 83.º e 122.º do CPA consagram o direito de consulta do processo administrativo pelos interessados, o que é virtualmente impossível se não existir esse processo devidamente organizado como uma unidade autónoma. Do mesmo modo, o artigo 195.º obriga o órgão que praticou o ato a remeter o processo administrativo em caso de recurso para a entidade competente para a sua apreciação. O processo administrativo deve também ser remetido para o órgão competente em caso de alteração da competência, nos termos do n.º 3 do artigo 37.º. Do mesmo modo o n.º 1 do artigo 84.º do CPTA obriga a entidade demandada a remeter o processo administrativo ao tribunal administrativo e fiscal, *"assim como todos os demais documentos respeitantes à matéria do processo"*.

[1114] Outro exemplo que poderíamos é o da atribuição de uma pensão de reforma pelos serviços de segurança social. O cálculo do seu valor, dependendo dos anos de vida ativa e de descontos efetuados, pode ser automatizado, operando os sistemas informáticos de forma eletrónica, a partir dos respetivos dados de suporte. Mesmo nos casos em que o interessado tenha efetuado descontos para mais do que um

No passado, quando estas operações eram efetuadas em suporte de papel, o processo administrativo tributário era uma unidade documentada em papel, estando devidamente estruturados os modelos de documentos que o compunham. Todas as diligências de tramitação do procedimento constavam do processo, pelo que a avaliação da legalidade dos atos praticados dependia apenas da análise do processo.

A falta de documentação impede o controlo da legalidade e da regularidade do procedimento, dado que os dados que servem de base para a operação dos sistemas informáticos são ininteligíveis para a avaliação da legalidade dos procedimentos. O processo administrativo é composto pelo conjunto dos documentos onde foram praticados os atos e as diligências, devidamente autuados, paginados e rubricados (n.º 2 do art.º 64.º do CPA), contendo todos os termos e autos nele produzidos (n.º 1 do art.º 64.º), de forma a evitar o seu extravio e a garantir a sua preservação. O processo administrativo não são os dados.

A existência de legislação que regule a documentação dos processos administrativos eletrónicos é muito importante num contexto em que o fenómeno da informatização, da desmaterialização e da automatização são crescentes e é expectável que rapidamente a generalidade dos procedimentos administrativos sejam tramitados de forma eletrónica.[1115] Aliás o próprio CPA estabelece no art.º 61.º, o princípio da preferência da tramitação eletrónica do procedimento, pelo que é o próprio legislador que reconhece a primazia dos suportes eletrónicos relativamente ao papel.[1116] É também nesse sentido que se integra o estabelecimento de um corpo de princípios e de conceitos relativos à administração eletrónica no art.º 14.º.

É certo que quando os procedimentos são informatizados e automatizados, no todo ou em parte, as diligências e os atos praticados mediante a mera operacionalidade

---

sistema de segurança social, por exemplo público e privado, esse cálculo pode ser automatizado mediante a comunicação eletrónica de dados entre os diversos órgãos competentes. O controlo da legalidade dos atos do procedimento necessita que todas as operações nele efetuadas sejam documentadas, sem o que o interessado não poderá defender os seus direitos.

[1115] Embora se trate de um conceito eivado de certo voluntarismo, o impacto das tecnologias eletrónicas no procedimento administrativo gerou o conceito de administração pública eletrónica ou e-administração, ou ainda do teleprocedimento. Por todos, Roques-Bonnet: *"Aujourd'hui, l'e-administration peut être definie (…) comme la suppression du support papier (…) comme un processus d'échanges non matérialisés se traduisant en particulier para le développement des "teleprocedures""*. Roques-Bonnet, M.C. (2010); Op. cit, pág. 28 .

[1116] A revisão do Código de Processo nos Tribunais Administrativos (CPTA), de 2015 (DL n.º 214-G/2015, de 2/10, veio, de forma inovadora, introduzir, no artigo 24.º, o princípio da organização eletrónica do processo, tanto no que respeita à documentação dos atos, com à própria tramitação do processo, que em ambos os casos devem ser eletrónicas. Estabelece, assim, o CPTA o princípio da total desmaterialização do processo administrativo. A regulamentação da organização do processo é deixada para portaria a publicar pelo governo.

dos sistemas informatizados podem ser sindicados mediante a auditoria aos registos existentes nos sistemas informáticos respetivos, uma vez que a informação relativa à prática desse tipo de tarefas e atos consta dos respetivos registos informáticos. O problema é o da acessibilidade a esses dados e o da sua dispersão pelas tabelas de suporte ao funcionamento dos respetivos sistemas. Para resolver esse problema, deveria a lei obrigar a que os serviços competentes para a tramitação dos procedimentos adequassem os sistemas informático para que estes gerassem um documento autónomo, em suporte eletrónico sempre que efetuam um ato ou uma diligência do procedimento, no qual constassem todos os correspondentes elementos relevantes.

Do mesmo modo deveria a lei exigir que a documentação do procedimento eletrónico automatizado fosse também publicada, juntamente com a análise funcional do programa informático.

As normas de organização, de conservação e de arquivo desse tipo de processos devem também ser objeto de previsão legal.

Os documentos do processo administrativo devem ser autenticados com elementos de segurança eletrónica, nomeadamente uma assinatura eletrónica ou um selo eletrónico, que garantam a sua autenticidade, integridade e autoria, bem como com os referenciais de tempo e lugar da respetiva prática.[1117]

A geração desses documentos e a sua assinatura eletrónica pelo titular do órgão competente para a tramitação do processo ou para a prática do ato, é também um instrumento fundamental de garantia do controlo humano sobre a qualidade de funcionamento do sistema informáticos e de imputação subjetiva dos atos praticados ao titular da respetiva competência, própria ou delegada. Por outro lado, todos os documentos praticados no âmbito de um procedimento devem ser carreados para o processo, que poderá ser um processo integralmente eletrónico.

1.3. A assinatura eletrónica e os serviços de confiança no procedimento administrativo

[1117] Como refere com pertinência Benjamim Rodrigues, embora relativamente à prova em processo penal, mas com aplicação idêntica ao procedimento e ao processo administrativo, "*Com o princípio da documentação de todas as fases de acesso, recolha, armazenamento, transferência, preservação ou apresentação da prova eletrónica-digital pretende-se traduzir a ideia de que se afigura imprescindível a documentação de todas as etapas, sob pena de se inviabilizar a 'cadeia de controlo'*". Rodrigues, B. S. (2009). Op. cit., pág. 728.

O CPA de 1991 não previa a utilização das tecnologias eletrónicas no procedimento administrativo, dado que a utilização da informática era meramente acessória e instrumental à tramitação do processo assente na documentação em papel.

O CPA de 2015 marca um avanço nesta matéria, contendo várias normas que regulam a utilização daquelas tecnologias no procedimento, tanto no que respeita à sua tramitação como à sua documentação, como ainda às respetivas comunicações.

A generalidade dos procedimentos administrativos tenderá a tornar-se documentada em suporte eletrónico, pelo que se justifica um elevado nível de exigência que garanta a sua autenticidade, integridade e preservação, para o que se torna necessária a generalização da utilização das assinaturas eletrónicas ou dos selos eletrónicos nos documentos eletrónicos nele produzidos ou utilizados.[1118]

O CPA só prevê a utilização da assinatura eletrónica na decisão final do procedimento, no n.º 2 do art.º 94.º. Trata-se de uma formulação que consideramos limitativa, dado que muitos outros documentos eletrónicos utilizados no procedimento justificariam a autenticação com assinatura eletrónica.[1119] É o caso, por exemplo, do requerimento inicial, que as alíneas c) e d) do n.º 1 do art.º 104.º admitem que seja entregue por *"transmissão eletrónica de dados"*, mas sem exigirem qualquer forma de autenticação que garanta segurança no que respeita à integridade do seu teor e à identidade do seu autor, bem como da efetividade da data de entrega.[1120] É certo que o n.º 5 do art.º 104.º do CPA estabelece que o requerimento deve observar o formato definido no sítio institucional da entidade pública, mas a previsão da autenticidade do requerimento é matéria que está para além do formato e deveria constar do próprio CPA.[1121] No mesmo sentido o art.º 105.º obriga os órgãos da administração a fazerem o registo dos requerimentos entregues, especificando no n.º 4, que o registo dos requerimentos entregues por via eletrónica deve ser um registo eletrónico, sem acrescentar outros requisitos. Seria também importante que a lei exigisse que esses

[1118] O Código de Processo Civil já prevê, no artigo que o processo civil é tramitado integralmente em forma eletrónica, estabelecendo o n.º 2 que se devem respeitar os princípios da *"integralidade, autenticidade e inviolabilidade"*. Esta previsão vem já desde ao ano 2008, quando foi aditado o então artigo 138.º-A.

[1119] Nos processos judiciais, a obrigação de utilização da assinatura é mais abrangente, estabelecendo o artigo 19.º da Portaria n.º 280/2013, de 26/8, que os atos processuais dos magistrados judiciais e do Ministério Público são sempre autenticados com assinatura eletrónica, devendo também sê-lo os autos e termos das partes (artigo 23.º).

[1120] As duas alíneas repetem a previsão da entrega mediante transmissão eletrónica, sem que aparentemente exista justificação para essa repetição.

[1121] De forma diversa e conferindo melhores garantias de segurança, a entrega de peças processuais em suporte eletrónico nos processos judiciais é sujeita às garantias da certificação da data e da hora de entrega, mediante certificação (artigo 13.º da Portaria n.º 280/2013, de 26/8.

registos fossem autenticados com selos temporais que garantissem com rigor a data de entrega dos requerimentos, dada a importância que a determinação do momento da entrega dos requerimentos tem para o procedimento e para o exercício dos direitos.[1122]

Os documentos juntos ao processo pelas partes, bem como aqueles que tenham sido recebidos de entidades terceiras, ou que tenham sido juntos pelo próprio órgão competente para o procedimento, deveriam obedecer a requisitos de autenticidade e de integridade. A necessidade de se observarem os requisitos de autenticidade e de integridade está enunciada genericamente no n.º 2 do artigo 14.º do CPA, mas não se estabelecem requisitos mínimos de fiabilidade dos serviços de confiança que devem ser utilizados.

O próprio CPA estabelece, no art.º 64.º, o princípio da integridade do processo administrativo, obrigando, para tal, o órgão responsável a rubricar todas as folhas do processo e permitindo que o próprio interessado também o faça, se assim o entender.

Justificar-se-ia norma idêntica para os casos em que o processo administrativo está documentado em suporte eletrónico, total ou parcialmente, e o próprio CPA assim o admite, dado que remete para diploma próprio o estabelecimento dessa previsão, no n.º 4 do art.º 65.º.

A necessidade de garantia de autenticidade dos documentos é comum a todos os elementos do procedimento e não apenas à decisão final. Por esta razão, a lei deveria obrigar a que todos os documentos do procedimento fossem autenticados com assinatura eletrónica oi selo eletrónico avançados ou qualificados.

A chamada Lei da Modernização Administrativa estabelece também a obrigação de os serviços da administração pública utilizarem meios eletrónicos nas comunicações que estabelecem entre si (art.º 22.º), bem como a obrigação de disponibilizarem aos interessados cópias em versão eletrónica de certidões, atestados e outros atos meramente declarativos (art.º 21.º).[1123] Estabelece também, no n. 2 do art.º 25.º, a obrigatoriedade de, nas comunicações efetuadas por meios eletrónicos, os órgãos da administração pública garantirem a autenticidade, não só dos documentos, como também da identidade dos "emissores". E essa autenticidade só é garantida através da assinatura eletrónica. Podemos considerar que esta obrigatoriedade se estende a todos os

[1122] Esta exigência legal seria importante para a salvaguarda dos direitos dos administrados, dado que, em caso de disputa acerca da data de entrega de petições ou outros documentos, será muito difícil aos administrados demonstrarem que a data da entrega é diferente daquela que alega o órgão competente da administração, dado que essa comprovação só pode ser efetuada pelo sistema informático deste último.
[1123] Referimo-nos ao DL n.º 135/99, de 22/4, com as alterações do DL n.º 73/2014, de 13/05.

tipos de procedimentos, mas teria sido mais adequado, em nosso entendimento, que ela constasse do CPA, dada relevância crescente da utilização dos meios eletrónicos nos procedimentos administrativos.

Além da tipificação dos documentos do procedimento e da autenticação dos que são entregues pelos interessados e dos que são gerados pelo órgão competente para o procedimento, deve exigir também a lei a documentação e a autenticação dos dados recebidos de outros órgãos da administração púbica.[1124]

Os procedimentos administrativos eletrónicos dependem muitas vezes da partilha de dados entre órgãos diferentes das administrações públicas. Esses dados devem ser documentados, devendo juntar-se ao processo administrativo os documentos demonstrativos do conteúdo dos dados recebidos, a data da sua receção, bem como a autenticação, que garanta que foram recebidos da entidade competente.[1125]

Por outro lado é necessário que se garanta a segurança no acesso aos dados de outros serviços da administração pública. Essa segurança adquire-se mediante a exigência de níveis de garantia na identificação eletrónica dessas entidades.

A lei deve exigir também o nível de garantia mínimo para a identificação eletrónica no procedimento administrativo, do próprio interessado no procedimento. A facilidade de acesso aos sítios *web* das administrações públicas e a generalização da utilização dos sítios web pelas administrações públicas têm generalizado a abertura a

[1124] As verificações que são efetuadas consistem em pedidos de dados a outros órgãos da administração pública. Quando esses pedidos são frequentes, e muitas vezes efetuados em massa, a comunicação entre os órgãos respetivos é efetuada de forma automatizada, mediante linha dedicada exclusiva entre ambas as entidades, também designada por *webservice*, em que a uma pergunta de um sistema, com uma configuração programada, outro sistema efetua uma resposta, num formato também previamente programado. Em muitos casos as respostas são impulsos eletrónicos, de sim ou não, que os sistemas analisam e tratam de forma automática. É esse o caso, por exemplo, do procedimento relativo ao pedido de isenção de taxas moderadoras, em que o Ministério da Saúde decida tendo em conta, entre outros fatores, o rendimento dos interessados, cujo limiar é informado pela administração tributária (n.º 2 do artigo 7.º Portaria n.º 311-D/2011, de 27/12, com a redação da Portaria n.º 289-B/2015, de 17/9 e artigo 6.º do DL n.º 113/2011, de 29/11). Este tipo de comunicações revela-se de elevada eficiência, em termos de economia e rapidez, e a sua utilização é uma obrigação legal prevista nos n.ºs 3 e 4 do artigo 22.º, bem como no artigo 13.º-A do DL n.º 135/99, de 22/4. É com esse fim que se prevê a utilização da plataforma de interoperabilidade da Administração Pública, prevista no n.º 6 do artigo 22.º e no n.º 3 do artigo 28.º-A, do mesmo diploma legal. Também nos processos judiciais este tipo de comunicações eletrónicas e automatizadas com órgãos da administração pública existem, obrigando o n.º 2 do artigo 31.º da Portaria da Tramitação Eletrónica dos Processos Judiciais (Portaria n.º 280/2013, de 25/10) a que seja gravado registo dessas comunicações, *"com identificação do respectivo emissor e destinatário, data de transmissão e número de processo a que se refere"*.

[1125] Em Itália o *Codice dell'Amministrazioni Digitale*, de 2005, estabelece, nos artigos 72.º e seguintes o *Sistema Público di Connettività*, que centraliza a comunicação e interação entre todos os serviços da administração pública, estabelecendo os princípios que a regulam e o seu modo de interação. Esse sistema foi regulado pelos DPCM de 26 marzo 2008 e DPCM 1 april 2008. Tossi, E. (2010). *Codice del Diritto Dell'Informatica e Di Internet*. 7.ª Edição, Celt, Casa Editrice La Tribuna. Piacenza., págs. 357, 1339 e 1341, respetivamente.

instauração eletrónica dos procedimentos por iniciativa dos interessados por via eletrónica. E tendo em conta os efeitos jurídicos que advêm do procedimento, é necessário garantir-se um nível elevado de segurança no que respeita à identificação eletrónica e ao acesso às funcionalidades dos sítios web, de entrega de petições e de documentos pelos interessados.

Por ouro lado, com a entrada em vigor do Regulamento EIDAS, o regime da identificação eletrónica permite a autenticação dos interessados no procedimento, mas isso não dispensa em caso algum que, nos casos em que esses interessados procedam ao envio de documentos eletrónicos, os autentiquem com a sua assinatura ou o selo eletrónico, que devem ser avançados ou qualificados. Seria, por essa razão, importante que a lei exigisse não só esse nível mínimo de garantia na identificação eletrónica, mas também que estabelecesse a necessidade de autenticação autónoma de cada um dos documentos entregues por essa via, dado que a identificação eletrónica não dispensa a autenticação e a garantia de integridade dos documentos.[1126]

1.4. A notificação eletrónica

Um domínio onde a utilização das tecnologias eletrónicas tem maior impacto é o das notificações e comunicações efetuadas nos procedimentos administrativos.[1127]

Portugal incluiu desde logo, na lei da assinatura eletrónica de 1999, a previsão da notificação eletrónica no procedimento administrativo. Para isso estabeleceu apenas algumas especificidades, destinadas a garantir a segurança e a certeza do envio e da receção da correspondência eletrónica. Essas especificações são as seguintes:[1128]

i) Haver acordo dos interessados e identificação de um endereço eletrónico para o qual as comunicações se consideram enviadas e recebidas, logo que recebidas pelo destinatário;

[1126] A necessidade de, além da autenticação individual dos interessados, os documentos electrónicos submetidos serem autenticados com a assinatura electrónica qualificada dos administrados, consta, por exemplo, de forma expressa, no artigo 54.º do Decreto-Lei n.º 96/2015, de 17 de agosto.

[1127] A Itália foi o primeiro país a criar legislação acerca da notificação eletrónica, existindo atualmente a "*Posta Electrónica Certificata (PEC)*", um instrumento que regista e autentica as caixas de envios e de receção das partes, certificando também a remessa das comunicações, nos termos previstos no artigo 48.º do *Codice D'ella Administrazioni Digitale.* A autenticação dos endereços eletrónicos, especialmente o da origem, e a utilização da assinatura eletrónica são essenciais. Ruggieri, F. (2008), pag. 38. Este sistema foi criado em 1988, pelo DM 29.5.88 No. 29 e pela Risol. Dir. Gen. Tasse nº 571134/88 de 19.7.88. "TEDIS Report", pág. 158, par. 357.

[1128] Este regime consta do artigo 6.º do DL n.º 290-D/99, de 2/8.

ii) A existência de uma validação cronológica;

iii) A comunicação ser autenticada com assinatura eletrónica qualificada que seja comunicada *"por meio de telecomunicações que assegure a efetiva receção"*, sendo nesse caso equivalente ao envio por carta registada. A lei não especifica que comunicação é esta, nem o que considera receção, dado que o destinatário pode não abrir a mensagem;

iv) Nos casos referidos no ponto anterior, considera-se que a comunicação equivale ao envio por carta registada com aviso de receção, se a receção for comprovada por mensagem de confirmação emitida pelo destinatário e recebida pelo remetente, com assinatura eletrónica qualificada;

v) A lei considera que a data do envio é a data da receção pelo destinatário;

vi) É também previsto que os operadores não podem tomar conhecimento do conteúdo das mensagens.

Este regime de comunicação eletrónica era inovador, mas tinha como limitação o facto a lei exigir a prova da receção das mensagens pelo destinatário. Esta necessidade geral faz sempre depender da vontade destes a sua consumação e, se isso garante uma maior segurança para este, também coloca na sua disponibilidade a realização dos atos subsequentes, quando de trata de notificações que estabelecem prazos fixos para a prática dos atos. Ora essa dependência não existe nas notificações em papel, cuja consumação é, de uma forma ou de outra, confirmada por uma entidade terceira.

Por outro lado a necessidade de validação cronológica e da existência de mecanismos que assegurem a efetiva receção das notificações, eram limitações que só viriam a ser ultrapassadas em 2006, com a incorporação das notificações eletrónicas no Serviço Público Postal Universal.[1129]

Em 2012 ocorreu um importante avanço nesta matéria, com o estabelecimento do regime da notificação eletrónica no procedimento tributário, quando foi inserida nos

[1129] DL n.º 112/2006, de 9/6 e Resolução do Conselho de Ministros n.º 50/2006, de 13/4. Foi disponibilizado aos cidadãos um serviço de entrega e receção de mensagens digitais, nomeadamente notificações e citações de organismos da administração pública e dos tribunais, tendo por principal objetivo garantir a segurança nas comunicações digitais. Nos termos da alínea c) do n.º 2, *"a CPE assegura a segurança, a confidencialidade e a integridade da comunicação e do seu conteúdo".* O envio das comunicações para os utilizadores é efetuado pelos CTT, que as recebem das entidades emissoras, assim evitando o Spam.

art.ºs 38.º, 39.º, 41.º a 43.º e 191.º a 193.º do Código de Procedimento e de Processo Tributário.

O CPA veio prevê-las e regulá-las, pela primeira vez em 2015, mas existem algumas incertezas no regime criado, em nosso entendimento, naturalmente.

O CPA distingue as comunicações das notificações enviadas pela Administração para os interessados no procedimento administrativo.

No que respeita às comunicações, prevê-se a possibilidade do seu envio:

i) Por correio eletrónico, para a caixa postal eletrónica de que o interessado *"é titular, nos termos previstos no serviço público de caixa postal eletrónica"*. (n.º 1 do art.º 63.º). Este meio aplica-se a qualquer interessado no procedimento, desde que tenha prestado por escrito prévio consentimento, na sua primeira intervenção ou posteriormente, indicando a sua caixa postal eletrónica;[1130]

ii) Para plataformas informáticas com acesso restrito ou;

iii) Para os endereços de correio eletrónico indicados em qualquer documento apresentado pelos interessados no procedimento administrativo.

As modalidades de comunicação referidas nos pontos ii) e iii) anteriores aplicam-se, exclusivamente, nas comunicações estabelecidas entre os serviços da administração pública e os interessados no procedimento administrativo, nos casos em que estes últimos sejam pessoas coletivas. Aplica-se, neste caso, a presunção de que estas entidades consentiram na utilização da comunicação eletrónica quando, anteriormente tenham estabelecido contacto regular através daqueles meios com os serviços, mesmo que não tenham consentido expressamente a sua utilização (n.º 2 do art.º 63.º do CPA). A modalidade referida em i) aplica-se a pessoas singulares e coletivas.

Relativamente às notificações efetuadas no procedimento administrativo, a alínea c) do n.º 1 do art.º 112.º do CPA também admite a sua emissão por três modalidades:

i) Por correio eletrónico;

[1130] O n.º 2 do artigo 63.º do CPA estabelece uma presunção de que o interessado consentiu na utilização deste meio de comunicação nos casos em que, apesar de não ter procedido à indicação da sua caixa postal eletrónica, tenha estabelecido contacto regular através dela.

ii) Por notificação eletrónica automaticamente gerada por sistema incorporado em sítio eletrónico pertencente ao serviço do órgão competente, mediante o consentimento expresso e prévio dos interessados;

iii) Por notificação eletrónica automaticamente gerada por sistema incorporado em sítio eletrónico pertencente ao balcão único eletrónico, mediante o consentimento expresso e prévio dos interessados;[1131]

O legislador tem o cuidado de distinguir o modo de emissão das notificações eletrónicas, do local para onde são enviadas ao destinatário. Esses locais de destino das notificações eletrónicas são os seguintes:

i) Para plataformas informáticas com acesso restrito, mediante o consentimento expresso e prévio dos interessados;

ii) Para os endereços de correio eletrónico indicados em qualquer documento apresentado no procedimento administrativo, quando se trate de pessoas coletivas, independentemente do consentimento destas.[1132]

O CPA não identifica o que sejam plataformas informáticas com acesso restrito, mas uma plataforma informática é um sistema informático, ao qual podem aceder várias pessoas e, sendo de acesso restrito, ele efetua-se mediante a utilização de um sistema de identificação e de autenticação eletrónica.

[1131] Esta alínea c) do n.º 1 do artigo 112.º do CPA distingue, aparentemente, a notificação eletrónica da notificação por correio eletrónico. A sua redação é a seguinte: *"Por telefax, telefone, correio eletrónico ou notificação eletrónica automaticamente gerada por sistema incorporado em sítio eletrónico pertencente ao serviço do órgão competente ou ao balcão único eletrónico"*. Prevê-se de forma separada o correio eletrónico e só depois a notificação eletrónica, separando esta em duas modalidades, sendo uma enviada para o sítio eletrónico do serviço competente e a outra para os balcões únicos eletrónicos. Parece-nos, porém, que em ambos os casos se trata de modalidades de notificação eletrónica, dado que de seguida são todas sujeitas ao mesmo regime. Parece-nos, porém, que a inclusão na mesma norrma desta modalidade de notificações juntamente com as que são realizadas por telefax e telefone, poderá relevar a importância limitada que o legislador confere, apesar de ser expectável que a generalização da utilização das novas tecnologias possa conduzir a que elas venham a ser dominantes no futuro próximo.

[1132] Quando os destinatários sejam pessoas coletivas, as notificações são enviadas para os endereços que tenham sido por elas indicados em qualquer documento apresentado no procedimento (alínea a) do n.º 2 do artigo 112.º), dado que se presume que essa indicação corresponde a um consentimento. Quando se trate de pessoas singulares, o envio eletrónico só ocorre, em qualquer caso, mediante consentimento escrito prévio, sendo que esse consentimento só opera desde que o interessado tenha indicado a sua caixa postal eletrónica, na primeira intervenção no procedimento ou posteriormente, com o exige o n.º 1 do artigo 63.º do CPA. Assim, em face desta norma, as notificações por via eletrónica só se podem realizar, para as pessoas singulares, para a sua caixa postal eletrónica e não para a sua caixa de correio eletrónico nem para plataformas informáticas com acesso restrito. Do mesmo modo, no caso em que as pessoas coletivas não tenham indicado em qualquer documento o seu endereço eletrónico, a notificação eletrónica segue o mesmo regime aplicável as pessoas singulares.

Como a lei não distingue, essas plataformas informáticas poderão ser, em primeiro lugar, os sítios *web* dos próprios serviços da administração pública responsáveis pelo procedimento administrativo no âmbito do qual são efetuadas as notificações, desde que esses sítios possuam um sistema de restrição de acessos ou utilizem um sistema de identificação e de autenticação da identidade dos utilizadores. Podem ser também plataformas específicas de notificação eletrónica, como é o caso do da caixa postal eletrónica, que atualmente é gerida pelo sistema Via CTT.[1133]

O regime da perfeição das notificações eletrónicas é estabelecido nos n.ºs 5 e 6 do art.º 113.º do CPA. Considera-se que as notificações se consumam nos momentos seguintes:

i) No caso de correio eletrónico, no momento em que o destinatário aceda ao específico correio enviado para a sua caixa postal eletrónica;

ii) No caso de outras notificações por transmissão eletrónica de dados, no momento em que o destinatário aceda ao específico correio enviado para a sua conta eletrónica aberta junto da plataforma informática disponibilizada pelo sítio eletrónico institucional do órgão competente;

iii) No 25.º dia posterior ao seu envio, nos casos e que o destinatário não tenha acedido à caixa postal eletrónica ou à conta eletrónica aberta junto da plataforma informática disponibilizada pelo sítio eletrónico institucional do órgão competente. Esta presunção não ocorre nos casos em que "*se comprove que o notificando comunicou a alteração daquela, se demonstre ter sido impossível essa comunicação ou que o serviço de comunicações eletrónicas tenha impedido a correta receção, designadamente através de um sistema de filtragem não imputável ao interessado*".

Da análise da definição do momento da perfeição das notificações resulta que o CPA só permite dois tipos de notificações eletrónicas, sendo o primeiro mediante o envio para a caixa postal eletrónica e o segundo a disponibilização no sítio web do próprio órgão responsável pelo procedimento.

[1133] O Via CTT é um sistema de Caixa postal Eletrónica, que está disponível no sítio web https://www.viactt.pt/website/index.html. Cada aderente cria nesse sistema uma conta, após a sua identificação perante a entidade gestora, que neste caso são os CTT, que emite um código de autenticação que essa pessoa deve utilizar de cada vez que pretenda aceder à sua conta. Nessa conta, também designada de caixa postal eletrónica, pode verificar as comunicações eletrónicas, incluindo as notificações eletrónicas que lhe foram dirigidas.

É certo que se prevê o envio por correio eletrónico e esse se poderia entender como o normal envio por *e-mail*, mas a lei só prevê que a notificação se consuma quando é utilizada a caixa postal eletrónica. E este é um conceito específico, sujeito a um regime jurídico específico.

Este regime levanta-nos, porém, quatro questões que consideramos relevantes, que são as seguintes:

A primeira é que o CPA permite, na alínea a) do n.º 2 do art.º 112.º, que, quando se trate de pessoas coletivas, a notificação seja enviada para os endereços de correio eletrónico indicados em qualquer documento por elas apresentado no procedimento administrativo. E essa modalidade de notificação não necessita de consentimento dos destinatários, podendo ser de iniciativa oficiosa do órgão competente do procedimento, desde que esse endereço tenha sido identificado no procedimento. Tratar-se-ia, aparentemente, de qualquer caixa de correio eletrónico, vulgarmente conhecidas por endereço de *e-mail*. Mas isso não pode ser assim, dado que quando no art.º 113.º se regula o regime de perfeição das notificações, nada se diz acerca deste meio. E se assim é, não prevê a lei quando se considera consumada a notificação efetuada por essa via.

Só se prevê o envio para a caixa postal eletrónica, para além da disponibilização na conta eletrónica aberta junto da plataforma informática disponibilizada pelo sítio eletrónico institucional do órgão competente. Só que a caixa postal eletrónica não é um endereço eletrónico que possa ser utilizado por qualquer entidade para enviar comunicações para os serviços da administração pública.

A Caixa Postal Eletrónica (CPE) é um meio de comunicação unidirecional, dos órgãos da administração pública para os interessados, que não funciona em sentido inverso. A Resolução do Conselho de Ministros n.º 50/2006, que criou o Serviço Universal de Caixa Postal Eletrónica, estabelece que se trata apenas de uma caixa de receção de mensagens eletrónicas, que está associada a um endereço físico, para a qual são enviadas comunicações de várias entidades, incluindo os serviços da administração pública. A CPE faz parte da concessão do serviço postal universal, nos termos da alínea d) do n.º 1 da Base II, tendo sido aditada pelo Decreto -Lei n.º 112/2006, de 9 de junho, na sequência da Resolução do Conselho de Ministros que anteriormente citámos. Nos termos daquela norma, o serviço público de CPE *"permite aos aderentes a este serviço receber, por via eletrónica ou por via eletrónica e física, comunicações escritas ou outras provenientes dos serviços e organismos da administração direta, indireta ou*

autónoma do Estado", bem como de outras entidades. Não permite a comunicação eletrónica dos particulares para aquelas entidades. Trata-se, portanto, apenas de um serviço de receção de mensagens eletrónicas.[1134]

De qualquer forma a lei não nos parece clara, podendo essa falta de clareza resultar da identidade entre o conceito de correio eletrónico e o de utilização da caixa postal eletrónica, bem como de uma certa falta de conformidade entre o CPA e o regime da caixa postal eletrónica.

Aparentemente, o CPA só admite o envio de notificações eletrónicas através daquilo a que chama o correio eletrónico, quando se trate da caixa postal eletrónica, e essa parece-nos ser uma opção acertada. Esse envio é efetuado por uma entidade terceira que assim pode certificar a data da disponibilização das notificações aos interessados, bem como a data em que estes especificamente acederam ao correio específico de onde consta a notificação.

A eventual possibilidade de serem feitas notificações para as comuns caixas de correio eletrónico, também conhecidas por *e-mail*, seria sempre um fator de insegurança, dado que não seria possível determinar, com rigor e isenção, a data de receção das notificações pelos interessados, a não ser que se colocasse na disponibilidade destes a conformação dessa data, dado que estaria sempre na sua disponibilidade a demonstração da receção. Embora alguns sistemas de *e-mail* disponham de serviços de informação de retorno acerca da abertura do correio pelos destinatários, outros existem que não possuem esse serviço, e mesmo aqueles que o possuem, permitem ao destinatário desativá-lo, pelo que ficaria sempre na disponibilidade destes a determinação da perfeição da notificação.[1135]

Por outro lado a utilização dos comuns sistemas de *e-mail* para o envio de notificações eletrónicas poderia também ser um fator de insegurança, pelo facto de essas caixas poderem receber correio eletrónico das mais várias proveniências e serem, por isso, vulneráveis a situações de ataques mediante o envio para elas de elevadas quantidades de comunicações, também designadas por *phishing*, podendo isso conduzir

[1134] Este serviço continua a integrar concessão do serviço postal universal, nos termos do DL n.º 160/2013 de 19/11. Deste modo, a norma do n.º 2 do artigo 63.º do CPA não se aplica às comunicações por via eletrónica.

[1135] A garantia da certificação da data de receção da notificação é essencial para a segurança jurídica e é um exemplo da importância da certificação eletrónica no procedimento administrativo. Como refere Nadal, *"Outro ejemplo son las notificaciones que envia la Administración, para las que hay que garantizar que el destinatário emitirá um acuse de recibo una vez que se ponga el mensage a su disposición"*. Nadal, A.G. (2009). Op. cit., pag. 55.

a que o destinatário não consiga descortinar a receção de notificações com relevância jurídica efetiva.

A caixa postal eletrónica, tal como está concebida na lei portuguesa, é administrada apenas por uma entidade com competência na área da distribuição postal, estando, assim, protegida contra as práticas de *phishing*.

Terão sido estas, uma parte das razões que conduziram o legislador do CPA a não admitir a realização de notificações através dos comuns sistemas de correio eletrónico. De qualquer forma teria sido desejável uma maior precisão conceptual da lei.

A segunda questão que se nos afigura relevante é a da falta de exigência do CPA, no que respeita à autenticação das notificações eletrónicas. A notificação deve ser efetuada com todas as garantias de segurança quanto à identidade do órgão e do respetivo titular que efetuam a notificação.[1136] E essa segurança só é possível de alcançar mediante a utilização da assinatura eletrónica do titular do órgão, ou então mediante o selo eletrónico do órgão notificante. Só que o CPA não exige nem a assinatura eletrónica nem a utilização do selo eletrónico. A utilização da assinatura eletrónica só está prevista para o documento de suporte ao ato administrativo praticado no procedimento e não está sequer prevista para as notificações. Ora, um dos instrumentos de segurança jurídica no procedimento é a certeza, do destinatário, acerca da autenticidade da origem e da legitimidade de quem o está a notificar. O CPA só exige a utilização da assinatura eletrónica ao longo de todo o procedimento, no documento que suporta a prática do ato de decisão final do procedimento, no n.º 2 do art.º 94.º. Trata-se, porém, de uma exigência minimalista e insuficiente, dado que também as notificações deveriam ser autenticadas com assinatura eletrónica ou instrumento que garanta a identidade do autor e a autenticidade de toda a informação dele constante.

É nesse sentido que o art.º 5.º do Decreto-Lei n.º 290-D/99, de 2/8, exige que os documentos eletrónicos emitidos pelos órgãos da administração pública sejam autenticados com a assinatura eletrónica qualificada dos respetivos autores, acrescentando o n.º 2 que se incluem as comunicações dos atos administrativos na obrigação de identificação da entidade e do titular do órgão competente que praticou o ato, bem como a comprovação da respetiva função. Essas exigências legais são

[1136] Como refere Malsipica, *"Las notificaciónes telemáticas en su vertente administrativa (...) deberian también firmarse de manersa telemática"*. Malsipica, S.G. (2004). *Notificaciones Telemáticas. Em: Ministerio de Economia. Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid., página 514.

garantidas mediante a assinatura eletrónica pelo que, apesar de não estarem previstas no CPA, e do nosso ponto de vista deveriam estar, devem ser respeitadas, em face das normas que acabamos de citar.

A terceira questão que se nos coloca relativamente ao regime das notificações eletrónicas do CPA é a da segurança no que respeita à data da sua realização. A data da perfeição das notificações possui um valor jurídico relevante, já que pode determinar a constituição de direitos e a conformação dos prazos para a prática de atos, o cumprimento de obrigações ou a execução dos atos.[1137]

A determinação da data e do momento da perfeição das notificações não deve estar na disponibilidade das partes e deve estar o mais possível ao abrigo de controvérsias. No paradigma do papel essa data é determinada por uma entidade terceira, que é o serviço de distribuição postal, estabelecendo a lei um conjunto de requisitos formais dessa determinação, de exigência variável quando determina a sua realização mediante carta registada com aviso de receção ou meramente registada. Em ambos os casos o papel da entidade que procede à distribuição postal, como entidade terceira que é, não interessada no procedimento, é essencial para a determinação da data da perfeição da notificação.

Ora esse papel das entidades terceiras parece ter sido esquecido pelo legislador do CPA no regime das notificações eletrónicas. E foi-o, em nosso entendimento, nos dois tipos de notificações eletrónicas previstos na lei:

i) Nas notificações efetuadas através da caixa postal eletrónica, não estabelece a lei qual a forma como se determina se o destinatário o tempo e o modo em que o destinatário acedeu *"ao específico correio enviado para a sua caixa postal eletrónica"* (n.º 5 do art.º 113.º do CPA). A quem cabe determinar se ocorreu esse acesso? Como se comprova se ele ocorreu ou não? O CPA não nos oferece resposta. E em que consiste esse acesso? Consiste na própria abertura do documento em forma que permita a sua leitura, ou poderá entender-se também que acedeu a ele quando abriu a caixa de correio e verificou a

[1137] A segurança quanto à data da perfeição das notificações eletrónicas é importante, dado que dessa data dependem vários prazos nos procedimentos, para o exercício de direito e para o cumprimento das obrigações das partes. Essa importância é reforçada pelo facto de a tramitação dos procedimentos ser cada vez mais desmaterializada e automatizada, procedendo os sistemas informáticos das administrações públicas à contagem desses prazos e ao avanço da tramitação dos procedimentos. Por essa razão, a lei deveria possuir um nível de exigência mais elevado. As tecnologias eletrónicas proporcionam uma maior eficiência e eficácia aos serviços da administração pública na sua atividade, mas ao mesmo tempo deve a lei exigir também mais elevados índices de exigência e de rigor na salvaguarda dos direitos dos cidadãos.

lista de comunicações recebidas, sem ter procedido à sua abertura para leitura? Aparentemente a lei exige que tenha sido aberto para leitura o específico documento de onde consta a notificação, mas poderia a formulação ser mais clara. De qualquer forma não está claro na lei, que compete à entidade gestora da caixa postal eletrónica a produção de um documento eletrónico comprovativo, que certifique esse acesso e o momento em que ocorreu a fim de esse documento, devidamente autenticado com a assinatura eletrónica daquela entidade, ser junto ao processo administrativo. Do mesmo modo devia regular a lei como se documenta a falta de acesso do destinatário ao correio enviado, a fim de determinar o início da contagem do prazo de 25 dias que a lei consagra como necessário à perfeição da notificação, no n.º 6 do art.º 113.º do CPA;

ii) Nas notificações efetuadas mediante envio para *"a conta eletrónica aberta junto da plataforma informática disponibilizada pelo sítio eletrónico institucional do órgão competente"* (segunda parte do n.º 5 do art.º 113.º). Embora a lei não especifique o que entende por estas plataformas informáticas, parece estar em causa a disponibilização, pelos órgãos da administração competentes para o procedimento, no seu sítio institucional, de um espaço individual para os cidadãos, de acesso restrito, onde fossem disponibilizadas as notificações em suporte eletrónico. Mediante acesso a esses sítios e inserção da sua autenticação, os interessados poderiam consultar essas notificações. Esta modalidade de notificação eletrónica levanta-nos as seguintes questões:

   a. Coloca na exclusiva disponibilidade do órgão competente para o procedimento a determinação da data e do momento da perfeição da notificação, o que, em caso de litígio, deixa o administrado sem modo de poder apresentar prova e contrário;

   b. Obriga os administrados a terem o ónus de consultar repetidamente os sítios institucionais dos órgãos competentes para o procedimento, a fim de verificarem se por eles foi disponibilizada alguma notificação. Essa obrigação pode tornar-se onerosa, em face do tempo de duração dos procedimentos e também da possibilidade

que sempre existirá de um mesmo administrado possuir vários procedimentos em curso em vários órgãos da administração, o que obrigaria o mesmo cidadão a ter que percorrer todos os sítios institucionais desses órgãos à procura de notificações que lhe tenham sido disponibilizadas;

c. Não se estabelece no CPA qualquer regime de segurança no que respeita à determinação da data e da hora em que o órgão da administração competente para o procedimento depositou na conta eletrónica do interessado o documento com a notificação eletrónica. Ora essa determinação é essencial para a perfeição da notificação, dado que a lei estabelece que, decorridos que sejam 25 dias, se considera consumada a notificação. O CPA não só não exige a intervenção de terceiros, como não exige qualquer prova ao órgão competente, da disponibilização da notificação, nem sequer um registo desse facto.

A quarta questão é a do sistema automático incorporado em que consiste a emissão de *"notificação eletrónica automaticamente gerada por sistema incorporado em sítio eletrónico pertencente ao serviço do órgão competente ou ao balcão único eletrónico*", prevista na alínea c) do n.º 1 do art.º 112.º do CPA. É que as notificações não são geradas pelos sítios *web*, comummente conhecidos por *sites*. Nesses sítios podem ser disponibilizadas, mas a sua geração é produzida pelos sistemas operativos internos dos serviços competentes para o procedimento. São esses sistemas internos que servem de suporte aos sítios eletrónicos, sendo estes apenas instâncias eletrónicas de disponibilização do produto do funcionamento desses sistemas internos.

As notificações eletrónicas são geradas pela operação normal dos sistemas informáticos internos destas entidades, sendo que nos sítios institucionais dos serviços são apenas disponibilizados para consulta externa pelos interessados. Por essa razão, não será o mais adequado afirmar-se que os sistemas que expedem a notificação eletrónica estão incorporados nesses sítios web.

Colocadas as questões que nos parecem merecer aperfeiçoamento no regime das notificações eletrónicas, cabe agora ponderarmos eventuais vias de solução. Parece-nos que a lei deveria, no que respeita às notificações efetuadas por via eletrónica, seguir um regime idêntico ao das notificações em papel, em que existe sempre uma entidade terceira que certifica, tanto o registo do envio da correspondência, como, nos casos em

que a lei o estabelece, a data de entrega ao destinatário. Esse nível de exigência recomendaria que também as notificações eletrónicas fossem feitas mediante a intervenção de uma entidade terceira. Essa entidade poderia ter duas modalidades:

i) Numa opção mais desejável, ela receberia, como nas notificações por via postal, o documento com a notificação, do órgão competente para o procedimento, e procederia à sua entrega ao destinatário. E tanto a receção como a entrega deveriam ser documentadas mediante um documento eletrónico autenticado, que deveria ficar guardado no processo administrativo. Do mesmo modo a abertura do específico correio com a notificação pelo destinatário, deverá ser documentada. Todos os acontecimentos ocorridos no processo de notificação deveriam ser certificados com selo temporal que garantisse a data da sua ocorrência;

ii) O segundo modelo poderia ser o da notificação mediante "*conta eletrónica aberta junto da plataforma informática disponibilizada pelo sítio eletrónico institucional do órgão competente"*. Do nosso ponto de vista, esta modalidade de notificação não deveria ser admitida, pelo facto de colocar todo o procedimento de notificação na disponibilidade do órgão competente para a sua tramitação, deixando os administrados numa situação de clara dependência e sem possibilidade de defesa. Essa modalidade de notificação não existe no paradigma do papel, provavelmente pelas escassas garantias de transparência que proporciona, e não deverá ser admissível no contexto eletrónico. Porém, a existir, parece-nos que a lei deveria exigir que os acontecimentos relevantes que ocorreram no procedimento de notificação fossem documentados por um selo temporal, emitido por uma entidade independente que certificasse a data e a hora da ocorrência desses factos. Por exemplo, a data da disponibilização da notificação nessa conta e a data em que o destinatário a ela acedeu.

Pensamos ainda que seria desejável que o CPA regulasse com maior minúcia o regime das notificações eletrónicas, dada a relevância e a frequência que podem vir a ter no futuro próximo, uma vez que a sua eficiência e rapidez, bem como a generalização da utilização das tecnologias eletrónicas, conduziram a que essa passe rapidamente a ser a modalidade de notificações mais frequente nos procedimentos administrativos.

Provavelmente foi a pensar nestas questões de maior pormenor que o legislador deixou para diploma específico o regime jurídico do procedimento administrativo em suporte eletrónico previsto no n.º 4 do art.º 64.º do CPA. Talvez seja essa a instância adequada para a resolução destas e de outras questões que a utilização dos suportes eletrónicos coloca no procedimento administrativo.

2. Os arquivos de documentos eletrónicos

A generalização da utilização das tecnologias eletrónicas está progressivamente a substituir a documentação das operações comerciais, administrativas e contratuais, do suporte em papel para o suporte eletrónico. A preservação dos documentos no tempo é um fator essencial à exigência pela lei de documento escrito. Em sede administrativa, a preservação dos documentos e dos processos administrativos é fundamental para um controlo eficaz da atividade dos órgãos administrativos e para a defesa dos direitos dos cidadãos.

Relevam particularmente, nesta matéria, as questões relativas à integridade dos documentos e à sua autenticidade, bem como as questões relativas à sua disponibilidade e acessibilidade.

Não existe legislação específica que salvaguarde esses requisitos dos arquivos dos documentos eletrónicos, e seria desejável que existisse, como forma de preservar a informação que deles consta, bem como o formato e o conteúdo que serviram de base à tramitação dos procedimentos administrativos.

Os problemas que se levantam relativamente ao arquivo dos documentos eletrónicos não são os mesmos dos que se relacionam com os documentos em papel. A leitura dos documentos eletrónicos depende sempre de um procedimento tecnológico de conversão que é necessário garantir que funciona sempre, sob pena de não serem legíveis. A legibilidade dos documentos e a sua acessibilidade devem ser asseguradas pelos responsáveis pelo seu arquivo, que no caso das entidades administrativas devem ser os órgãos competentes onde foi tramitado o procedimento, porque são eles os seus depositários, bem como os beneficiários da utilização das tecnologias eletrónicas.[1138]

[1138] A problemática jurídica dos arquivos eletrónicos respeita não só ao seu conteúdo e formato, mas também à manutenção da tecnologia necessária à sua disponibilidade. Como refere Bazin, atualmente podemos consultar documentos em papel com centenas de anos, mas não existe segurança de que possamos fazer o mesmo com os documentos eletrónicos, dada a volatilidade dos equipamentos e dos

A autenticidade e a integridade dos documentos arquivados devem, também, ser asseguradas. Uma das formas de garantir esses dois requisitos poderia ser mediante a obrigação de o titular do procedimento assinar todos os documentos ou de o serviço responsável aplicar sobre todo o processo um selo eletrónico que garantisse a integridade do processo naquele momento, que perduraria para o futuro.[1139]

Além do regime jurídico do arquivo dos documentos eletrónicos, deveria ser estabelecido por lei um regime jurídico do arquivo dos dados eletrónicos detidos pelos serviços das administrações públicas. Nos suportes eletrónicos os dados são anteriores aos documentos e constituem o seu suporte, mas só podem ser tratados se forem armazenados em determinados formatos. Para além dos fins a que destinam, esses dados podem possuir virtualidades suscetíveis de produzirem conhecimento e valor acrescentado noutros domínios, nomeadamente na investigação científica.

No domínio das relações comerciais, as empresas são obrigadas, nomeadamente pela lei fiscal e comercial, a guardar os documentos de suporte à sua contabilidade durante um período temporal relevante, pelo que também, relativamente a elas, a existência de um regime jurídico dos arquivos eletrónicos poderia ser vantajosa, nomeadamente no que respeita à dispensa dos arquivos em papel.

O CPA estabelece, no art.º 17.º, o princípio da administração aberta e o direito de os interessados acederem aos documentos em poder da administração que lhes digam respeito, mesmo que fora de um procedimento administrativo. Não estabelece, porém, qualquer norma relativa aos deveres dos respetivos órgãos na formação e na manutenção e gestão desses arquivos.

A lei obriga os serviços da administração pública a manter em arquivo os documentos durante os prazos de conservação administrativa, correspondentes aos

---

sistemas informáticos necessários para a sua leitura. *"The true problema regarding digital evidence is the question of the integrity of conservation over time. Today, we can read paper documents that are several hundred years old. But it is debatable whether we will be able to read digital files produced by computer systems which have long disappeared"*. Bazin, Philippe; *op. cit*, pag. 182.

[1139] Em matéria de arquivo eletrónico é relevante a Diretiva 2003/58/CE, de 15/7 2003 do Parlamento Europeu e do Conselho, que estabeleceu a obrigatoriedade de os estados criarem arquivos eletrónicos até 2007, para os documentos das sociedades que são de publicidade obrigatória. A Alemanha criou o seu arquivo eletrónico para este tipo de documentos em 2000. Antes de arquivados os documentos são autenticados mediante intervenção notarial e os responsáveis pelo registo eletrónico procedem à sua verificação antes da sua aceitação. Gassen, D. (2008). Introducing and Working With Electronic Signatures in Mass Applications: Notaries And The German Commercial Register. *Digital Evidence and Electronic Signature Law Review*. Vol 5, pag. 68.

períodos em que eles são necessários, de forma permanente ou ocasional, à sua atividade, passando essa obrigação a ser dos arquivos distritais após essa fase.[1140]

A lei estabelece também a obrigação de os serviços competentes para a tramitação dos procedimentos, procederem à *"implantação de sistemas de gestão de documentos"*.[1141]

Este conjunto de obrigações de conservação aplica-se também aos documentos eletrónicos, dada a abrangência do conceito de arquivo que contido no diploma legal que vimos citando, considerando como tal os documentos, em qualquer suporte, reunidos por uma determinada entidade no exercício da sua atividade, e que sejam conservados tendo em vista, entre outros, objetivos de prova.[1142]

Do mesmo modo, a Lei de Acesso aos Documentos Administrativos inclui no conceito de documento administrativo os documentos em suporte eletrónico, considerando como tal qualquer suporte de informação.[1143]

Falta, porém, um regime jurídico do arquivo dos documentos eletrónicos que estabeleça as obrigações dos órgãos competentes da administração pública no que respeita à preservação da sua autenticidade, integridade e particularmente à garantia da sua disponibilidade futura, sendo que essa disponibilidade envolve a garantia da disponibilidade dos suportes dos dados, dos equipamentos informáticos e dos sistemas que permitam o respetivo acesso. A falta de um regime jurídico de arquivo dos documentos eletrónicos das administrações públicas é um fator de insegurança que necessita de ser eliminado.

A importância dos arquivos eletrónicos e da preservação dos efeitos das assinaturas e dos selos eletrónicos, em termos gerais, é reconhecida pelo Regulamento EIDAS, que autonomiza esse como um serviço de confiança, no artigo 34.º. Trata-se do serviço destinado a garantir o prolongamento do efeito das assinaturas e dos selos

---

[1140] Artigo 4.º do DL n.º 16/93, de 23/1 e artigo 5.º do DL n.º 149/83, de 5/4.

[1141] Artigo 14.º do DL n.º 16/93, de 23/1.

[1142] A definição de arquivo consta do n.º 2 do artigo 80.º da Lei n.º 107/2001, de 8/9, que tem a seguinte redação: *"Entende-se por arquivo o conjunto orgânico de documentos, independentemente da sua data, forma e suporte material, produzidos ou recebidos por uma pessoa jurídica, singular ou colectiva, ou por um organismo público ou privado, no exercício da sua actividade e conservados a título de prova ou informação"*. Por sua vez o n.º 1 do artigo 4.º do DL n.º 16/93, de 23/1, define arquivo do seguinte modo: "*Arquivo é um conjunto de documentos, qualquer que seja a sua data ou suporte material, reunidos no exercício da sua actividade por uma entidade, pública ou privada, e conservados, respeitando a organização original, tendo em vista objectivos de gestão administrativa, de prova ou de informação, ao serviço das entidades que os detém, dos investigadores e dos cidadãos em geral"*.

[1143] A alínea a) do n.º 1 do artigo 3.º da Lei n.º 46/2007, de 24/8, define documento administrativo como *"qualquer suporte de informação sob forma escrita, visual, sonora, eletrónica ou outra forma material, na posse dos órgãos e entidades referidos no artigo seguinte, ou detidos em seu nome"*.

eletrónicos para além da sua validade tecnológica, mantendo assim a possibilidade de se manterem as condições para verificação da autenticidade e da integridade dos documentos que constituem o processo administrativo eletrónico. Este serviço deve ser prestado por prestadores qualificados sempre que se trate de assinaturas ou selos eletrónicos qualificados.

Outro serviço eletrónico relevante para os arquivos eletrónicos é o serviço de verificação das assinaturas ou dos selos eletrónicos, previsto nos artigos 32.º e 40.º do Regulamento EIDAS, mediante o qual os prestadores de serviços de confiança efetuam a verificação de uma assinatura ou de um selo eletrónico e certifica aa sua validade. Essas certificações poderão acompanhar os documentos eletrónicos para além do período útil de validade da tecnologia das respetivas assinaturas ou selos eletrónicos.

Desta forma, existem condições tecnológicas, faltando, porém, um regime jurídico do arquivo dos documentos eletrónicos.

3. A interoperabilidade funcional

A emergência dos documentos eletrónicos veio criar dois tipos de suporte de dados com relevância jurídica, onde anteriormente só existia o papel como instrumento de perdurabilidade da vontade e do conhecimento jurídico expressos. Ambos os suportes possuem regimes próprios de autenticação e de segurança jurídica. Esses regimes são próximos, sendo que o princípio da equivalência funcional permitiu que a construção do regime da assinatura eletrónica utilizasse conceitos e metodologias jurídicas que são tributárias da cultura jurídica da segurança dos documentos em papel.

Um dos problemas desta dualidade de suportes é o da sua interoperabilidade e da comunicabilidade da autenticação dos documentos quando são transpostos de um suporte para o outro. Quando se transpõe um documento eletrónico para um documento em suporte de papel, essa transposição não é acompanhada nas garantias de autenticidade e integridade que a assinatura eletrónica lhe conferia. A eficácia da assinatura eletrónica não se transmite, sem mais, aos documentos em papel que resultaram da impressão de um documento eletrónico.

Do mesmo modo, em situação inversa, a autenticidade de um documento em papel perde-se quando é digitalizado e transposto, mediante cópia, para um suporte eletrónico.

Os instrumentos de autenticação dos documentos em papel servem apenas para esse suporte, do mesmo modo que os de autenticação dos documentos eletrónicos servem só para o respetivo suporte. Não existe comunicabilidade da autenticação, de um suporte para o outro.

Daqui resulta que a emergência dos documentos em suporte eletrónico não veio trazer só a necessidade de existir um regime jurídico que lhe confira validade jurídica, mas também a necessidade de se prever a validade jurídica dos documentos que são originariamente elaborados num suporte e depois convertidos para o outro.

A LMCE contempla a possibilidade de existirem processos negociais em que são utilizados vários suportes nas mensagens trocadas, incluindo o papel e o eletrónico, e mesmo dentro do eletrónico podem ter sido trocadas mensagens EDI e outro tipo de mensagens eletrónicas.[1144] Um documento em papel passa a ser um documento eletrónico quando digitalizado, do mesmo modo que o inverso também é verdadeiro, mas a autenticação não se transmite, pelo que os regimes de autenticação e de segurança são paralelos.

Uma das primeiras normas reguladoras da interoperabilidade funcional foi o art.º 17.º, n.º 5 da LMCE[1145], que prevê a possibilidade de os documentos de transporte internacional de mercadorias, que são ao mesmo tempo títulos de propriedade, possam mudar de suporte, de papel para suporte eletrónico e vice-versa, e estabelece o respetivo regime. As partes podem passar da utilização de mensagens eletrónicas para o uso de documentos em papel, mas é pressuposto essencial da validade dessa transposição que a partir daí não se utilizem mais documentos eletrónicos e se passe a utilizar apenas o suporte de papel. É ainda estabelecido que o novo documento resultante da transposição contenha uma menção ao facto de esta ter sido efetuada. A LMCE estabelece ainda que esta transposição, que na verdade é uma substituição, não afeta quaisquer direitos e obrigações das partes.

Alguns anos mais tarde o n.º C-1.1.º da lei reguladora do quadro jurídico das tecnologias da informação do Estado do Quebéque, no Canadá, estabeleceu, no ponto 17.º, que os documentos que estejam num suporte (a lei utiliza o conceito de numa tecnologia) podem ser transpostos para outro suporte livremente pelas partes,

---

[1144] *"There may exist situations where digitalized information initially dispatched in the form of a standardized EDI message might, at some point in the communication chain between the sender and the recipient, be forwarded in the form of a computer-generated telex or in the form of a telecopy of a computer print-out. Such situations are intended to be covered by the Model Law"*. "A/CN.9/WG.IV/WP.64", par. 31.

[1145] "Guide to Enactment LMCE (1996)", pág. 13.

independentemente da tecnologia que seja utilizada pelas partes, mas com a condição de que se devem cumprir um conjunto de requisitos:

i) Que o processo de conversão fique documentado;

ii) Que essa documentação demonstre que todo o conteúdo foi transposto nos mesmos termos;

iii) Que se demonstre que foi respeitada a integridade do documento transposto;

iv) Que esteja assegurada a integridade do documento que resultou da transposição;

v) Que da documentação da transposição conste a informação seguinte:

   a. Acerca do formato do documento de origem;

   b. Acerca do procedimento de transposição utilizado;

   c. Acerca das garantias que esse procedimento proporciona, nomeadamente quanto à integridade da informação transposta.

vi) Que a documentação anteriormente referida fique guardada durante todo o tempo em que existir o documento resultante da transposição.

A mesma lei estabelece ainda que sendo destruído o documento original após a sua transposição para outro suporte, não poder ser invocado, para efeitos probatórios, que o documento não se encontra na forma original.[1146] Estabelece também o ónus, para a entidade em cuja disponibilidade se encontra o documento, de manter a sua integridade e a sua legibilidade.[1147]

Em 2009, nas chamadas Regras de Roterdão, aplicáveis ao transporte internacional de mercadorias por via marítima, foi introduzida uma norma que prevê a transposição dos documentos de transporte de um suporte para o outro.[1148] Essa transposição depende de acordo entre as partes (o possuidor das mercadorias e o transportador), estabelecendo-se como condição que o documento que foi substituído, no caso de ser em suporte de papel seja entregue pelo seu possuidor ao transportador,

---

[1146] *"Lorsque le document source est détruit, aucune règle de preuve ne peut être invoquée contre l'admissibilité d'un document résultant d'un transfert effectué et documenté conformément à l'article 17 et auquel est jointe la documentation qui y est prévue, pour le seul motif que le document n'est pas dans sa forme originale."*. § 1.º da "Loi Concernant le Cadre Juridique des Technologies de L'information", http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_1_1/C1_1.html (última consulta efetuada em 2016/01/06).

[1147] *Idem*, § 2.º.

[1148] "United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea"; United Nations Commission on International Trade Law; United Nations, Vienna, 2009, pág. 11.

incluindo todas as cópias, ficando cancelados os seus efeitos jurídicos, incluindo a sua validade.[1149]

Nos EUA o *Uniform Commercial Code* contém normas idênticas, destinadas a garantir a segurança na transição entre os documentos em suporte papel e eletrónico, e vice-versa.[1150] Acrescenta, porém, esta norma, que o responsável pela transposição do documento em papel para o suporte eletrónico deve garantir a todos os possíveis intervenientes na cadeia de transações mediante aquele documento, que possuía em seu poder todos os documentos em papel antecedentes, para dessa forma garantir que não existem em paralelo títulos representativos da titularidade das mercadorias, em suporte eletrónico e de papel. A lei estabelece o mesmo regime para os casos em que a transição ocorre dos documentos em papel para o suporte eletrónico.

Em Itália o *Codice D'ella Administrazioni Digitale* prevê que os documentos em papel (analógico) possam ser convertidos em documentos eletrónicos mediante a sua digitalização, mas para garantir a sua fiabilidade exige-se a intervenção de notário ou entidade dotado de fé pública, nos casos em que se trate de documentos originais[1151].

Quando se trata da transposição de um documento em papel para o suporte eletrónico, a qualificação de original desse documento não se deve limitar a depender da garantia de conservação e de integridade desde o momento em que foi digitalizado. Se esse documento foi criado em papel e é considerado um original autenticado, a sua versão eletrónica deve garantir esses atributos de integridade não apenas desde a data da sua digitalização, mas também desde a data da sua criação como original como mensagem de dados, e não apenas como mensagem de dados em forma eletrónica. É esse o sentido da parte final da alínea a) do n.º 1 do art.º 8.º da LMCE, que anteriormente citámos.[1152]

[1149] Do mesmo modo, A/CN.9/WG.IV/WP.118/Add.1, 17 August 2012, par. 45.

[1150] O artigo 7-105, b),2) do Uniform Commercial Code tem a seguinte redação: *"(b) Upon issuance of a tangible document of title in substitution for an electronic document of title in accordance with subsection (a): (1) the electronic document ceases to have any effect or validity; and (2) the person that procured issuance of the tangible document warrants to all subsequent persons entitled under the tangible document that the warrantor was a person entitled under the electronic document when the warrantor surrendered control of the electronic document to the issuer"*. https://www.law.cornell.edu/ucc/7/7-105 (consulta efetuada em 2015/01/06.

[1151] Artigo 23.º, n.º 1, comentado por Ruggieri, F. (2008)., pag. 34.

[1152] *"As regards the words "the time when it was first composed in its final form" in paragraph (l)(b), it should be noted that the provision is intended to encompass the situation where information was first composed as a paper document and subsequently transferred on to a computer. In such a situation, paragraph (1) (b) is to be interpreted as requiring assurances that the information has remained complete and unaltered from the time when it was composed as a paper document onwards, and not only as from the time when it was translated into electronic form"*. "A/CN.9/426", par. 76.

A interoperabilidade é considerada como um instrumento essencial para o desenvolvimento do comércio eletrónico, e foi identificada pela UE como um instrumento fundamental nesse domínio.[1153]

Em Portugal, o art.º 32.º do Decreto-Lei n.º 135/99, de 22/4, prevê um regime de conversão de documentos em suporte de papel para documentos eletrónicos no âmbito do procedimento administrativo. Assim, sendo exibido o original no serviço competente para o procedimento, deve este declarar a respetiva conformidade no próprio documento ou em documento autónomo. Este procedimento é, porém, relativamente inseguro.

Também nos parece pouco seguro o procedimento que o n.º 4 do mesmo art.º estabelece para os casos em que são apresentados documentos eletrónicos que estão arquivados noutros serviços da administração pública. Nesse caso a lei exige uma declaração de conformidade do dirigente do serviço onde o documento está arquivado (alínea b)). Com os meios tecnológicos de autenticação existentes, essa declaração deveria ser substituída por uma assinatura eletrónica, ou então um selo eletrónico. Só assim se garante a autenticidade do documento, como a sua integridade, que não pode ser garantida pela declaração manual de qualquer dirigente.

Esta norma é importante, porque o mesmo diploma legal passou a consagrar o direito dos cidadãos de não apresentarem documentos aos órgãos da administração pública, nos casos em que esses documentos estejam arquivados noutros serviços.[1154] Nestes casos, e mediante autorização do interessado, deve o serviço competente para o procedimento obter o documento no serviço que o possuir, e que o interessado tiver indicado. Também esta norma deveria salvaguardar a autenticidade e a integridade dos documentos respetivos.

Este regime de conversão dos suportes dos documentos é também insuficiente porque aplicável apenas a procedimentos em concreto, não sendo um regime genérico, aplicável a qualquer tipo de documento.

Uma medida relevante de interoperabilidade é a possibilidade de os órgãos da administração pública emitirem documentos em suporte eletrónico, com a menção, quando impressos em papel, de um código para validação eletrónica. Esse código

---

[1153] *"A interoperabilidade das aplicações da administração pública em linha requer a interoperabilidade das Infraestruturas de Chave Privada (PKI) mediante um Serviço Europeu de Validação (European Bridge)"*. "Mercado único digital competitivo - a administração pública em linha como força motriz. Resolução do Parlamento Europeu, de 20/4/2012, sobre um mercado único digital competitivo - a administração pública em linha como força motriz (2013/C 258 E/09)". JOCE, 7.9.2013, C 258 E/65.

[1154] Artigo 28.º-A do DL n.º 135/99, de 22/2, aditado pelo DL n.º 73/2014, de 13/5.

servirá para que, posteriormente, mediante a sua inserção, qualquer pessoa ou entidade que assim o pretenda, poder consultar o original em suporte eletrónico, no sítio *web* da entidade emissora. A utilização deste mecanismo está prevista também no n.º 3 do art.º 28.º-A, do Decreto-Lei n.º 135/99, de 22/4.

Apesar das medidas de interoperabilidade entre os documentos em papel e os documentos eletrónicos previstas neste diploma, falta um regime que seja aplicável a todos os documentos, quer sirvam para as relações administrativas quer privadas, e que contemple tanto a transposição dos documentos em papel para documentos eletrónicos como em sentido inverso. Esse regime é muito importante para a generalização da utilização dos meios eletrónicos, em especial num contexto de transição dos suportes de papel para os suportes digitais.

Um regime desse tipo poderia também ele assentar no princípio da autonomia contratual e no estabelecimento de um regime geral assente na intervenção de entidades terceiras que certificassem a autenticidade e integridade das transposições, bem como os referenciais de tempo e lugar em que ocorreram.

Esse regime deveria estabelecer as condições de transição da autenticidade dos documentos que se encontram num suporte para o outro suporte, devendo existir sempre algum tipo de certificação que a assegure.

A existência de um regime desse tipo é muito importante para que as empresas e os particulares pudessem digitalizar os seus arquivos, transpondo-se para os correspondentes documentos eletrónicos a validade e eficácia jurídica dos documentos em papel.

4. A identidade eletrónica

A identidade é a representação objetivada que terceiros têm acerca de uma pessoa determinada. O conceito de identidade define-se como o conjunto de atributos que servem para identificar uma pessoa singular ou coletiva, ou seja uma entidade.[1155]

[1155] A norma ISO/IEC DIS 29115 utiliza a dicotomia entre "*identidade*" e "*entidade*", sendo com este último conceito que se refere à pessoa, singular ou coletiva, que é sujeito de direitos. Nos termos dessa norma, uma "*entity*" é "*something that has separated and distinct existence and that can be identified in a context*" (3.4). O Regulamento (EU) 910/2014, de 23/7 (EIDAS), utiliza o conceito de "*Utilizador*", definindo-o como "*a pessoa singular ou colectiva que utiliza a identificação eletrónica ou o serviço de confiança*" (n.º 6 do artigo 3.º). Do mesmo modo, o Regulamento de Execução (UE) 2015/1502, de 5/9/2015 utiliza o conceito de "*pessoa*", apesar de se basear na norma ISO/IEC DIS 29115, antes referida.

Trata-se de um conjunto de referenciais que permitem estabelecer a conexão entre uma pessoa e os atos que ela pratica. Esses referenciais, ou atributos, podem ser vários e de diversa natureza, mas são sempre objetivos, apreensíveis por terceiros de forma relativamente uniforme. A pessoa está sempre antes e para além desses atributos, como sujeito irrepetível e irredutível, que se expressa exteriorizando a sua vontade, o seu conhecimento e a sua personalidade, através de sinais exteriores e apreciáveis pelos outros. Alguns desses sinais são únicos e específicos de cada pessoa, e são eles, pela sua especificidade e representatividade, que servem, como modos objetivos e exteriorizados de desvelamento de uma pessoa, de instrumentos de mediação que revelam a presença dessa pessoa.

Nas relações presenciais, a identidade é revelada pelos traços físicos ou comportamentais da pessoa, pela sua voz, as feições do seu rosto, a sua presença física, o seu comportamento. A constatação de que estamos perante uma pessoa determinada depende da utilização de um ou vários desses atributos, que no seu conjunto podemos designar de identidade. É através desses sinais, cuja repetição os torna típicos, que os outros reconhecem a personalidade perante quem se encontram. A tipificação desses sinais conduz a que eles sejam utilizados com mais frequência para determinar ao conhecimento acerca da presença de uma pessoa. O conjunto desses sinais, ou uma parte deles, revela a identidade de uma pessoa.[1156]

Alguns desses elementos são utilizados nos documentos que as entidades competentes para a identificação civil ou comercial emitem e que servem para identificar as pessoas, por exemplo o bilhete de identidade ou o passaporte, porque deles constam, nomeadamente a fotografia, as impressões digitais, a forma como assina, etç. Mas também são esses elementos que servem para que as entidades competentes para a emissão desses documentos, se assegurem de que esses documentos se referem à pessoa que em concreto identificam. Cada um desses atributos da pessoa que é usado para a sua identificação designa-se de fator de identificação. Um fator de identificação pode utilizar um ou mais atributos de identificação, sendo que a utilização de vários elementos torna o fator de identificação mais seguro, porque permite uma constatação da identidade da pessoa de uma forma mais completa.

Utilizamos a expressão "*pessoa*", como o sujeito das relações jurídicas, e que pode incluir pessoas singulares e coletivas

[1156] A Norma ISO/IEC DIS 29115 define identidade como "*set of attributes related to an entity*", acrescentando em nota explicative que "*an identity may have one or more identifiers to allow an entity to be uniquely recognized*" (3.13).

A identificação de uma pessoa é um processo, mediante o qual se determina a sua identidade. Esse processo inicia-se, normalmente, com a invocação, por uma pessoa, de uma identidade que alega ser sua.[1157] Trata-se de uma declaração, verbal ou escrita, que necessita de ser verificada pelo respetivo destinatário, a fim de comprovar a sua veracidade. Essa verificação é normalmente efetuada pela pessoa perante quem é proferida a declaração em que é invocada a identidade, e designa-se de autenticação. A autenticação é o processo de confirmação da identidade invocada por uma pessoa, efetuada por terceiros, mediante os fatores de identificação que lhe são apresentados. A identidade pode provar-se, e essa comprovação designa-se de autenticação.

O processo de autenticação não é simples, tanto para o sujeito que se identifica como para a entidade ou pessoa perante quem essa identificação é efetuada, porque deve ser sempre acompanhada, para além da declaração de identificação, dos elementos de prova correspondentes. Para a entidade recetora dessa declaração, os procedimentos de verificação da autenticidade dos fatores de identificação também não será simples. Ambos os procedimentos são, porém, simplificados, se uma parte da autenticação poder ser substituída por certificação de uma entidade especializada, que possua crédito suficiente para gerar confiança nos agentes, confirmando que efetuou a autenticação de um conjunto de fatores de identificação. É o que ocorre com as entidades públicas competentes que executam o serviço público de identificação civil, que depois de efetuarem um procedimento de identificação e de autenticação de uma determinada pessoa emitem um instrumento objetivo que certifica que a pessoa que os possui está identificada e corresponde à identidade que invoca. Esses instrumentos assumem muitas vezes a forma de documentos, por exemplo o cartão de identificação ou o passaporte, e tornam a identificação mais simples, porque dispensam as tarefas de autenticação que conduziram à sua emissão, sendo sucedâneas delas.

Na verdade, uma vez invocada uma identidade, aquele perante quem essa invocação é feita poderá verificar essa identidade de forma mais simples mediante esses instrumentos, sem necessidade de repetir os procedimentos que conduziram à sua geração, e que eles representam. Essa simplicidade resulta apenas do facto de beneficiar do trabalho de identificação que já foi efetuado pela entidade que a efetuou e que conduziu à emissão daquele instrumento de identificação, dado que a existência desse

[1157] A Norma ISO/IEC DIS 29115 utiliza o conceito de "*claim*", definindo-o como "*statement that something is the case, without being na accurate and up-to-date source of information*", acrescentando que este conceito é próximo do de "*assertion*" (3.6).

instrumento dispensa, porque substitui, o processo de identificação que conduziu à sua emissão. Esses instrumentos são designados como meios de identificação. A verificação e a prova da identidade seriam muito mais difíceis sem esses meios de identificação.

O documento de identificação ou o passaporte que uma pessoa apresenta para que o seu interlocutor possa comprovar a identidade por si invocada são as suas credenciais de identificação. Na posse delas, o interlocutor compara os respetivos com a pessoa que com eles se identificou, por exemplo, verificando a fotografia. Quando esse procedimento é sistematizado, por exemplo quando é efetuado por profissionais de forças de segurança ou outros, designa-se de protocolo de autenticação.

4.1. - As dificuldades adicionais da identificação eletrónica

Nos suportes eletrónicos a determinação da identidade é mais difícil do que nas relações estabelecidas fisicamente, pela dificuldade em apreender os fatores de identificação, dado que esses fatores têm que consistir sempre em dados, e é necessário garantir uma ligação segura entre os dados e a pessoa. Ora, os fatores de identificação eletrónica têm, relativamente aos da identificação em geral, a dificuldade da sua apreensão naturalística. Na verdade, a imediatez que se pode constatar quando os elementos de identificação são a voz, o estilo da escrita, a fotografia, o comportamento e as impressões digitais, não é possível com os dados em suporte eletrónico.

Esses dados necessitam de ser produzidos e a sua produção deve garantir uma ligação efetiva e segura à pessoa, de modo que se possam considerar representativos dessa pessoa e se possam considerar fatores de identificação. Por essa razão, a produção desses dados deve respeitar um conjunto de requisitos de segurança, dos quais depende o seu nível de garantia e de confiança.

Depois de produzidos, esses dados são utilizados pelo respetivo titular para se identificar nos ambientes eletrónicos. Esses dados devem ser protegidos contra utilizações indevidas ou fraudulentas, para o que devem estar sempre na posse ou domínio do seu titular, de modo que não fiquem expostos à utilização por terceiros. Para isso podem ser gravados num suporte material que permita a sua portabilidade e a sua utilização segura.

Esse suporte é designado como um meio de identificação eletrónica.[1158] A segurança dos meios de identificação eletrónica, tanto no que respeita à sua criação como à sua manutenção e utilização é de importância fundamental para a segurança jurídica e a confiança na utilização dos meios eletrónicos.

Sempre que uma pessoa se pretenda identificar perante um sistema informático, está a invocar os dados da sua identificação, ou seja, a reivindicar uma identidade.[1159] O responsável pelo sistema informático que está a ser utilizado tem o dever de confirmar essa identidade e de se certificar de que ela corresponde à pessoa que a invoca. Para isso utiliza os dados de identificação que a pessoa disponibiliza e que constam do meio de identificação eletrónica que foi utilizado. Essa operação de verificação designa-se de autenticação e, mediante ela, constata a identificação de uma pessoa e adquire a confiança de que a pessoa que a invoca corresponde efetivamente ao titular dessa identidade.[1160] Os meios de identificação podem conter um ou vários fatores de identificação que, quando utilizados na confirmação da identidade reivindicada, se convertem em fatores de autenticação. Esses fatores de autenticação podem separar-se em três categorias:

i) Fatores baseados na posse. Algo que a pessoa possui, por exemplo um passaporte ou um cartão de identificação com assinatura, uma credencial ou uma chave privada, um código ou um *token*. A posse desse fator comprova a identidade;

ii) Fatores baseados no conhecimento. Algo que a pessoa sabe, por exemplo uma palavra-chave, uma senha de acesso, cuja invocação e utilização comprova a identidade;

iii) Fatores inerentes à pessoa. Algo que é intrínseco à pessoa, por exemplo as caraterísticas biométricas.[1161]

[1158] O n.º 2 do artigo 3.º do EIDAS, define meio de identificação eletrónica como "*uma unidade material e/ou imaterial que contenha os dados de identificação pessoal e que seja utilizada para autenticação de um serviço em linha*".

[1159] O Regulamento EIDAS não define o que se entende por reivindicação de uma identidade e o Regulamento de execução 2015/1502 também não, mas a Norma ISO/IEC DIS 29115

[1160] A autenticação eletrónica é definida pelo regulamento EIDAS como "*o processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou colectiva ou da origem e integridade de um determinado dado em formato eletrónico a confirmar*".

[1161] O Regulamento de Execução (EU) 2015/1502, de 5/9/2015, enuncia no seu anexo I estes três fatores de autenticação, apesar de ele se basear na Norma ISO/IEC DIS 29115, que enuncia 4 fatores, incluindo, para além dos que anteriormente referimos, os fatores baseados no comportamento ("*something na entity tipically does*").

A identificação eletrónica é um instrumento de segurança jurídica que confere confiança à utilização dos meios eletrónicos, tal como a assinatura eletrónica, mas não se confunde com ela, porque enquanto esta última se refere a documentos, a primeira refere-se a pessoas.

A invocação da identidade e a sua verificação é utilizada no contexto eletrónico para habilitar as pessoas a acederem a serviços prestados mediante plataformas eletrónicas. Por exemplo, para acesso a publicações eletrónicas, à consulta de informação, bancária fiscal, de identificação, processual, bem como no acesso a serviços culturais, literários, musicais, filmográficos, etç. Na função administrativa a identificação serve para legitimar o acesso a informação protegida, por exemplo a dados pessoais, constantes de bases de dados das administrações públicas, pelo próprio interessado ou à consulta de procedimentos em curso ou concluídos e a outros serviços de natureza idêntica.

Nestes casos não é necessária a utilização da assinatura eletrónica, dado que não se trata do envio de documentos cuja autenticação seja necessária. Trata-se apenas do acesso a determinadas funções e serviços, reservados a determinadas pessoas, pelo que bastará a invocação, por estas, da sua identidade, e a sua confirmação pela entidade competente, para legitimar o acesso.

O crescimento da utilização dos meios eletrónicos na atividade económica antes da consolidação dos regimes legais respetivos conduziu à proliferação dos meios de identificação, sendo que muitos deles foram desenvolvidos por agentes económicos e entidades públicas. É comum que cada um desses agentes possua um sistema próprio, na maioria dos casos em forma de palavras-passe, associadas a um conjunto de dados recolhidos previamente, em convenção prévia de autenticação entre essas entidades e os respetivos utilizadores.[1162] Nesses casos, sempre que um utilizador pretende interagir com uma dessas entidades, invoca a sua identificação, mediante a inserção do seu nome de utilizador, solicitando o sistema, de seguida, a confirmação com a palavra passe, que uma vez inserida permite constatar, com aos dados que existem no sistema informático, a autenticidade dos dados de identificação do utilizador.[1163]

[1162] *"A maioria dos sistemas de autenticação assenta em senhas (passwords) de utilização única e sinais especiais (tokens)"*. COM(2006) 120 final, pág. 6.

[1163] Como se refere na proposta da CE, de regulamento relativo à identificação eletrónica, *"A fiabilidade de uma identificação eletrónica depende da disponibilidade de meios de autenticação (ou seja, da possibilidade de verificar a validade dos dados da identificação eletrónica)*". COM(2012) 238 final, pág. 6.

Não existe uma identidade eletrónica universal que possa ser utilizada, com a mesma simplicidade com que se utiliza a identificação civil nas relações não eletrónicas. Ao contrário do paradigma do papel, em que existe um único sistema de identificação, que é um serviço de natureza pública, e é composto pelo documento de identificação oficial, nos sistemas eletrónicos não existe um modelo universal de identificação. Essa lacuna, associada à proliferação de meios de identificação eletrónica, produz dois resultados, ambos problemáticos:

i) É, em si mesma, uma ameaça à segurança e à confiança na utilização dos meios e dos serviços eletrónicos, em especial pela dificuldade, para os respetivos utilizadores, de guardarem em condições de segurança e manterem secretos e ao mesmo tempo utilizáveis, os respetivos meios de identificação eletrónica;

ii) É um entrave à utilização dos meios eletrónicos no tráfego jurídico e comercial, pelas dificuldades de gestão, pelos interessados, dos diversos meios de identificação, e pela necessidade de repetirem, o processo de identificação e autenticação de cada vez que pretendem aceder a um serviço diferente.

4.2. – Os efeitos do regime europeu da identificação eletrónica

O sistema de reconhecimento mútuo que o Regulamento EIDAS institui, e que podemos designar como sistema europeu de identificação eletrónica, proporciona aos cidadãos dos Estados Membros dois importantes bens jurídicos:

i) O princípio do aproveitamento dos atos de autenticação, mediante o qual, quando tenha ocorrido a comprovação da identidade de um cidadão, para efeitos de identificação, mesmo que de meios de identificação não eletrónica, não será necessário repetir esses procedimentos, sendo substituídos pelos meios de identificação que foram gerados e os representam;

ii) O princípio do reconhecimento mútuo e da interoperabilidade, que permite que uma pessoa, singular ou coletiva, possua apenas, no limite, uma identificação eletrónica e que a possa utilizar em todos os Estados Membros como meio de identificação eletrónica perante os respetivos órgãos da administração púbica.

Naturalmente que estes dois resultados, que consubstanciam outros dois direitos dos cidadãos, só se produzem nos casos em que se trate de meios de identificação seguros, no limite com nível de garantia elevado. Mas trata-se de dois importantes resultados, que vêm tornar muito mais simples e segura a utilização de meios eletrónicos.

4.2.1. – No espaço da União Europeia

Nas transações eletrónicas intracomunitárias, a inexistência de um sistema de reconhecimento mútuo e de interoperabilidade eletrónica era agravado pela segmentação de sistemas de identificação e pelo não reconhecimento dos sistemas de identificação eletrónica entre os Estados Membros.

A identificação eletrónica, para ser segura, assenta sempre na identificação não eletrónica, dado que o elemento fundamental da identificação é a presença física da pessoa e o confronto dos seus traços físicos com os dados de identificação que constam do documento correspondente. Ora, para uma pessoa que pretenda realizar transações com relevância jurídica, no limite com órgãos da administração púbica de todos os Estados Membros, teria que se deslocar fisicamente a todos eles para que, pelo menos na primeira vez, em cada um se emitisse um meio de identificação eletrónica. E poderia ter que repetir esse procedimento perante cada um dos órgãos com quem pretendesse efetuar transações, pelo que, se num mesmo Estado Membro necessitasse de efetuar transações eletrónicas com vários órgãos públicos, dado que essa interoperabilidade também não existe dentro de cada Estado.

Esta necessidade representava um constrangimento de relevo à utilização dos meios eletrónicos, dado que eliminava uma das suas principais vantagens, que é a da possibilidade de se efetuarem transações à distância, com relevo jurídico e sem necessidade da deslocação física.

Por outro lado, mesmo depois de cada pessoa possuir um meio de identificação eletrónica que lhe permitisse efetuar transações eletrónicas em todos os Estados Membros, a falta de reconhecimento transacional, obrigava a que utilizasse cada um deles de forma diferenciada nas transações que efetuasse em cada Estado Membro, o que tornava muito difícil a sua gestão e a realização das respetivas operações.

Ambos os tipos de constrangimentos elevam também os riscos de segurança jurídica, porque os intervenientes tendem a adotar soluções mais simples que são ao mesmo tempo mais inseguras, e também pela dificuldade em gerir com segurança uma tão elevada quantidade de meios de identificação eletrónica.

O Regulamento EIDAS vem dar resposta a ambos os problemas, permitindo que, no limite, cada pessoa possua apenas um meio de identificação eletrónica seguro, que pode utilizar em todas as transações eletrónicas que efetuar, criando as condições para a sedimentação de um espaço europeu eletrónico integrado.

Na verdade, os meios de identificação eletrónica com níveis de garantia substancial e elevado adquirem validade e eficácia em todo o espaço da União Europeia. Em consequência, tendencialmente, os cidadãos dos Estados Membros que possuam um desses meios passarão a poder utilizá-lo para acederem a todos os serviços prestados em linha por órgãos da administração pública em qualquer outro Estado. Aqueles que possuam um meio de identificação com nível de garantia substancial poderão utilizá-lo para aceder a serviços eletrónicos que exijam o correspondente nível de garantia, mas já não o poderão utilizar naqueles que exijam nível elevado. Esta universalidade é o mais importante resultado do Regulamento EIDAS e um verdadeiro direito dos cidadãos europeus à identificação eletrónica única.

Estabelece-se assim um direito dos cidadãos da União Europeia à utilização transfronteiriça dos meios de identificação eletrónica, que se constitui logo que exista notificação, publicitação pela Comissão e reconhecimento pelos Estados Membros respetivos. Esse direito é o principal efeito do Regulamento, no que respeita à identificação eletrónica, e é aquele que está na base do mercado digital europeu.

4.2.2. – No seio de cada Estado Membro

O sistema de reconhecimento mútuo instituído pelo Regulamento coloca a questão da sua eficácia interna, na jurisdição de cada Estado Membro. Atualmente existe uma elevada multiplicidade de meios de identificação eletrónica, mesmo nos serviços prestados em linha pelos diversos órgãos da administração pública. Por exemplo, em Portugal, além do cartão do cidadão, que é um meio de identificação eletrónica, a administração tributária tem um sistema próprio de identificação e de autenticação e a Segurança Social tem outro sistema próprio, para além do sistema dos

Tribunais e outros. As pessoas singulares ou coletivas, que tendencialmente podem necessitar de operar com todos esses serviços eletrónicos, necessitam de se identificar previamente perante os respetivos órgãos, para serem gerados os respetivos meios de identificação eletrónica e depois, sempre que pretendam aceder a cada um deles necessitam de utilizar cada um desses diferentes meios.

Ou seja, os problemas da segmentação e da falta de reconhecimento mútuo entre os Estados Membros da União Europeia existem também no seio de cada um dos Estados. Coloca-se, por isso, a questão de saber se o Regulamento se aplica às relações jurídicas internas no seio de cada Estado. Ou dito de outro modo, o direito que um cidadão tem de utilizar um meio de identificação num Estado Membro diferente daquele onde foi produzido, aplica-se também ao direito de esse mesmo cidadão utilizar esse meio de identificação para aceder a todos os serviços em linha dos diversos órgãos da administração pública do seu país?

Em nosso entender não, nesta parte o Regulamento aplica-se apenas à autenticação transfronteiriça e vincula apenas os Estados à aceitação da utilização de sistemas de identificação gerados noutros Estados, quando o nível de garantia seja igual ou superior. Retiramos essa conclusão do texto do próprio n.º 1 do artigo 6.º do Regulamento EIDAS, sendo manifesto em todo o seu conteúdo que o legislador do Regulamento teve o cuidado de não pretender abranger as relações jurídicas internas estabelecidas em cada Estado Membro. O problema é que daqui resulta uma discriminação, dado que o mesmo órgão da administração pública está obrigado a aceitar a utilização de meios de identificação eletrónica diferentes daquele que utiliza normalmente, quando gerados noutros Estados Membros, mas essa obrigação já não existe quando sejam gerados no interior desse mesmo Estado. Esta discriminação necessita de ser eliminada pela legislação interna.

Em Portugal o Cartão do Cidadão é um meio de identificação eletrónica, como estabelece a alínea b) do n.º 2 do artigo 6.º e o n.º 1 do artigo 18.º da Lei n.º 7/2007 de 5 de fevereiro, servindo também de documento autêntico de identificação, nos termos do artigo 2.º do mesmo diploma legal.

As especificações legais que regulam a atribuição do Cartão do Cidadão correspondem ao nível de garantia elevado, nos termos do n.º 3 do artigo 8.º do Regulamento EIDAS, sendo também o único meio de dentificação eletrónica em Portugal cujo regime legal de criação, gestão, segurança, cancelamento e suspensão estão regulados.

Apesar disso não existe uma obrigação legal de os órgãos da administração pública aceitarem, em exclusividade, a identificação e autenticação do Cartão do Cidadão. Essa obrigação legal deve, porém, ser instituída, constituindo-se o Cartão do Cidadão como o meio de identificação eletrónica universal em Portugal, obrigando-se todos os órgãos da administração pública a aceitá-lo como tal.[1164]

Por outro lado deverá também o direito interno português consagrar o princípio da interoperabilidade e o direito dos cidadãos a poderem utilizar apenas um meio de identificação eletrónica em todos os serviços em linha disponibilizados pelas administrações públicas portuguesas. Só assim se elimina a discriminação, que atualmente já existe, entre os titulares de meios de identificação eletrónica produzidos noutros Estados Membros, que já possuem esse direito, e os titulares desses meios produzidos em Portugal, que não podem beneficiar desse direito nas transações eletrónicas internas.

4.2.3. – Nas empresas privadas

O sistema de interoperabilidade e reconhecimento mútuo da identificação eletrónica aplica-se apenas, de forma obrigatória, à identificação perante serviços em linha das administrações púbicas, estabelecido pelo Regulamento EIDAS. No entanto esse desiderato faz parte de um outro mais amplo, que é enunciado nos próprios considerandos do Regulamento, de criação de um "*mercado único digital*" (ponto 5), envolvendo também as empresas privadas.

O envolvimento das empresas privadas é admitido expressamente no texto legal, embora seja meramente facultativo. Esse envolvimento pode ocorrer do lado dos próprios sistemas que os Estados pretendam notificar à Comissão, mas com a condição de esses sistemas estarem a operar ao serviço ou por conta de um organismo público (alíneas a) e b) do artigo 7.º).[1165]

[1164] Não entendemos que essa obrigatoriedade resulte já da lei portuguesa, tal como defende Francisca Almeida D'Eça, que entende que "um cidadão só pode utilizar legalmente para este efeito, o certificado digital atribuído pelo cartão do cidadão e não outro". Almeida D'Eça, F. (2009). *Registos On Line, 2.ª Edição Revista e Actualizada*. Edições Almedina, S. A. Coimbra, pág. 48.

[1165] Prevê-se inclusivamente a responsabilidade dessas empresas privadas pelos danos causados pela criação dos meios de identificação eletrónica, nos casos em que tenham resultado de ação culposa, dolosa ou negligente (n.º 2 do artigo 11.º do Regulamento EIDAS)

O envolvimento das entidades privadas ocorrerá com maior efetividade, como entidades utilizadoras, conferindo aos agentes económicos e cidadãos que pretendam adquirir bens ou serviços por meio dos serviços eletrónicos, a possibilidade de utilizarem meios de identificação eletrónica emitidos por entidades públicas e que estejam publicitados pela Comissão. Essa possibilidade permitirá a esses cidadãos e agentes económicos ficarem dispensados de possuírem um meio de identificação eletrónica específico para essas empresas, o que aumenta a simplicidade e a segurança do comércio eletrónico. Esta possibilidade postula as entidades privadas como utilizadoras ou adquirentes de serviços eletrónicos

O Regulamento prevê também, na segunda parte da alínea f) do artigo 7.º essa mesma possibilidade relativamente às entidades privadas que sejam prestadoras de serviços eletrónicos. Nessa função, essas empresas privadas utilizam, para autenticar a identidade dos seus clientes, os sistemas de identificação eletrónica de organismos públicos de outros Estados Membros.

Esta possibilidade é relevante para a criação do mercado único digital e a promoção do comércio eletrónico e poderá conduzir, também ela a que, progressivamente se reduza a quantidade de sistemas de identificação eletrónica existentes em cada Estado Membro, contribuindo assim também para o incremento do mercado digital integrado.

Esta mesma possibilidade deveria também ser prevista na legislação interna portuguesa, o que não ocorre atualmente.

4.3. – As limitações do regime europeu da identificação eletrónica

O regime de identificação eletrónica instituído pelo Regulamento EIDAS não é um sistema de identificação eletrónica. Trata-se apenas de um regime de interoperabilidade dos sistemas nacionais de identificação eletrónica. Ele opera sobre os regimes que já existem ou que venham a existir nos Estados Membros da União Europeia e não se substitui nem concorre com eles.[1166] O seu objetivo fundamental é permitir que esses sistemas nacionais possam ser reconhecidos e os respetivos meios de identificação utilizados noutros Estados Membros. O reconhecimento mútuo é o

[1166] Essa preocupação é claramente expressa nos considerandos do Regulamento: "*O presente regulamento não visa intervir em matéria de sistemas de gestão da identidade eletrónica (…) existentes nos Estados-Membros*". Ponto 12.

instituto jurídico fundamental e o regime de interoperabilidade o quadro jurídico que garante a sua efetividade.

Trata-se de um importante avanço no direito da identificação eletrónica, que tem impacto na chamada economia digital, bem como no próprio procedimento administrativo. A instituição do direito dos cidadãos à utilização transnacional dos meios de identificação eletrónica, que deriva do Regulamento é também um passo importante.

Mas este regime não institui ainda um direito à identidade eletrónica. Um direito desse tipo habilitaria cada cidadão a poder utilizar um único instrumento de identificação para a realização de todas as transações com relevância jurídica. Não apenas para a identificação perante serviços eletrónicos, mas para a identificação e autenticação de todas as transações que se podem fazer por meios eletrónicos.

A falta de um instrumento único de identidade eletrónica, bem como de um regime jurídico sistematizado, conduziu ao longo do tempo, à multiplicação de meios de identificação, quase tantos quanto os agentes económicos ou administrativos que operam por meios eletrónicos, e quase sempre mediante recurso a soluções assentes em tecnologia insegura e menos universalizável, nomeadamente a das senhas de acesso.[1167] Essa multiplicação é um fator de insegurança e um obstáculo ao desenvolvimento do comércio eletrónico, há muito tempo diagnosticada.[1168]

A identificação da necessidade de um regime jurídico sistemático nesta matéria tem sido acompanhada do reconhecimento da insuficiência dos avanços nesta disciplina jurídica. A adoção dos regimes jurídicos de assinatura eletrónica era apresentada, inicialmente, como a solução para o problema, existindo a expetativa de que, mediante

---

[1167] A proliferação das senhas de acesso como instrumento de identificação e de autenticação predominante nas práticas comerciais pelos agentes económicos e pelas administrações públicas era reconhecida em 2010 pela CE, reconhecendo-se também, implicitamente, o relativo fracasso das assinaturas digitais, no Programa da Agenda Digital: *"Actualmente, o meio mais comum de autenticar consiste na utilização de senhas (passwords). Para muitas aplicações, as senhas podem ser suficientes, mas são cada vez mais necessárias soluções mais seguras"*. COM(2010)245 final, pág. 12.

[1168] A possibilidade de existência de um instrumento de identidade eletrónica não colide necessariamente com o n.º 5 do artigo 35.º da Constituição, dado que o que essa norma proíbe é e existência de "um número nacional único" atribuído a cada cidadão. Na verdade, os diferentes órgãos da administração pública podem ter números de identificação de cada um dos cidadãos que com eles operam. Esse é, aliás, um dos procedimentos habituais dos sistemas informáticos. Esse número específico que identifica cada um dos cidadãos, pode estar associado a um meio de identificação eletrónica que pode ser utlizado por cada cidadão, e apenas por ele, sendo que quando ele invoca essa identificação eletrónica em cada um desses órgãos desencadeia a referenciação para a identificação interna com que esse órgão o conhece nos seus sistemas informáticos internos. Esse procedimento já era utilizado nos sistemas não eletrónicos, dado que para a emissão dos diversos números de identificação, por exemplo o Número de Identificação Fiscal, o Número de Identificação da Segurança Social, o Número de Identificação da Saúde, se baseiam sempre na utilização, por cada cidadão, da identificação constante do Cartão do Cidadão.

esse regime, se criaria um instrumento jurídico universal para a identificação e a autenticação eletrónica. Mas apesar do fenómeno legiferante que se desenvolveu nesta matéria na transição do século, manteve-se o fenómeno da proliferação dos meios de identificação eletrónica, quase sempre nos instrumentos pouco seguros das palavras-chave.[1169]

Provavelmente os custos da criação das assinaturas eletrónicas qualificadas poderão ser uma das causas deste aparente insucesso. Do mesmo modo a falta de interoperabilidade internacional dos vários sistemas nacionais de assinaturas eletrónicas é um fator impeditivo da diminuição da proliferação de meios de identificação eletrónica.[1170]

A necessidade de um regime de interoperabilidade dos sistemas de identificação eletrónica, há muito diagnosticada, é a primeira resposta jurídica ao problema da insegurança resultante da multiplicidade de meios de identificação eletrónica e o regime jurídico do Regulamento EIDAS é o produto da resposta a essa necessidade.[1171]

A interoperabilidade assenta no reconhecimento jurídico de todos os sistemas de identificação eletrónica, mas isso implica a sua existência, pelo que não resolve o problema daquela proliferação. Subsiste, portanto, a necessidade da criação de condições jurídicas para que cada cidadão possa utilizar um meio universal de identificação eletrónica. Essa possibilidade seria um fator de segurança jurídica e de eficiência económica.

O conhecimento que permitiu a criação da tecnologia das chaves assimétricas permite também que seja possível a criação de um regime jurídico da identidade eletrónica, proporcionando aos cidadãos e aos agentes económicos a possibilidade de se apresentarem nos meios eletrónicos com a sua própria identidade.

[1169] Esse fracasso relativamente às expectativas era reconhecido num relatório da CE de 2006. *"Havia alguma esperança de que a adopção da Directiva ajudasse o mercado das assinaturas eletrónicas a arrancar"* E mais adiante, *"Não existe explicação simples para o facto de o mercado das assinaturas eletrónicas não se ter desenvolvido mais rapidamente"*. COM(2006) 120 final.

[1170] Com se refere no mesmo relatório, *"A falta de interoperabilidade técnica a nível nacional e transfronteiras é outro obstáculo à aceitação das assinaturas eletrónicas no mercado, tendo dado origem a muitas ilhas "isoladas" de aplicações de assinatura eletrónica em que os certificados só podem ser utilizados numa única aplicação"*. COM(2006) 120 final, pág. 8.

[1171] A necessidade da interoperabilidade dos meios de identificação e de autenticação eletrónica é mais difícil quando se trata da utilização de palavras-passe, e tem sido objeto de várias iniciativas da CE, em especial a Agenda Digital Europeia. *"Como haverá inúmeras soluções, as empresas, apoiando-se em iniciativas políticas – em particular os serviços de governo electrónico – devem garantir a interoperabilidade baseada em normas e em plataformas de desenvolvimento aberto"*. COM(2010)245 final, pág. 12.

A identificação eletrónica, a assinatura eletrónica e em geral todos os serviços de confiança eletrónica têm reconhecidamente como instrumento mais seguro o conhecimento e a tecnologia das chaves assimétricas e das assinaturas digitais.[1172] Do mesmo modo, todos esses instrumentos jurídicos de segurança e de confiança eletrónica correspondem a formas de manifestação da identidade eletrónica das partes em negócios ou em atos jurídicos.

Na verdade, do que se trata, tanto na identificação eletrónica como nas assinaturas eletrónicas, nos selos eletrónicos e na autenticação dos sítios *web*, é de vincular pessoas a factos jurídicos por elas produzidos por intermédio de meios eletrónicos, ou seja, de superar a impessoalidade dos meios eletrónicos. Por essa razão, independentemente da função que cada um desses serviços de confiança eletrónica cumprem, todos eles têm na sua base a identificação de uma pessoa determinada. Trata-se, em todos os casos, antes de mais, de instrumentos de determinação da identidade eletrónica e da sua comprovação. E assim sendo, todos eles se poderiam reunir num único instrumento.

Os meios de identificação eletrónica que utilizam níveis de garantia elevados utilizam a tecnologia das assinaturas digitais e os mecanismos de identificação e de autenticação que são, na sua essência, os mesmos. Na verdade, quando se utiliza um meio de identificação eletrónica assente na criptografia das chaves assimétricas, utiliza-se o mesmo procedimento tecnológico que serve de base às assinaturas eletrónicas. O resultado é diferente, porque no primeiro caso se identifica uma pessoa e no segundo se autentica um documento, mas numa assinatura de um documento também é parte integrante dela a identificação de quem assina, e o processo da sua determinação é o mesmo. Assim, tanto as assinaturas eletrónicas como os selos eletrónicos, a autenticação dos sítios *web*, e até os serviços de envio de envio registado eletrónico têm em comum, antes de mais, a identificação de uma pessoa, singular ou coletiva, sendo que, além disso, cumpre cada um deles outra função.

Por essa razão faria sentido que o quadro legal fosse orientado no sentido de uma uniformização, em ordem a que um único instrumento de identidade eletrónica pudesse ser utilizado pelos agentes nas operações eletrónicas que efetuam, e que se caminhasse no sentido da criação de um conceito de identidade eletrónica.

[1172] O reconhecimento da segurança das assinaturas assimétricas é pacífico, sendo relevado pelas organizações internacionais de forma pacífica. *"As assinaturas digitais baseadas na criptografia de chaves públicas são actualmente a forma mais reconhecida de assinatura eletrónica"*.COM(1998) 297 final, pág. 10.

A identidade eletrónica é um conceito mais abrangente que o de identificação eletrónica e deve abranger todos os instrumentos de representação de uma pessoa no tráfego eletrónico, desde a presença eletrónica à identificação, à autenticação e, em geral, à vinculação dessa pessoa a todos os comportamentos que exterioriza por via eletrónica.

E embora essa seja uma necessidade genericamente reconhecida, e exista o conhecimento jurídico e tecnológico para que seja criada essa função universal, da identidade eletrónica, a verdade é que essa tecnologia das chaves assimétricas não se tem generalizado com a rapidez que era expectável, e os legisladores têm-se, pelo contrário, visto confrontados com a necessidade de conferirem relevância e interoperabilidade às assinaturas mediante palavra-chave.

A criação de um instrumento de identidade eletrónica é um desafio jurídico de elevado relevo, para o futuro. É nesse sentido que devemos interpretar a preocupação do legislador que no artigo 49.º do Regulamento EIDAS estabelece uma avaliação ao regime do reconhecimento mútuo dos meios de identificação eletrónica e a apresentação de propostas de revisão do regime, em face da evolução tecnológica.

Esse passo seria importante, tanto para a instituição de um direito dos cidadãos europeus à utilização de uma única identificação eletrónica, que pudesse utilizar de forma universal, não só em termos transfronteiriços, como também no interior de cada Estado Membro.

A inexistência de uma identidade eletrónica era particularmente sensível nos países da União Europeia, porque se tratava de um obstáculo à livre circulação e à criação de um mercado único do domínio digital. Na verdade, enquanto nas relações presenciais os cidadãos europeus se podem identificar com o seu documento de identificação perante qualquer entidade pública ou privada de outro estado membro, isso não era possível no tráfego eletrónico, onde não existe um sistema de identificação comum como aquele, que os agentes económicos e as entidades públicas possam utilizar de forma generalizada.

O problema foi reconhecido em 2010 pela União Europeia, no Programa da Agenda Digital Europeia, onde se fala, pela primeira vez, na identidade eletrónica, indo-se até mais longe, com a ideia de uma cidadania europeia neste domínio.[1173] Dois anos

[1173] Como se refere textualmente, *"As tecnologias de identidade eletrónica (eID) e os serviços de autenticação são essenciais para as transacções na Internet tanto no sector privado como no público"*. COM(2010)245 final, pág. 12

depois reconhece-se não existir um quadro europeu para a identificação eletrónica, e que a Diretiva 1999/93/CE não preenche essa lacuna, porque não foi previsto pelo legislador.[1174] Ainda em 2012, é aprovada a proposta que viria a dar origem ao Regulamento EIDAS, consignando num único documento legislativo o regime da identificação, da assinatura eletrónica e dos serviços de confiança conexos (que passaram a ser conhecidos pela sigla "EIDAS").[1175]

Mas o regime da identificação eletrónica do Regulamento EIDAS fica ainda distante do desiderato de se alcançar um regime de identificação eletrónica que possua a abrangência, a universalidade e a simplicidade do sistema tradicional de identificação pessoal em ambiente não eletrónico.

No domínio eletrónico só a assinatura digital possuirá as condições para vir a assumir essa função universal, mas a verdade é que a tecnologia das chaves assimétricas não se tem generalizado com a rapidez que era expectável, e os legisladores têm-se, pelo contrário, visto confrontados com a necessidade de conferirem relevância e interoperabilidade às assinaturas mediante palavra-chave.[1176] Esse facto impede a criação de um sistema de identificação eletrónica simples e universal, dado que a tecnologia das palavras-chave pressupõe sempre a existência de uma relação prévia no âmbito da qual se estabeleça uma convenção de autenticação. Pelo contrário, a tecnologia das chaves assimétricas proporciona condições para a identificação eletrónica sem a necessidade dessa convenção prévia, porque o conhecimento da identidade é garantido a toda a comunidade de eventuais terceiros interessados, pelas entidades terceiras de confiança que prestam serviços de certificação eletrónica.

Apesar do entusiasmo com que cada país se lançou na criação de legislação acerca da assinatura eletrónica, a sua expansão ficou aquém das expectativas iniciais,

---

[1174] Nomeadamente nos seguintes termos: *"There is no comprehensive EU cross-border and cross-sector framework for eIAS services. At EU level, a legal framework exists only for e-signatures but not for e-identification and authentication nor for related ancillary trust services"*. SWD(2012) 136 final, ponto 1.

[1175] Este conceito foi utilizado pela primeira vez em documentos dos órgãos da UE, na proposta de regulamento sobre a Identificação Eletrónica: *"identificação, a autenticação e a assinatura eletrónicas e os serviços de confiança conexos (sigla inglesa «eIAS»)"*. "COM(2012) 238 final", ponto 2 da Exposição de Motivos.

[1176] A necessidade da interoperabilidade dos meios de identificação e de autenticação eletrónica é mais difícil quando se trata da utilização de palavras-passe, e tem sido objeto de várias iniciativas da CE, em especial a Agenda Digital Europeia. *"Como haverá inúmeras soluções, as empresas, apoiando-se em iniciativas políticas – em particular os serviços de governo electrónico – devem garantir a interoperabilidade baseada em normas e em plataformas de desenvolvimento aberto"*. COM(2010)245 final, pág. 12.

nomeadamente as assinaturas eletrónicas mais seguras, que são as qualificadas.[1177] A assinatura eletrónica qualificada é, reconhecidamente, o sistema mais aperfeiçoado de identificação e de autenticação eletrónica, pelas garantias que oferece de segurança e de possibilidade de utilização universal.[1178] Apesar disso, essa universalização não ocorreu, sendo que a dificuldade na sua expansão tem conduzido a que proliferem sistemas paralelos que são desenvolvidos por várias instituições públicas e privadas, nomeadamente mediante a adoção da tecnologia mais insegura e menos universalizável, das senhas de acesso.[1179] Uma das razões que é identificada para esse insucesso relativo é precisamente o facto de pouco se ter avançado na interoperabilidade internacional, bem como na criação de um regime geral de identificação e de autenticação.[1180]

Muitos países avançaram com a criação dos chamados bilhetes de identidade eletrónicos, como é o caso de Espanha[1181] e Portugal, que possuem instrumentos de criação de assinaturas eletrónicas incorporados.[1182] Essa solução revela-se adequada porque concentra num único instrumento a identificação tanto física como eletrónica, mas continuam as dificuldades na generalização da sua utilização como instrumento de identificação e de autenticação universal nos suportes eletrónicos. Essa dificuldade advém também do facto de a utilização do cartão do cidadão ou dos bilhetes de identidade eletrónicos só ser possível mediante a utilização de um leitor associado aos

[1177] Esse fracasso relativamente às expectativas era reconhecido num relatório da CE de 2006. *"Havia alguma esperança de que a adopção da Directiva ajudasse o mercado das assinaturas eletrónicas a arrancar"* E mais adiante, *"Não existe explicação simples para o facto de o mercado das assinaturas eletrónicas não se ter desenvolvido mais rapidamente"*. COM(2006) 120 final.

[1178] O reconhecimento da segurança das assinaturas assimétricas é pacífico, sendo relevado pelas organizações internacionais de forma pacífica. *"As assinaturas digitais baseadas na criptografia de chaves públicas são actualmente a forma mais reconhecida de assinatura eletrónica"*.COM(1998) 297 final, pág. 10.

[1179] A proliferação das senhas de acesso como instrumento de identificação e de autenticação predominante nas práticas comerciais pelos agentes económicos e pelas administrações públicas era reconhecido em 2010 pela CE, reconhecendo implicitamente o relativo fracasso das assinaturas digitais, no Programa da Agenda Digital: *"Actualmente, o meio mais comum de autenticar consiste na utilização de senhas (passwords). Para muitas aplicações, as senhas podem ser suficientes, mas são cada vez mais necessárias soluções mais seguras"*. COM(2010)245 final, pág. 12.

[1180] Com se refere no mesmo relatório, *"A falta de interoperabilidade técnica a nível nacional e transfronteiras é outro obstáculo à aceitação das assinaturas eletrónicas no mercado, tendo dado origem a muitas ilhas "isoladas" de aplicações de assinatura eletrónica em que os certificados só podem ser utilizados numa única aplicação"*. COM(2006) 120 final, pág. 8.

[1181] O *Documento Nacional de Identidad Electrónico* foi criado pelo Real Decreto 1553/2005, de 23 de diciembre e contém um certificado de assinatura eletrónica inserido no respetivo cartão.

[1182] A Lei n.º 7/2007, de 5/2, que cria o Cartão do cidadão, estabelece que ele contém, nos termos do artigo 18.º, um certificado de assinatura eletrónica e um certificado de autenticação, que permite ao seu titular autenticar-se perante os sítios web que aceitem o cartão do cidadão como instrumento de identificação eletrónica, bem como assinar com assinatura eletrónica qualificada quaisquer documentos eletrónicos.

computadores, que permita aos sistemas informáticos interagirem com os dados do cartão, sendo necessário ultrapassar esse constrangimento. [1183]

É também relevante o constrangimento que resulta do custo associado à obtenção de um dispositivo de assinatura eletrónica qualificada, adicionado pelo facto de necessitar de renovação periódica. Esse fato, associado á gratuitidade das palavras-passe e à desnecessidade da sua renovação, tem impedido a expansão da utilização das assinaturas qualificadas.

Resultam também dificuldades do facto de também no que respeita aos instrumentos de identificação tradicional existir uma multiplicidade de sistemas de identificação, como analisamos de seguida.

4.4. – Crítica e limitações

O regime de interoperabilidade e reconhecimento mútuo tem por objeto a identificação e a autenticação eletrónicas. Essas funções servem apenas para que as partes se conheçam através dos meios eletrónicos e que se assegurem da sua identidade. Esse conhecimento serve para adquirir segurança acerca de quem demanda um serviço eletrónico e para conhecer a legitimidade desse utilizador para a ele aceder.

O acesso não implica necessariamente a prestação do serviço nem sequer o direito a ela. Serve apenas para identificar o utilizador que demanda o serviço. Saber se a pessoa que demanda o serviço tem a legitimidade ou o direito a aceder a ele é já uma questão do domínio da relação jurídica eventualmente existente, ou não, entre as partes.[1184] A identificação eletrónica confere apenas conhecimento e segurança acerca da identidade do utilizador que demanda o sistema eletrónico. Esse procedimento é prévio, mas é separado da avaliação acerca da sua legitimidade para receberem os serviços que demandam ou acederem à informação que pretendem.

[1183] Outra forma de ultrapassar a situação atual, em que uma mesma pessoa necessita de possuir vários modos de autenticação em cada serviço que utiliza, seria a da criação de um sistema de interoperabilidade desses sistemas. Nesse sentido foi criada em Portugal a chamada Chave Móvel Digital (CMD), pela Lei n.º 37/2014, de 26/6 e regulamentada pela Portaria n.º 189/2014, de 23/9. Uma mesma pessoa pode utilizar um único instrumento para se autenticar em diversos serviços eletrónicos públicos. Este sistema revela-se, porém, inseguro, dado que a lei prevê que essa senha seja emitida para o telefone móvel do requerente.

[1184] Essa ressalva é também expressa nos considerandos do Regulamento: "*O acesso a esses serviços em linha e a sua prestação final ao requerente deverão estar estrei-tamente ligados ao direito a beneficiar de tais serviços nas condições estabelecidas pela legislação nacional*" (ponto 14).

O sistema de interoperabilidade que o Regulamento EIDAS institui ao nível europeu surge num contexto em que existe uma vasta multiplicidade de sistemas de identificação. À medida que foram disponibilizando serviços eletrónicos e em face da inexistência de sistemas e serviços autónomos de identificação eletrónica, os organismos públicos criaram os seus próprios meios, o que conduziu à atual proliferação. O Regulamento EIDAS vem qualificar juridicamente o nível de garantia desses sistemas e conferir-lhe relevância jurídica.

Mas muito antes da criação dos meios de identificação eletrónica, os organismos públicos e as empresas privadas já haviam sentido a necessidade de criar meios de identificação próprios. Isso ocorreu antes da emergência do estado tecnológico que permitiu a disponibilização de serviços eletrónicos em linha, quando começaram a ser utilizados programas informáticos nas suas operações internas, por essas entidades, para cumprirem a sua missão.

O tratamento informatizado de dados, quando envolvem uma elevada quantidade de pessoas, sejam elas clientes, fornecedores ou administrados, pressupõem que a identificação dessas pessoas seja efetuada com referenciais numéricos, que permitam aos sistemas informáticos efetuar os tratamentos de agregação e referenciação desses dados relativamente às pessoas a quem respeitam. Essa necessidade é muito anterior à disponibilização de serviços eletrónicos em linha e de comunicação entre essas entidades e essas pessoas. Ela ocorreu quando aquelas entidades começaram a ter necessidade de utilizar sistemas informáticos para as suas operações internas.

Estão nesta situação, por exemplo, os sistemas de identificação fiscal e do sistema de identificação da Segurança Social em Portugal. Estes sistemas necessitam de operar sobre uma base de identificação numérica dos agentes económicos e cidadãos que são seus contribuintes. Nestes casos, as respetivas administrações públicas já haviam tido a necessidade de desenvolver sistemas de identificação específicos, que lhe permitissem digitar a identidade dos respetivos contribuintes e beneficiários, de modo a poderem efetuar tratamentos massivos de informação que lhes respeite. Por exemplo, a administração tributária recolhe dados relativos ao rendimento e à riqueza dos sujeitos passivos de impostos e necessita de os agregar por referência à identidade do respetivo titular, sendo que essa identidade é representada nos sistemas informáticos que efetuam esse tratamento de dados, de forma numérica. Para isso é necessário que seja efetuada a identificação desses sujeitos passivos e a criação de um referencial numérico, que em

Portugal é o Número de Identificação Fiscal (NIF), que representa a identidade dos sujeitos passivos.

No nosso país o NIF é o instrumento de subjetivização do sistema, dos dados que a administração tributária recolhe, dispõe e trata, e mediante o qual os respetivos sistemas informáticos os agregam relativamente a cada contribuinte. Para isso a administração tributária possui um cadastro de contribuintes, contendo a sua identificação associada a um código numérico que é o NIF. A existência de NIF é uma obrigação de todos os sujeitos passivos de impostos em Portugal, nos termos do artigo 3.º do Decreto-Lei n.º 14/2013 de 28/01. Essa obrigação surgiu pela primeira vez no sistema fiscal português em 1979, como resposta a uma necessidade de tratamento dos dados fiscais dos sujeitos passivos de impostos, quando se iniciaram os primeiros tratamentos informatizados.[1185]

O NIF é um instrumento de identificação e a sua criação depende da prévia identificação e autenticação presencial dos respetivos elementos da identificação civil ou comercial de cada sujeito passivo.[1186]

A obrigação da existência do NIF emerge assim, diretamente, do estabelecimento de uma relação jurídica tributária, pelo que se tata de uma obrigação de natureza fiscal, e não apenas de um meio de identificação.

A partir do NIF a administração tributária constituiu um sistema de identificação eletrónica próprio, que serve para que os sujeitos passivos possam aceder, por via eletrónica, aos seus dados fiscais, bem como a outros serviços, como é o caso do cumprimento de obrigações fiscais.

Ora, se para se aceder a esses serviços eletrónicos é necessária a prévia existência do NIF e a obtenção deste exige a prévia identificação e autenticação de cada sujeito passivo, e essa função se cumpre, na sua base, com a sua presença física, frustra-

[1185] O NIF foi instituído pelo Decreto-Lei n.º 463/79, de 30 /11 e tinha como objetivo a "*rápida e correcta identificação do contribuinte, um contrôle eficaz do cumprimento dos respectivos deveres tributários, uma maior eficiência administrativa permissiva de um mais fácil e melhor contacto com aquele*", bem como "*dotar a administração fiscal de um meio indispensável à consecução de qualquer política fiscal que passe pelo combate frontal à evasão fiscal*" (preâmbulo do diploma legal). Este modelo de autenticação está atualmente vigente, nos termos do n.º 2 do artigo 8.º do Decreto-Lei n.º 14/2013 de 28/01: "*A verificação da fidedignidade dos elementos identificativos declarados deve ser feita pelo serviço recetor, por cotejo dos dados constantes no documento identificativo do interessado*".

[1186] O artigo 4.º do Decreto-Lei n.º 463/79, de 30/11, obrigava a essa identificação e autenticação presencial, por funcionário competente, mediante a invocação de uma identificação pelos sujeitos passivos através do preenchimento de uma ficha e o "*confronto do teor das declarações constantes da ficha, com o bilhete de identidade, cartão de eleitor ou qualquer outro documento ou certidão relativos aos dados declarados pelo contribuinte cuja comprovação for exigida pela Direcção-Geral das Contribuições e Impostos*".

se um dos objetivos do Regulamento EIDAS, que é exatamente o de evitar a repetição dessas diligências.

Por outro lado, sempre que um cidadão de outro Estado Membro pretenda cumprir uma obrigação fiscal em Portugal por via eletrónica, não o poderá fazer, nos termos da lei atualmente em vigor no nosso país, porque terá que previamente cumprir a obrigação fiscal de obter o NIF, o que, por sua vez, exige a sua presença física ou do seu representante legal, para os procedimentos de identificação e autenticação, nos termos do artigo 10.º do Decreto-Lei n.º 14/2013 de 28/01.

Embora os sujeitos passivos de impostos em Portugal que possuam meios de identificação eletrónica produzidos noutros Estados sejam titulares de um direito a utilizá-los perante os organismos administrativos em Portugal, esse direito de pouco serve se para isso for necessária a existência de NIF e se a sua obtenção exigir a sua prévia identificação e autenticação mediante a presença física.

Coloca-se então a questão da existência de um eventual conflito entre ambos os regimes. Esse conflito é particularmente intenso nos casos em que um titular de um meio de identificação eletrónica produzido noutro Estado Membro se apresenta perante o Portal das Finanças e pretende utilizá-lo para cumprir a obrigação fiscal de criar um NIF. Isso acontecerá, por exemplo, quando um cidadão de outro Estado Membro pretende adquirir um imóvel em Portugal e para isso necessita de pagar o Imposto Municipal Sobre a Transmissão Onerosa de Imoveis (IMT) através do serviço eletrónico. Nos termos da norma antes referida, deverá previamente obter o NIF e para isto deve identificar-se pessoalmente ou mediante representante, através de presença física e da exibição dos elementos de identificação física correspondentes.

A existência de NIF e a sua exibição são indispensáveis ao cumprimento de todas as obrigações fiscais, como estabelece o artigo 29.º do Decreto-Lei n.º 14/2013 de 28/01, estabelecendo o artigo 31.º que devem ser recusados e considerados como não apresentados todos os requerimentos ou documentos apresentados perante órgãos da administração tributária quando não acompanhados do NIF.

É verdade que depois de cumprida a obrigação fiscal de possuir NIF, podem os sujeitos passivos aceder aos serviços eletrónicos da administração tributária mediante o sistema de interoperabilidade criado pelo Regulamento EIDAS, mas coloca-se a questão de saber se as normas de criação do NIF, sendo essenciais à identificação eletrónica, não violam o princípio do reconhecimento mútuo.

Na verdade, o Regulamento de Execução (UE) 2015/1501 estabelece que, para os efeitos da identificação eletrónica, se consideram dispensáveis os procedimentos de identificação e de autenticação mediante presença física dos interessados, sempre que tenham sido adotados para os efeitos de criação de um meio de identificação, eletrónica ou não, já existente (ponto 2.1.2) do Anexo.

Daqui resulta que os requisitos legais nacionais que regulam a criação do NIF podem conflituar com aquelas normas e com o princípio do reconhecimento mútuo, dado que os procedimentos de criação do NIF repetem os procedimentos de criação de meios de identificação eletrónica de que o interessado seja já titular.

Ao mesmo tempo, a administração tributária portuguesa passará a poder aceder a todos os elementos necessários à criação do NIF com um nível de segurança, que pelo menos é igual ao que é estabelecido na lei portuguesa, mediante a obtenção dos dados de identificação e da sua autenticação, a que tem acesso no quadro da interoperabilidade estabelecido pelo Regulamento EIDAS. Assim, as normas relativas a criação do NIF, constantes do Decreto-Lei n.º 14/2013 de 28/01, devem considerar-se derrogadas pelo regime do Regulamento EIDAS, no que respeita às exigências de identificação e de autenticação do sujeito passivo. Não conflitua com o Regulamento EIDAS a obrigação tributária de criação do NIF, porque se trata de uma obrigação tributária emergente da relação jurídica tributária que se estabelece entre o Estado português e os sujeitos passivos de imposto, mas conflituam as normas que impedem a identificação e autenticação eletrónica de sujeitos passivos que não possuam NIF. Desta forma deverá entender-se, do nosso ponto de vista, que a administração tributária deve disponibilizar aos sujeitos passivos que possuam meios de identificação eletrónica, a possibilidade de se identificarem com esses meios perante o seu serviço eletrónico, permitindo-lhes, de seguida, cumprirem a obrigação fiscal da obtenção do NIF por essa via, sendo que os elementos para essa obtenção podem ser obtidos através do sistema de interoperabilidade, no momento da autenticação da identificação.

As considerações que anteriormente efetuámos aplicam-se, de forma correspondente, aos restantes organismos administrativos, que possuem sistemas de identificação próprios.

Resultará destas considerações a desnecessidade da existência do NIF e de elementos de identificação correspondentes? Entendemos que não, que esses elementos serão sempre indispensáveis para o funcionamento dos serviços da administração pública mediante sistemas informáticos. Mas essa necessidade não pode contender com

o princípio da interoperabilidade e do reconhecimento mútuo. E para isso é necessário que a lei reguladora da atribuição do NIF e dos elementos correspondentes de identificação, bem como os órgãos competentes para a sua administração, implementem mecanismos de correspondência que permitam a criação do NIF a partir dos elementos constantes do meio de identificação eletrónica que os sujeitos passivos queiram utilizar. E é necessário ainda que seja estabelecida uma conexão lógica e unívoca entre esses meios e o NIF.

Finalmente, esses princípios devem também ser assegurados aos cidadãos nacionais que possuam outros meios de identificação eletrónica.

5. A entrada em vigor do Regulamento EIDAS e o regime transitório

O Regulamento EIDAS aplica-se, genericamente, a partir de 1 de julho de 2016, em conformidade com o previsto no n.º 2 do artigo 52.º. Nesse mesmo dia fica revogada a Diretiva 1999/93/CE. Analisamos os efeitos desta transição, nos que respeita ao direito interno português e aos seguintes tópicos:

5.1. – Os prestadores qualificados de serviços de confiança

O Regulamento EIDAS cria, pela primeira vez o estatuto dos prestadores qualificados de serviços de confiança. Essa classificação depende de reconhecimento prévio pelas entidades de supervisão, nos termos da alínea g) do n.º 4 do artigo 17.º, sendo que só esses prestadores de serviços podem gerar certificados e dispositivos de criação de assinaturas eletrónicas qualificadas.

No regime do Decreto-Lei n.º 290-D/99, de 2 de agosto, com as alterações do Decreto-Lei n.º 88/2009, de 9 de abril, não existia esse estatuto, sendo que as assinaturas eletrónicas eram consideradas como qualificadas, nos casos em que se baseassem num certificado qualificado e se fossem criadas através de um dispositivo seguro de criação de assinatura. Dado o princípio da liberdade de acesso às atividades de certificação, consagrado no artigo 9.º, bastava que os prestadores de serviços

criassem os dispositivos e os certificados em conformidade com os requisitos, respetivamente da alínea j) do artigo 2.º e do artigo 29.º, para que as assinaturas fossem consideradas como qualificadas.

O Decreto-Lei n.º 290-D/99, de 2 de agosto, previa a possibilidade de um reconhecimento dos prestadores de serviços que emitiam certificados qualificados, mediante credenciação, mas tratava-se de um mecanismo meramente voluntário (n.º 1 do artigo 9.º), apesar da obrigatoriedade de inscrição no registo na entidade credenciadora, de todos os prestadores de serviços que gerassem certificados qualificados.

Este regime cessou em 1 de julho de 2016. A partir dessa data, os prestadores de serviços de confiança que emitem certificados qualificados podem passar a ser considerados como prestadores qualificados de serviços de confiança nos termos previstos no Regulamento. Porém, essa qualificação depende da avaliação positiva, feita pela entidade supervisora, de que cumprem todos os requisitos que o Regulamento estabelece. Essa avaliação será feita a partir de um relatório de avaliação de conformidade cada prestador de serviços terá que entregar à entidade supervisora, até ao dia 1 de julho de 2017, nos termos do n.º 3 do artigo 51.º do Regulamento. Enquanto essa avaliação não estiver concluída, essas entidades são consideradas, provisoriamente como prestadores qualificados.

Deixam, porém, de ser considerados prestadores qualificados, a partir de 2 de julho de 2017, aqueles que não entreguem o referido relatório de avaliação no prazo antes referido (n.º 4 do artigo 51.º 1 do Regulamento).

Embora o Regulamento não o enuncie expressamente, a partir de 1 de julho de 2016, todos os prestadores qualificados passam a estar sujeitos à disciplina e ao controlo das entidades de supervisão, incluindo aqueles que o regulamento considera assim considera transitoriamente, até que esteja concluída a avaliação do respetivo relatório de avaliação de conformidade. Esse relatório deve considerar-se que substitui as auditorias que devem ser efetuadas nos termos do n.º 1 do artigo 20.º do Regulamento.

Embora o artigo 51.º não o preveja expressamente, logo que a entidade de supervisão conclua a avaliação do relatório de forma positiva, deve promover a sua publicação nas listas de confiança a que se refere o n.º 1 do artigo 22.º, nos termos do n.º 3 do artigo 21.º

5.2. – As assinaturas eletrónicas qualificadas

A partir do dia 1 de julho de 2016, só são consideradas qualificadas as assinaturas eletrónicas baseadas em certificados qualificados e criadas por dispositivos qualificados de assinatura eletrónica, como estabelece o n.º 2 do artigo 52.º do Regulamento EIDAS.

Os certificados qualificados só podem ser gerados por prestadores qualificados de serviços de confiança (alínea b) do anexo I) e os dispositivos qualificados necessitam de ser previamente certificados (artigo 30.º) por uma entidade pública ou privada designada pelo Estado.

A partir de 1 de julho de 2016, só são qualificados os prestadores de serviços a quem tenha sido atribuído o estatuto de qualificado, nos termos do Regulamento, só eles podendo gerar certificados qualificados de assinatura eletrónica.

Em consequência, nenhum dos certificados qualificados emitidos em conformidade com a Diretiva cumpre os requisitos do Regulamento, dado que não existia o estatuto de prestador qualificado.

Apesar disso, o Regulamento cria um regime transitório, estabelecendo que esses certificados se consideram certificados qualificados nos termos do Regulamento, considerando-se as respetivas assinaturas eletrónicas como qualificadas, nos termos do n.º 2 do artigo 52.º.

Ao mesmo tempo, os dispositivos seguros de criação de assinaturas passam a ser considerados como qualificados, em face do disposto no n.º 1 do artigo 51.º.

Porém, a qualificação como qualificados nos termos do Regulamento cessa quando caducarem os certificados. Assim, caso os respetivos signatários pretendam manter um dispositivo de assinatura eletrónica, terão que o adquirir já de acordo com o regime do Regulamento.

Durante um período transitório, após 1 de julho de 2016, o n.º 3 do artigo 52.º qualifica os prestadores de serviços que emitam certificados qualificados nos termos da Diretiva de 1999, como sendo prestadores qualificados à luz do Regulamento. Essa qualificação é transitória e caduca com a avaliação, pela entidade de supervisão, do relatório de avaliação de conformidade que esses prestadores de serviços devem apresentar até, no máximo, 1 de julho de 2017.

A questão que se coloca é a de saber se durante esse período, considerando-se estes prestadores como qualificados nos termos do Regulamento, podem emitir

certificados qualificados, nos termos do Regulamento. Em princípio não deviam poder, dado que, na verdade, eles não possuem o reconhecimento do estatuto de prestadores qualificados, que lhe é atribuído pela entidade de supervisão. É certo que possuem esse estatuto, mas ele deriva apenas do Regulamento e não da atribuição nos termos normais previstos no próprio Regulamento.

No entanto, a circunstância de eles possuírem esse estatuto, confere-lhe todos os direito que o Regulamento estabelece para esse tipo de prestadores de serviços, pelo que se terá que considerar que podem emitir certificados, que se considerarão como qualificados, com base no regime do regulamento. A essa conclusão chegamos também pelo facto de o teor literal do n.º 3 do artigo 51.º os considerar como "*prestadores qualificados de serviços de confiança na aceção do presente regulamento*", ou seja, considerando-os como tal para todos os efeitos do Regulamento.

A partir de 2 de julho de 2017 perdem o estatuto de prestadores qualificados aqueles que emitiam certificados qualificados nos termos da Diretiva de 1999 e não entregarem o relatório até ao dia anterior. Perdem-no também aqueles cuja avaliação pela entidade de supervisão for negativa, a partir da data da conclusão da avaliação. Nesses casos esses prestadores deixarão de poder emitir certificados qualificados.

Desta forma, as assinaturas eletrónicas qualificadas, nos termos do Decreto-Lei n.º 290-D/99, de 2 de agosto, são também consideradas como qualificadas, nos termos do Regulamento, mas apenas até caducarem os respetivos certificados.

5.3. – Os certificados eletrónicos de assinatura eletrónica atribuídos a pessoas coletivas

Os certificados qualificados de assinatura eletrónica de pessoas coletivas caducam na data de 1 de julho de 2016, bem como os restantes certificados, dado que a assinatura eletrónica passa a existir apenas para pessoas singulares. O Regulamento não estabelece nenhum regime transitório para este tipo de assinaturas eletrónicas, pelo que, sendo revogada a diretiva de 1999 e estabelecendo o n.º 2 do artigo 50.º que todas as referências a essa diretiva passam a ser consideradas como reportadas ao Regulamento, então os certificados de assinatura de pessoas coletivas passam a estar em desconformidade com o Regulamento e se consideram sem efeito a partir da sua entrada em vigor.

A partir dessa data o modo de autenticação dos documentos emitidos por pessoas coletivas são os selos eletrónicos.

5.4. Os dispositivos certificados de assinatura eletrónica

Relativamente aos dispositivos seguros de assinaturas eletrónicas produzidos com base na Diretiva e existentes à data de 1 de julho de 2016, passam a considerar-se dispositivos qualificados nos termos do Regulamento, como estabelece o n.º 1 do artigo 51.º do Regulamento. O Regulamento assume esses dispositivos como válidos para os seus fins, sem qualquer limitação.

5.5. – As listas de confiança

O Regulamento prevê a existência de duas listas de confiança em matéria de assinaturas eletrónicas:

i) Relativas aos prestadores qualificados de serviços de confiança n.º 1 do artigo 22.º), publicada pelos Estados Membros;

ii) De dispositivos qualificados e certificados de criação de assinatura eletrónica, nos termos do n.º 2 do artigo 31.º, publicada pela Comissão Europeia, incluindo a lista de dispositivos qualificados e certificados de criação de selo eletrónico (n.º 3 do artigo 39.º).

Estas listas devem ser publicadas a partir da data da aplicação do Regulamento, em 1 de julho de 2016, e embora o Regulamento não estabeleça essa obrigatoriedade, ela resulta da necessidade de estarem disponíveis a partir da data da entrada em vigor do sistema de interoperabilidade das assinaturas eletrónicas.

A Comissão Europeia publicou, em 8 de setembro de 2015, as especificações técnicas e os formatos a que devem obedecer essas listas, devendo os Estados Membros publicitá-las a partir da respetiva entrada em vigor.[1187] Essas listas podem conter a identificação dos prestadores qualificados e também prestadores não qualificados, deve

[1187] Decisão de Execução (EU) 2015/1505 da Comissão, de 8 de setembro de 2015, que entrou em vigor em 28 de setembro de 2015, como estabelece o seu artigo 5.º.

que seja feita menção de não serem qualificados nos termos do Regulamento EIDAS.[1188]

5.6. – Interoperabilidade

A interoperabilidade das assinaturas e dos selos eletrónicos é uma das preocupações do Regulamento EIDAS, tal como o é também para a identificação eletrónica, como analisámos no Capítulo V da Parte II.

Para isso torna-se obrigatório que os certificados qualificados de assinatura eletrónica contenham uma indicação, adequada ao tratamento automático, de que o certificado foi emitido como qualificado (alínea a) do anexo I aplicável também aos certificados de selos eletrónicos, nos termos da alínea a) do AnexoIII).

Por outro lado as listas publicadas devem ser adequadas ao tratamento automatizado, tendo em vista permitir uma maior interoperabilidade, nomeadamente no que respeita à verificação das assinaturas eletrónicas (parte final do n.º 4 do artigo 22.º).

Desta forma, e tendo em vista a operacionalidade do sistema em 1 de julho de 2016, essas listas devem cumprir esses requisitos.

5.7. – Revogação do Decreto-Lei n.º 290-D/99, de 4 de agosto.

Este conjunto de normas transitórias levanta algumas questões que devemos analisar. A primeira é a de saber a legislação interna dos Estados Membros, em matéria de assinatura eletrónica se considera revogada com a revogação da diretiva, operada a partir de 1 de julho de 2016, pelo n.º 1 do artigo 50.º do Regulamento. O Regulamento estabelece um regime das assinaturas eletrónicas qualificadas que podemos considerar fechado, porque fá-lo depender da qualificação dos prestadores de serviços e essa qualificação depende de um ato de reconhecimento que é de carácter público. Essa qualificação é essencial para o reconhecimento dessas assinaturas, automático e imperativo, em todos os Estados Membros. Por essa razão, a partir de 1 de julho de 2016, só são consideradas qualificadas as assinaturas baseadas em certificados qualificados emitidos nos termos do regime anterior ao Regulamento, enquanto os

[1188] Em Portugal essa lista está disponível em https://www.gns.gov.pt/trusted-lists.aspx (última consulta efetuada em 2017/07/04).

certificados forem válidos. Logo que caduquem, nos termos que anteriormente analisámos, deixam de existir assinaturas eletrónicas qualificadas cujos certificados e dispositivos não tenham sido produzidos com base no Regulamento.

A outra questão é a de saber se os Estados Membros podem estabelecer normas próprias de reconhecimento do estatuto de prestadores qualificados de serviços de confiança ou de credenciação de prestadores de serviços que possam emitir certificados qualificados. A resposta é claramente negativa, nos casos em que essas normas não cumpram estritamente os termos do Regulamento. Desta forma, entendem-se como revogados os regimes de credenciação dos artigos 9.º a 36.º do Decreto-Lei n.º 290-D/99, de 4 de agosto, por colidirem com as normas do regulamento, que é diretamente aplicável no direito interno português. Do mesmo modo se considera revogado o correspondente regime sancionatório previsto no mesmo diploma legal, dado que a descrição dos tipos legais de contraordenação tem por base a legislação revogada.

A outra questão que se coloca é a da validade das assinaturas baseadas em certificados qualificados produzidos com base na legislação anterior ao Regulamento, enquanto não caducarem, mas cujos prestadores de confiança que os produziram não entregaram o relatório de avaliação de conformidade e deixaram de ser considerados como qualificados a partir de 2/7/2017. Consideramos que, nesse caso, o n.º 2 do artigo 51.º do Regulamento é norma especial, e que, por essa razão, mantêm-se como certificados qualificados até caducarem.

Das restantes normas do Decreto-Lei n.º 290-D/99, de 4 de agosto, devem considerar-se revogadas as relativas às definições, por colidirem com as do regulamento, bem como os artigos 7.º e 8.º que regulam a assinatura eletrónica qualificada e a obtenção dos dados de criação de assinatura, respetivamente, por se tratar de matéria também prevista no Regulamento.

Entendemos que será mais duvidosa a eventual vigência dos artigos 3.º a 6.º, pelo que se justifica uma análise mais pormenorizada:

i) No que respeita à força probatória dos documentos, a atribuição do efeito probatório constante do artigo 3.º não colide com o disposto no artigo 40.º e no artigo 25.º do Regulamento, especificando o seu sentido, mas reportam-se a tipos de assinaturas que passaram a ser inexistentes após a entrada em vigor do Regulamento, pelo que se devem considerar também revogado este artigo;

i) Entendemos que se mantém em vigor o artigo 4.º, porque se trata de norma relativa ao efeito probatório dos documentos eletrónicos, como norma de direito interno, e que não colide com as normas do Regulamento. Na verdade trata-se de equiparar as cópias de documentos eletrónicos a cópias de outros tipos de documentos, para fins probatórios, e isso não colide, com o disposto no artigo 46.º do Regulamento;

ii) O artigo 5.º admite a possibilidade de as entidades públicas emitirem documentos eletrónicos, desde que autenticados com assinatura eletrónica qualificada, mas esta norma parece-nos que colide com o disposto no artigo 27.º do Regulamento, dado que este admite a possibilidade da existência de documentos eletrónicos autenticados com assinatura eletrónica avançada nos serviços públicos, pelo que o devemos também considerar revogado o n.º 1 do artigo 5.º do Decreto-Lei n.º 290-D/99, de 4 de agosto. Entendemos também que o n. 2 se deve considerar em vigor, dado que se trata de norma relativa ao conteúdo dos documentos eletrónicos emitidos em procedimentos administrativos, que em nada colidem com o disposto no Regulamento;

iii) O regime de comunicações eletrónicas constante do artigo 6.º regula sobre a mesma matéria dos artigos 43.º e 44.º do Regulamento, pelo que se terá que considerar também revogado. Na verdade, o artigo 43.º estabelece no n.º 1 o princípio da equivalência do envio registado eletrónico, relativamente às comunicações em meios tradicionais. Esta equiparação corresponde à que consta do n.º 1 do artigo 6.º, sendo que esta é mais limitativa porque faz depender a sua validade da existência de acordo prévio das partes. O n.º 2 estabelece uma presunção de integridade, envie de receção, bem como da data e hora, nos casos em que se trate de um serviço qualificado de envio registado eletrónico, que revoga os n.ºs 3 e 4 do artigo 6.º do Decreto-Lei n.º 290-D/99, de 4 de agosto.

5.8. – Entrada em vigor do regime da identificação eletrónica

O regime da identificação eletrónica do Regulamento EIDAS só estará plenamente em vigor em 29 de setembro de 2018, ou seja, 3 anos depois da aplicação do Regulamento de Execução 2015/1502, de 8 de setembro, cuja entrada em vigor ocorreu no dia 29 de setembro de 2015, como estabelece a alínea c) do n.º 2 do artigo 52.º do Regulamento EIDAS.

Os três anos de vigência do Regulamento de Execução, antes da entrada em vigor do sistema, são os necessários para se completarem as quatro fases do procedimento de reconhecimento pelos Estados Membros dos meios de identificação eletrónica. Para isso entraram em vigor, logo em 17 de setembro de 2014, as normas que obrigam a Comissão a publicar os Regulamentos de Execução e, em simultâneo com as aplicação desses regulamentos, as normas que regulam os procedimentos de notificação dos sistemas produtores de meios de identificação, da sua publicação e do reconhecimento (n.º 2 do artigo 52.º do Regulamento EIDAS.

A entrada em vigor do sistema do reconhecimento mútuo corresponde ao início da efetividade do direito à utilização transnacional dos meios de identificação eletrónica pelas pessoas singulares e coletivas da União Europeia. Essa efetividade implica que até essa data todos os Estados Membros tenham executados os procedimentos necessários para que a interoperabilidade prevista no regime, dos sistemas eletrónicos dos organismos públicos e das entidades produtoras de meios de identificação eletrónicos seja efetiva.

Conclusões

Em face da investigação que efetuámos e que acabamos de apresentar propomo-nos apresentar as seguintes conclusões:

1. No paradigma do papel a assinatura manuscrita tem como funções fundamentais a identificação do seu autor e a sua vinculação a um documento. Trata-se de uma entidade relacional e transitiva, que se situa entre uma pessoa e um documento, vinculando-os;
2. A identificação do autor é sempre efetuada por reporte a dados gerados por entidades terceiras, competentes para a identificação civil;
3. Existem vários tipos de assinatura manual, com eficácia vinculativa diferenciada;
4. Os suportes eletrónicos, que passaram a ser alternativa ao papel como suporte documental, assentam na linguagem binária, que tem na sua base apenas dois dígitos, de um e zero, também designados bites. Essa linguagem funda-se na filosofia da Lógica Matemática de Leibniz e seus discípulos, que fizeram corresponder as proposições lógicas a impulsos elétricos, correspondendo a passagem de energia ao dígito 1 e o seu impedimento ao dígito zero, nascendo assim a linguagem digital;

5. A possibilidade de converter os suportes escritos, o som e a imagem na linguagem digital fez emergir os suportes eletrónicos como alternativa ao papel;
6. A possibilidade de ligação de computadores por linha telefónica, através da qual circulam sequências de bites, de forma não hierarquizada e não centralizada, deu origem à Internet, a rede das redes, acessível de forma cada vez mais generalizada e capaz de fazer circular todos os tipos de informação e de conhecimento, com elevada rapidez e acessibilidade generalizada;
7. A utilização dos suportes eletrónicos na atividade económica expandiu-se com a tecnologia EDI que, mediante mensagens *standardizadas* permite a comunicação sistemática de declarações negociais entre os sistemas das empresas, o que permite também o seu tratamento automatizado;
8. O EDI é uma rede fechada de comunicações eletrónicas entre duas ou mais empresas que através dela ligam os seus sistemas informáticos, mediante convenção prévia de troca de mensagens;
9. Foi a generalização da utilização do EDI pelas empresas na comunicação de declarações negociais que fez emergir o direito da segurança jurídica na utilização dos meios eletrónicos;
10. A utilização do EDI na atividade económica exigia o reconhecimento da validade e eficácia jurídica das mensagens eletrónicas, a sua admissibilidade como instrumento de prova, a sua equiparação a documentos escrito e a originais, e a questão do seu arquivo. A metodologia jurídica utilizada foi a aplicação do princípio da equivalência funcional, nos termos da qual, cumpridos que sejam os correspondentes requisitos, os suportes eletrónicos possuem a mesma validade e eficácia do papel na documentação das relações jurídicas;
11. O primeiro critério de equivalência era o da prevalência da autonomia contratual na determinação do modo de autenticação das mensagens eletrónicas trocadas pelas partes, o que resolvia o problema da idoneidade jurídica das mensagens EDI, dado que esta tecnologia pressupõe uma convenção prévia entre as partes;
12. A utilização da Internet na atividade económica trouxe problemas de insegurança, por se tratar de uma rede aberta, onde as partes podiam

estabelecer relações contratuais com pessoas que até aí não se conheciam mutuamente. Na Internet é fácil simular a identidade, os documentos e os sistemas, pelo que a insegurança dos suportes eletrónicos atinge a sua máxima dimensão;

13. O direito da assinatura eletrónica tem as suas origens nas convenções de autenticação nos mercados financeiros e dos transportes internacionais de mercadorias;
14. A assinatura digital é uma criação de juristas, matemáticos e informáticos, destinada a garantir a segurança jurídica nas transações em redes abertas e é o instrumento de juridificação da Internet e dos suportes eletrónicos;
15. A assinatura digital utiliza a criptografia, de forma inversa, não como instrumento de ocultação da informação, mas de vinculação segura de dados e entre dados e pessoas. A encriptação com uma chave privada serve para demonstrar que só a pessoa que a possui a podia ter feito. A desencriptação serve para constatar a vinculação de uma assinatura a um documento e a uma pessoa;
16. Para a segurança da assinatura digital foram decisivas as descobertas da criptografia das chaves assimétricas, que separa a chave de encriptação e a de desencriptação, permitindo a desencriptação sem necessidade de conhecimento da chave de encriptação, apesar de ambas as chaves estarem matematicamente relacionadas e não ser possível derivar a primeira a partir da segunda;
17. A impossibilidade desta derivação resulta do facto de se usarem algoritmos muito complexos, compostos por números primos. Para que essa complexidade não afete a necessidade de rapidez nas transações eletrónicas, as chaves privadas só se aplicam a um resumo dos documentos que é elaborado previamente mediante encriptação efetuada por uma chave simétrica. Esse resumo designa-se *hash*. É apenas sobre este resumo que se aplica a chave privada, fazendo uma segunda encriptação;
18. O objeto da assinatura eletrónica são os documentos eletrónicos, considerando-se estes como todos os conteúdos em suporte eletrónico, sejam eles texto, som, imagem ou outros. O conceito de documento eletrónico tem na sua génese as mensagens de EDI, mas é mais amplo que

elas, abrangendo mesmo os elementos de identificação de uma pessoa perante um sistema informático que necessitam de ser autenticados;

19. O conceito de documento eletrónico foi sendo progressivamente alargado e o Regulamento EIDAS adota a definição mais abrangente, correspondendo a qualquer conteúdo armazenado em formato eletrónico. Este conteúdo é suscetível de ser mais abrangente pelo facto de todas as relações estabelecidas por meios eletrónicos serem suportadas em dados, não existindo declarações verbais;
20. Os documentos eletrónicos não são objetos unos, como no papel, mas processos duais, onde se separa o suporte digital dos dados, da sua apresentação para análise num interface. O documento eletrónico não é nenhuma dessas dualidades, mas ambas em simultâneo;
21. As declarações negociais emitidas automaticamente por sistemas informáticos são sempre imputáveis ao titular do despectivo sistema uma vez que os equipamentos não possuem vontade e são apenas instrumentos, mais ou menos complexos, de ação humana;
22. Além da assinatura digital existem outros tipos de assinatura eletrónica, como é o caso da digitação do nome, da assinatura digitalizada, das palavras-chave e dos métodos biométricos.
23. Existem também vários níveis de segurança destes tipos de assinatura, desde as assinaturas avançadas às assinaturas qualificadas, correspondendo estas últimas ao mais elevado nível de segurança. O conceito de assinatura é anterior ao da sua eficácia probatória;
24. Os prestadores de serviços de confiança eletrónica desempenham o papel fundamental de fornecer o bem jurídico confiança, nomeadamente na criação e fornecimento de chaves e de dispositivos de assinatura, de identificação dos titulares, de garantia da conexão entre as chaves e os titulares e da relação matemática entre estas, bem como da sua segurança, e ainda de gestão do ciclo de vida útil dos certificados de assinatura eletrónica;
25. A assinatura eletrónica consiste em dados, porque são eles a substância dos suportes eletrónicos. Como os documentos eletrónicos são, na sua base essencial, dados, é sobre eles e não apenas sobre a sua apresentação nos interfaces legíveis que devem operar os mecanismos de vinculação, tendo

em conta que aquilo que os interfaces apresentam é determinado pelas sequências como estão organizados aqueles dados na sua base;

26. Os dados que consubstanciam a assinatura devem estar ligados aos dados que consubstanciam o objeto que ela autentica, sendo que essa ligação é de dois tipos – uma mera ligação entre eles ou uma conexão logica. A primeira é uma ligação qualquer, sem exigência nem condições.
27. Sendo a conexão lógica, a assinatura é o resultado de uma operação matemática que aplica uma chave privada, pessoal, única, exclusiva e irrepetível, sobre os dados do documento a assinar. Dessa operação resulta um produto composto por dados, com uma sequência também ela única, que vincula de forma segura a assinatura ao documento;
28. Quando existe segurança dos procedimentos de identificação do titular da chave privada, bem como da sua entrega e detenção, está garantida a conexão entre a chave e a pessoa que assina, pelo que se consuma também a vinculação entre a pessoa e o documento assinado. Essa segurança é dada pelos prestadores de serviços de confiança;
29. Qualquer pessoa pode verificar essa vinculação, utilizando uma chave pública que está matematicamente relacionada com a chave privada. Essa verificação é efetuada mediante a aplicação da chave pública sobre aquilo que a chave privada encriptou. Como só aquela pode desencriptar o que esta encriptou, e ambas as chaves estão matematicamente relacionadas, a operação de desencriptação revela qual foi a chave usada para encriptar. Estando essa chave associada a uma pessoa, consuma-se a constatação da vinculação dessa pessoa aos documentos;
30. A assinatura eletrónica qualificada é a que possui o mais elevado nível de eficácia jurídica vinculativa, por ser a que garante o mais elevado nível de segurança e cumpre requisitos legais substanciais e formais de segurança nos procedimentos de criação, identificação e gestão, bem como de credibilidade e reconhecimento dos prestadores de serviços de confiança que a asseguram;
31. A assinatura eletrónica qualificada cumpre os requisitos legais do mais elevado nível de segurança, equivalentes aos que a lei exige para as assinaturas manuais, garantindo-se assim uma equivalência plena entre as

assinaturas eletrónicas e todos os tipos de assinaturas manuais, mesmo as de maior exigência formal;

32. As assinaturas eletrónicas qualificadas caraterizam-se pelo controlo público que é exercido no que respeita ao conteúdo e aos procedimentos de geração dos certificados qualificados e dos dispositivos qualificados de criação de assinaturas eletrónicas, bem como na dependência do acesso à atividade de prestador qualificado de serviços de confiança do reconhecimento e do controlo sistemático da sua atividade;
33. O conceito de assinatura eletrónica evoluiu na legislação e na doutrina, sendo fundamentalmente um instrumento de identificação, de autenticação e de integridade, estabelecendo a vinculação de uma pessoa a um conteúdo em suporte eletrónico e não apenas de autoria e de aprovação;
34. Nas funções da assinatura eletrónica distinguem-se aquelas que são típicas da assinatura em geral daquelas que, não o sendo, são indispensáveis no paradigma eletrónico.
35. São típicas da assinatura as funções de identificação, autenticação, integridade e não repúdio na origem;
36. Não são típicas da assinatura as funções de confidencialidade e de não repúdio no destino;
37. A função de identificação é essencial à assinatura eletrónica e a identificação do assinante deve acompanhar sempre o objeto assinado. Sem ela não existe assinatura;
38. Nas redes abertas a função identificação é essencial em todas as transações com relevo jurídico, dado que as relações estabelecidas são sempre mediadas por máquinas e é necessária a identificação do autor das comunicações. A identificação é essencial no contexto eletrónico;
39. Enquanto no paradigma do papel a assinatura vincula pessoas a documentos, no contexto eletrónico ela é essencial para a identificação das partes em todas as transações;
40. A necessidade da identificação é mais intensa nas redes abertas, que se caraterizam pela necessidade do estabelecimento de relações jurídicas com pessoas anteriormente desconhecidas, que exigem identificação e vinculação jurídicas rápidas e eficazes, em face do próprio modo de funcionamento das relações em linha;

41. Embora a identificação eletrónica seja essencial à assinatura eletrónica, o inverso não é verdadeiro. Na verdade a identificação eletrónica é essencial para o direito de acesso a serviços eletrónicos disponibilizados quer pelas empresas quer pelas administrações públicas, caso em que a legitimidade depende da identificação. Nesses casos a identificação autonomiza-se da assinatura e não a substitui.
42. A identificação eletrónica pressupõe sempre o confronto entre dados que são fornecidos pela parte e dados gerados por entidades públicas ou terceiros de confiança;
43. A função de aprovação do conteúdo das mensagens comunicadas por meios eletrónicos não é essencial à assinatura eletrónica, dado que a vontade de vinculação que a assinatura exterioriza não abrange relativamente a um documento não revela necessariamente o acordo, ou não da pessoa, acerca do seu conteúdo;
44. A exigência de aprovação constava apenas das normas jurídicas concebidas no contexto do EDI e pretendiam vincar a vinculação subjetiva das mensagens eletrónicas, mesmo quando emitidas por sistemas automatizados mediante programação;
45. A exigência de aprovação deixou de fazer parte da legislação logo que se formou o conceito de assinatura eletrónica, dado o poder de vinculação desta;
46. Integra o conceito de assinatura a vontade do assinante, de se vincular a um documento, mas essa vontade é diferente da avaliação do entendimento que ele adota acerca do seu conteúdo;
47. A assinatura é sempre um ato de vontade de vinculação, que se pressupõe consciente e livre;
48. A função autenticação revela a origem pessoal de um documento ou de uma assinatura. Trata-se de uma função essencial à assinatura, que no paradigma eletrónico adquire maior importância por as relações serem sempre mediadas por máquinas, bem como pelo facto de a vinculação, para ser eficaz, necessitar de ir além dos interfaces com que os documentos se apresentam ao entendimento humano, assentando sobre os próprios dados de suporte;

49. É a função autenticação que estabelece o nexo de vinculação jurídica entre quem assina e o documento assinado. Esse nexo, sendo expresso pela assinatura, que o manifesta, revela a origem do documento e funda o vínculo jurídico entre a pessoa e o documento;
50. A estrutura concetual da autenticação eletrónica compõe-se de dois nexos de vinculação. Um, entre o documento e a assinatura, ou seja, o sinal ou o procedimento objetivado que evidencia o ato de assinar e outro, diferente, entre esse instrumento e a pessoa que é o seu titular. É dessa dupla conexão que resulta a autenticidade do documento;
51. A função autenticação é uma construção jurídica que assentou, no contexto das redes fechadas, das convenções prévias entre as partes, prevalecendo a sua vontade. Porém, nas redes abertas, sem essas convenções, ela só é possível e segura mediante as assinaturas eletrónicas qualificadas;
52. Nas redes abertas, uma das necessidades de autenticação consiste na confirmação dos elementos de identificação que as partes fornecem. Essa confirmação materializa-se no confronto com os elementos de identificação gerados pelas entidades competentes;
53. Autenticar é diferente de identificar. As pessoas não se autenticam, identificam-se. Mas podem autenticar-se os elementos informativos relativos à identificação, sempre por reporte às entidades competentes, podendo esse reporte ser direto ou indireto e envolver, ou não, outras entidades terceiras;
54. Quando alguém se identifica perante um sistema informático, por exemplo para realizar uma operação com relevo jurídico, o sistema autentica a sua identificação mediante a conformação dos seus dados de identificação com os respetivos elementos oficiais;
55. A autenticação dos elementos de identificação de uma pessoa, podendo utilizar os mesmos mecanismos técnicos da assinatura eletrónica, é uma função que se distingue da assinatura em si mesma. A assinatura é um instrumento de mediação e de vinculação entre um documento, que é uma entidade autónoma da pessoa, e a própria pessoa. Esse instrumento é importante porque se trata de entidades separadas.
56. A identidade de uma pessoa não se separa dela própria, acompanha-a naturalmente, e é-lhe imanente, pelo que não necessita de haver

instrumento mediador que garanta a vinculação da pessoa à sua própria identificação.

57. O conceito de identidade eletrónica autonomiza-se do de assinatura eletrónica e é mais abrangente do que ela, sendo que esta se deve limitar à sua função natural que é a de autenticar documentos eletrónicos;
58. Nessa linha, o Regulamento EIDAS separa a função de autenticação dos elementos de identificação eletrónica de uma pessoa, dos restantes serviços de confiança eletrónica, que são a assinatura eletrónica os selos eletrónicos, os selos temporais, os documentos eletrónicos, os serviços de envio eletrónico registado e a autenticação dos sítios web;
59. A integridade é uma função que opera sobre o próprio conteúdo dos documentos eletrónicos, assegurando a sua estabilidade. Trata-se de uma garantia dinâmica de autenticidade, que acompanha o documento ao longo da sua existência, assegurando a inalteração ou a deteção da alteração do documento assinado;
60. A integridade é mais crítica nos suportes eletrónicos, em face da facilidade e impercetibilidade da sua adulteração, bem como da dificuldade de as partes detestarem, pelos seus próprios meios a integridade dos documentos, como ocorre no papel;
61. A integridade protege o autor do documento contra as adulterações que tenham em vista estender a sua vinculação para além do âmbito da sua vontade expressa pela sua assinatura, mas protege também o destinatário contra situações de repúdio pelo autor ou subscritor, com fundamento na alegada alteração posterior do documento assinado;
62. A determinação da integridade ocorre quando o destinatário de um documento assinado eletronicamente repete a função *hash* que o emitente havia realizado e o resultado é o mesmo;
63. A função de integridade não é essencial à assinatura, porque ela opera apenas depois do ato de assinar e tem em vista detetar adulterações que são posteriores. Trata-se de um requisito do documento, mais do que da assinatura, mas ela é essencial na assinatura eletrónica, dada a dificuldade de alteração dos documentos eletrónicos e a necessidade de garantir a sua deteção;

64. A integridade do documento distingue-se da integridade da assinatura, porque esta, sendo o produto da interceção dos dados de cada documento com os dados da chave privada, é diferente para cada documento e não pode ser transposta para documentos diferentes daqueles que a produziram, sem ser corrompida;
65. A função de não repúdio na origem garante que o autor ou subscritor de um documento não possa mais tarde vir a alegar que afinal o vínculo que assumiu não existe;
66. A função de não repúdio no destino é dada pelos sistemas de comunicação, nomeadamente de notificação eletrónica e garante que quem recebeu uma mensagem eletrónica não possa vir a negar tê-la recebido;
67. A função de não repúdio no destino não é própria da assinatura eletrónica, mas pode ser proporcionada pela tecnologia das assinaturas eletrónicas, nomeadamente os selos temporais e os serviços de envio eletrónico certificado;
68. Antes da disponibilização da tecnologia das assinaturas digitais, a LMCE considerava enviadas e recebidas as mensagens eletrónicas no momento da sua entrada no sistema informático do destinatário;
69. A função da confidencialidade não é própria das assinaturas eletrónica, tal como não é nas assinaturas manuais, mas o facto de as comunicações eletrónicas nas redes abertas poderem ser acessíveis aumenta a necessidade de proteção e de confidencialidade. Essa necessidade pode ser satisfeita pelas assinaturas eletrónicas que utilizam a criptografia;
70. A idenficação eletrónica é função dos certificados eletrónicos. Os certificados são declarações emitidas por entidades terceiras de confiança, que atestam publicamente, para conhecimento geral, a identidade do titular de uma chave privada, que ela se relaciona com uma chave pública, qual a natureza e validade do certificado e o estatuto com que a pessoa assina;
71. A função dos certificados de assinatura eletrónica é fundamental, porque são eles que permitem o estabelecimento de relações jurídicas nas redes abertas, mesmo entre pessoas que anteriormente não se conheciam e entre as quais não existia qualquer convenção prévia de autenticação, e são eles que asseguram a certeza do efeito vinculativo da chave privada sobre uma pessoa determinada;

72. Existem vários tipos de certificados, desde os de identificação, aos de atributos e aos certificados de sítios *web*;
73. Um certificado possui um grau de confiança jurídica correspondente ao da entidade que o emitiu, que nele é também identificada;
74. A validade dos certificados é limitada no tempo, por razões de segurança, devendo também ser cancelados ou revogados pela entidade que os emitiu, sempre que a chave privada tenha estado exposta ao acesso por terceiros ou quando a personalidade jurídica do seu titular se tenha extinguido, bem como nos casos em que tenham sido emitidos com erro, pelo que o sistema de gestão dos certificados pela entidade que os emitiu é essencial à sua segurança. Dessa gestão faz parte a publicitação, pela entidade emitente, de listas de certificados suspensos ou cancelados;
75. Os regimes jurídicos da assinatura eletrónica assentam em quatro grandes princípios, sendo eles o princípio da inalteração do direito subjacente, o princípio da equivalência funcional, o princípio da neutralidade tecnológica e o princípio da liberdade contratual;
76. O princípio da inalteração do direito subjacente traduz a natureza do direito da assinatura eletrónica como uma disciplina de suportes documentais e não dos direitos emergentes das relações jurídicas;
77. O princípio da equivalência funcional postula que os suportes eletrónicos possuem a mesma idoneidade que o papel para documentarem as relações jurídicas, cumpridos que sejam determinados requisitos. Este princípio foi adotado como metodologia jurídica de reconhecimento da validade e eficácia jurídica dos suportes eletrónicos, partindo-se da análise das funções que as assinaturas desempenham no suporte papel e conferindo-as aos suportes eletrónicos. Essa metodologia supriu a ausência de meios técnicos de autenticação disponíveis antes da emergência da assinatura digital;
78. O princípio da equivalência funcional desdobra-se nas funções de equivalência dos documentos e das assinaturas. Quanto aos documentos, a versão mais clássica do princípio, transporta para os suportes eletrónicos a validade e eficácia jurídica do papel, quando estejam verificados um conjunto de requisitos. Quanto às assinaturas, só depois da emergência das

assinaturas digitais foi possível consagrar o princípio de que as assinaturas eletrónicas produzem os mesmos efeitos das assinaturas manuscritas;

79. O princípio da equivalência funcional desdobra-se nas vertentes da não discriminação, que impede que sejam retirados efeitos jurídicos aos documentos só pelo facto de se apresentarem em forma eletrónica e que sejam estabelecidos requisitos legais para estes documentos, diferentes dos suportados em papel; e na vertente da equivalência, que consagra que os suportes eletrónicos podem equivaler às mais elevadas exigências que a lei consagra aos documentos e às assinaturas em papel, mesmo que formais e reconhecidas;
80. O princípio da equivalência funcional impede que as partes sejam obrigadas à utilização dos suportes eletrónicos, consagrando a igualdade de meios e a liberdade da sua utilização;
81. Os procedimentos que se designam de assinatura eletrónica são estruturalmente diversos da assinatura manual, porque são de natureza técnica e não pessoal, extrínseca e não imanente e intrínseca como o é a assinatura manual. A designação de assinatura àqueles procedimentos eletrónicos é apenas uma convenção resultante do princípio da equivalência funcional;
82. O princípio da equivalência funcional equipara suportes, tornando-os juridicamente equivalentes. As tecnologias eletrónicas são apenas mais uma técnica que o conhecimento humano produziu, como muitas outras no passado. A utilização da técnica é inerente à ação humana desde sempre;
83. O princípio da neutralidade tecnológica postula os diversos tipos de assinatura e de autenticação eletrónica em condições de igualdade, não devendo o legislador optar por nenhum deles, para o que os requisitos de segurança jurídica e de produção de efeitos jurídicos devem ser objetivos e não discriminatórios.
84. O princípio da liberdade contratual consagra o direito das partes em estabelecerem livremente o método de autenticação que utilizam nas relações jurídicas que estabelecem entre si. As necessidades de segurança na vinculação das partes são diferenciadas, em conformidade com o contexto das relações que entre elas se estabelecem. Quando as partes se

conhecem e confiam, podem utilizar mecanismos de autenticação parcelares, mais simples e económicos;

85. Os sujeitos da relação jurídica da assinatura eletrónica são o titular da assinatura, os prestadores de serviços de confiança e os terceiros que confiam na assinatura;
86. Os prestadores de serviços de confiança eletrónica fornecem a todos os interessados, esse serviço essencial do sistema de assinaturas eletrónicas que é a confiança. Trata-se de um serviço idêntico, mas não igual, ao que é prestado no paradigma do papel, pelas entidades competentes para a identificação civil e os notários, que são também entidades de confiança;
87. Os prestadores de serviços de confiança fornecem dispositivos de assinatura, nomeadamente pares de chaves, identificam, mediante certificados, os titulares e dão conhecimento dessa identidade, asseguram a conexão entre as chaves e a vinculação ao titular, e fornecem serviços de gestão e de informação acerca da validade dos certificados. Estas entidades podem também certificar ou serem certificadas por outras entidades no que respeita ao cumprimento dos requisitos e procedimentos legais de criação e de gestão de dispositivos de assinatura eletrónica;
88. Para o fornecimento dos pares de chaves, os prestadores de serviços de confiança devem assegurar normas rigorosas de identificação dos titulares, de segurança na sua entrega, de certeza de que as chaves estão matematicamente relacionadas e a chave privada não pode ser derivada a partir da chave pública, que a chave privada está válida, que a chave pública é capaz de determinar alterações à chave privada e aos documentos por ela assinados. Essas entidades asseguram estas garantias aos titulares e a todos os terceiros interessados;
89. As Infraestruturas de Chaves Públicas (PKI) correspondem à forma como estão organizados, nos seus direitos e deveres e como se articulam nas suas funções, em cada ordem jurídica, o autor da assinatura, os prestadores de serviços de certificação e as partes que confiam. Uma das mais importantes funções da PKI é assegurar as designadas hierarquias de confiança, que asseguram quem são as entidades que prestam serviços de confiança, quais aquelas que prestam serviços de segundo nível, auditando e certificando a qualidade dos procedimentos utilizados. Essa certificação, que em alguns

sistemas se designa de credenciação, é essencial para que as partes que assinam e aquelas que recebem documentos assinados conheçam o tipo de assinatura, nomeadamente se é qualificada;

90. As PKI estão organizadas por hierarquias de confiança, com entidades credenciadoras, ou certificadoras dos procedimentos de outras entidades, entidades que prestam serviços diretamente aos interessados, entidades de registo, assinantes e terceiros. Podem também estar organizadas mediante certificação cruzada, em que as entidades se certificam mutuamente;
91. Na configuração das PKI tem evoluído o papel do Estado como entidade de supervisão e mesmo de credenciação, desde as correntes anglo-saxónicas que não a defendem, às correntes continentais, que mais recentemente vêm adotando um modelo de supervisão público, que não exclui a participação de entidades certificadoras privadas. O crescimento da intervenção pública reflete a crescente relevância pública do bem jurídico correspondente à segurança jurídica dos suportes eletrónicos;
92. O Regulamento EIDAS assume o caráter público da supervisão da credenciação eletrónica, assente na obrigatoriedade de cada estado membro estabelecer uma entidade de supervisão, para os prestadores de serviços de confiança eletrónica, com competência no respetivo território. Essas funções incluem a atribuição do estatuto de prestador qualificado de serviços e asseguram funções de auditoria, controlo e autoridade. Em Portugal desempenha funções de entidade credenciadora a Autoridade Nacional de Segurança;
93. O Regulamento EIDAS criou a figura dos prestadores qualificados de serviços de confiança, os únicos que podem emitir certificados qualificados de assinaturas e de selos eletrónicos;
94. Os prestadores de serviços de confiança estão sujeitos a um regime de responsabilidade pelos prejuízos causados aos titulares da assinatura e a terceiros. Trata-se de um regime de responsabilidade pela culpa, pelo incumprimento dos seus deveres funcionais. O ónus da prova da culpa tem evoluído, sendo que ela se presume no Regulamento EIDAS, quando se trate de assinaturas eletrónicas qualificadas, cabendo a quem invoque a responsabilidade nos restantes casos. O valor dessa responsabilidade pode ter um limite máximo voluntariamente estabelecido;

95. O reconhecimento e a validade internacional das assinaturas eletrónicas é um problema ainda não resolvido de forma satisfatória, que causa constrangimentos no comércio eletrónico internacional. No espaço da União Europeia vigora um regime de validade obrigatória dos certificados emitidos por prestadores de serviços sedeados num estado membro, sendo que os emitidos por agentes localizados em países terceiros só serão reconhecidos com base em acordo bilateral entre os estados despectivos. O desafio atual é a criação de um sistema de autenticação universal, ou de um "paradigma universal de autenticação". Nessa linha foi consagrado em regulamento europeu o quadro da identificação eletrónica dos cidadãos europeus, com vigência em todos os Estados Membros. Foi também criado um regime de supervisão europeia dos prestadores de serviços de confiança eletrónica;
96. Embora os primeiros instrumentos normativos definissem o titular da assinatura eletrónica como o detentor do dispositivo de assinatura ou a pessoa que executa as operações de assinatura consideramos mais adequado, até pelo interesse da proteção de terceiros, que esse titular seja aquele que está identificado no certificado emitido pela entidade que presta serviços de confiança. Esse entendimento foi adotado pela legislação mais recente;
97. O caráter objetivo e instrumental dos dispositivos de assinatura eletrónica torna possível que as pessoas coletivas possam assinar diretamente os suportes eletrónicos dos documentos que emitem, sendo que a autenticação deve ser efetuada por um seu representante habilitado ou por sistemas informáticos próprios.
98. Apesar dessa possibilidade, o Regulamento EIDAS reserva as assinaturas eletrónicas para as pessoas singulares;
99. O Regulamento EIDAS criou o serviço de confiança designado de selos eletrónicos, cuja função é idêntica à das assinaturas eletrónicas, de autenticação de documentos emitidos por pessoas coletivas. Os selos eletrónicos qualificados cumprem funções idênticas e produzem os mesmos efeitos das assinaturas eletrónicas qualificadas;
100. Os órgãos da administração pública podem ser titulares de selos eletrónicos, para a autenticação das transações que efetuam, podendo

também a respetiva tecnologia ser utilizada para garantir o sigilo das transações. Podem também existir certificados de atributos, de assinaturas eletrónicas para assinatura pelos titulares desses órgãos. São ainda instrumentos de autenticação das operações eletrónicas realizadas por esses órgãos, os selos eletrónicos, os selos temporais e a autenticação dos sítios web;

101. A autenticação de sítios *web* é um serviço de confiança que garante a autenticidade da identificação da entidade que é titular do sítio *web*, conferindo segurança aos respetivos utilizadores;

102. A autenticação dos sítios *web* não autentica as transações eletrónicas nem os documentos eletrónicos que são produzidos pelas partes nessas transações, função que é própria das assinaturas e dos selos eletrónicos;

103. Os selos temporais são serviços de confiança destinados a garantir a certificação e o controlo da data e da hora da produção de factos em suporte eletrónico;

104. Com a possibilidade de se generalizar a desmaterialização das relações jurídicas em muitas empresas e órgãos da administração pública, adquire relevo o conceito de sede eletrónica, como instrumento de determinação do local de realização de operações, exercício de direitos e cumprimento de obrigações;

105. Os titulares de dispositivos de assinatura eletrónica são responsáveis por adotarem os comportamentos necessários à garantia da exclusividade do despectivo acesso e respondem pelos prejuízos que resultarem da violação desse dever. Trata-se de um regime de responsabilidade pessoal e pela culpa, que inclui o dever de comunicação de todas as situações em que o dispositivo esteve, ou podia ter estado, sujeito a ser acessível a terceiros;

106. As partes que confiam nas assinaturas eletrónicas são as pessoas que recebem documentos eletrónicos autenticados e que utilizam as chaves públicas dos despectivos autores para verificar essa autenticidade. Essas pessoas têm o dever de fazer essa verificação, incluindo da validade dos certificados;

107. Os documentos e as mensagens eletrónicas foram inicialmente equiparados a documentos escritos, mediante o princípio da equivalência funcional, desde que estivessem reunidos os pressupostos de acessibilidade

e posterior usabilidade ou, como estabelece a lei portuguesa, suscetibilidade de representação como declaração escrita. Esta equivalência foi metodologicamente superada com a consagração do conceito de documento eletrónico;

108. A originalidade é um conceito próprio dos documentos em papel, que assegura a autenticidade e a integridade, bem como a deteção de eventuais alterações posteriores;

109. Nos documentos que titulam direitos, a originalidade garante também a singularidade dos documentos, essencial para a segurança jurídica;

110. Antes da emergência das assinaturas qualificadas, a originalidade dos documentos eletrónicos era considerada consumada por equivalência funcional, nos casos em que se reunissem os requisitos de autenticidade e integridade, sendo que o da singularidade dependia da exclusividade da sua detenção;

111. Nos documentos eletrónicos não deve existir o conceito de originalidade, porque todos eles são originais, mas os seus atributos emergem imediatamente das assinaturas eletrónicas qualificadas, em resultado do elevado grau de certeza acerca da autenticação e integridade dos documentos eletrónicos;

112. O requisito da singularidade, que é fundamento de segurança nas transações mediante entrega da posse, nos títulos que incorporam direitos, não existe nos documentos eletrónicos porque a sua comunicação implica sempre o envio de uma cópia do que está gravado no computador, existindo situações em que o problema se ultrapassou com a criação de registos de direitos e da sua transmissão;

113. A singularidade em sentido material assenta na relação entre o documento e a relação jurídica subjacente e garante que o seu autor não emitiu outro documento igual. Em sentido formal garante que um documento, depois de emitido não foi duplicado. A primeira não possui qualquer especificidade nos suportes eletrónicos, dado que é relativa às pessoas e não aos documentos e a segunda pode ser garantida pelas assinaturas eletrónicas qualificadas e pelos selos temporais;

114. Nos documentos eletrónicos não existe o conceito da exclusividade da posse, que é essencial aos títulos negociáveis, sendo esse requisito

substituído pela criação de registos dos direitos e das suas transações. A criação dos títulos eletrónicos transacionáveis pode ser facilitada pela emergência dos selos eletrónicos e dos selos temporais, mas ainda não existe um regime jurídico próprio;

115. O arquivo de documentos eletrónicos necessita de regulamentação legal específica, em especial pela necessidade de além dos próprios documentos ser necessário garantir a disponibilidade dos equipamentos, dos suportes eletrónicos e dos sistemas operativos que assegurem as funções de interface na disponibilização e reprodução dos documentos;

116. É ainda necessário criar normas que garantam a integridade dos documentos arquivados, a data e hora em que foram produzidos, arquivados ou o seu suporte foi alterado, bem como a durabilidade dessas certificações, para além da validade da própria tecnologia;

117. A garantia do arquivo e da conservação dos documentos pode ser prosseguida mediante a intervenção de entidades terceiras especializadas que garantam todos os atributos dos documentos arquivados;

118. Os documentos eletrónicos fazem prova plena em juízo quando autenticados com assinatura eletrónica qualificada, bem como, relativamente aos respetivos factos, quando possuam selo eletrónico, selo temporal ou tenham sido objeto de envio registado eletrónico qualificado, sempre que esses produtos de confiança sejam qualificados. A lei equipara esses documentos a documentos reconhecidos;

119. As administrações públicas estiveram desde logo na origem da utilização de meios eletrónicos e da assinatura eletrónica, em especial no domínio aduaneiro e fiscal, em face da sua conexão com a atividade empresarial;

120. Os procedimentos administrativos são essencialmente instâncias de receção e tratamento de informação, muitas vezes em massa, pelo que a utilização dos meios eletrónicos é instrumento de eficiência;

121. A utilização de meios eletrónicos no procedimento administrativo é promovida pelo CPA de 2015, que reconhece aos interessados o direito de entrega de documentos por via eletrónica e a utilização das comunicações e notificações eletrónicas pelos órgãos respetivos;

122. Tal como relativamente à atividade comercial as redes abertas alteraram o conceito de mercado, eliminando os conceitos de tempo e espaço,

também nas relações administrativas se alterou o conceito de localização espacial e delimitação temporal do exercício dos direito e do cumprimento das obrigações, criando-se assim as condições para a alteração dos conceitos de competência territorial, de descentralização e de desconcentração administrativa;

123. As tecnologias eletrónicas permitem a desmaterialização e automatização de extensos segmentos da instrução dos procedimentos administrativos, podendo ela estender-se até à própria decisão nos casos em que ela seja vinculada;

124. Os procedimentos eletrónicos podem ser automatizados integralmente nos casos em que a apreciação e a decisão sejam estritamente vinculadas, bem como quando, sendo embora passíveis de discricionariedade, podem ser estabelecidos critérios quantificados e parametrizáveis, que contemplem todas as situações possíveis;

125. Não existem decisões informáticas nem atos administrativos informáticos, sendo sempre ao tos administrativos, mesmo que operados por máquinas informáticas, manifestações de vontade do órgão competente para a decisão, sendo essa vontade expressa no programa informático;

126. Os programas informáticos não se enquadram tipicamente no conceito dos regulamentos administrativos, porque se trata da tradução, para a linguagem informática, de regras especificadas na lei ou em regulamentos, e não de normas dirigidas a qualquer universo de pessoas. Não se trata de fontes normativas, mas de mecanismos de previsão e de produção de efeitos determinísticos;

127. Apesar disso, tratando-se de especificações que devem ser objeto de escrutínio, pelo que devem ser obrigatoriamente aprovados pelo órgão competente para a decisão, publicitados e suscetíveis de impugnação;

128. A assinatura eletrónica é um instrumento de autenticação dos documentos eletrónicos e uma garantia de segurança jurídica dos respetivos suportes, fundando assim um paradigma dual dos suportes documentais, onde anteriormente só existia o papel. Existem agora dois regimes jurídicos de autenticação, mas eles são separados e não interoperáveis, pelo que quando se converte um documento de um suporte para o outro, a autenticação não se comunica. Essa é uma lacuna jurídica que necessita de

ser suprida apesar de existirem soluções episódicas que não são generalizáveis. Esse problema pode resolver-se mediante a intervenção de notários;

129. A proliferação de formas de autenticação e de assinatura eletrónica, e a onerosidade das assinaturas avançadas e qualificadas é um constrangimento à utilização dos meios eletrónicos que poderia ser ultrapassado com a criação de um regime de interoperabilidade dos vários tipos de assinatura que uma mesma pessoa possua ou então com a criação de uma identidade eletrónica que seja suporte da cidadania eletrónica;

130. A notificação eletrónica é uma forma de comunicação eletrónica que necessita de autenticação eletrónica para produzir efeitos jurídicos seguros. Essa autenticação é diferente da autenticação dos documentos que eventualmente a acompanhem. A segurança jurídica pressupõe também a certificação eletrónica da data do seu envio e receção. Essa certificação deve ser feita por entidades terceiras de confiança, tal como ocorre nas notificações em papel;

131. Existe em Portugal um mecanismo de notificação eletrónica certificada por entidades terceiras, que é a caixa postal eletrónica;

132. A previsão do CPA, de que podem ser efetuadas notificações eletrónicas para a caixa de correio eletrónico mencionado pelas pessoas coletivas, é problemática, por não estar garantida a segurança. Do mesmo modo a falta de previsão acerca da autenticação dessas notificações constitui facto de insegurança. Normas específicas devem suprir essas lacunas, nomeadamente conforme ao estabelecido na lei da assinatura eletrónica, que exige que os documentos eletrónicos emitidos pelos órgãos da administração pública sejam autenticados com a assinatura eletrónica qualificada dos respetivos autores;

133. Do mesmo modo deve o regime das notificações eletrónicas do CPA estabelecer o regime de certificação da data e hora do envio e da receção, não devendo a sua determinação ficar na disponibilidade das partes;

134. As notificações efetuadas através dos sítios *web* dos órgãos da administração pública só devem ser admitidas nos casos em que a sua disponibilização e o acesso pelos interessados sejam certificados por entidades terceiras de confiança. Essa forma de notificação não é

recomendável, porque não é efetuada para um domínio eletrónico individual dos interessados e exigirá destes consultas repetidas aos sítios *web* dos diversos órgãos administrativos onde possuem procedimentos em curso;

135. No procedimento administrativo em suporte eletrónico, a lei deve exigir a autenticação dos documentos, nomeadamente o requerimento inicial, os documentos juntos ao processo, incluindo os provenientes de outros órgãos da administração pública, devendo a autenticação abranger a data e a hora em que foram juntos ao processo, sendo que o CPA só exige autenticação do documento de onde conste a decisão do procedimento. Estes requisitos são fundamentais para garantir o princípio da integridade do processo administrativo;

136. A segurança jurídica dos suportes eletrónicos exige também um regime jurídico dos arquivos eletrónicos que salvaguarde a autenticidade, integridade e particularmente a garantia da sua disponibilidade futura e que estabeleça as obrigações a que ficam responsáveis os titulares dos órgãos competentes no arquivamento desses documentos. Ao mesmo regime devem ser submetidos os dados que foram utilizados nos processamentos. Este regime é especialmente importante no procedimento administrativo, para a defesa dos direitos dos cidadãos;

137. É necessário criar um regime jurídico do processo administrativo eletrónico. A informatização de muitas tarefas dos procedimentos administrativos, que em muitos casos é completa, produziu uma desestruturação do processo administrativo, como suporte documental da tramitação do procedimento, que é necessário preservar. O problema agrava-se porque os sistemas automatizados operam apenas com dados e o controlo da legalidade efetua-se com documentos, pelo que é necessário garantir também a documentação de todos os atos e diligências do procedimento eletrónico mesmo que desmaterializado e automatizado. O CPA contém várias normas sobre a organização e a segurança do processo em papel, que necessitam de ser alargadas ao processo eletrónico;

138. É necessário estabelecer o regime jurídico do documento administrativo eletrónico, criando uma obrigação de documentação, pela administração

pública, das tarefas efetuadas no procedimento administrativo mediante a operação automática dos sistemas informáticos;

139. É necessária a criação de normas legais que regulem o regime do procedimento administrativo eletrónico, nomeadamente a obrigatoriedade de aprovação da programação dos sistemas informáticos que operam os atos e diligências do procedimento e a sua publicação pelo titular do órgão competente;

140. Nos procedimentos automatizados, a programação e os sistemas informáticos são apenas instrumentos técnicos de ação administrativa que em caso algum substituem o titular do órgão na tramitação e decisão;

141. Os interessados devem sempre ser informados, antes da sua abertura, de que os procedimentos administrativos são informatizados e automatizados, sendo caso disso, podendo ter acesso às regras da respetiva programação;

142. Nos procedimentos automatizados informatizados deve permitir-se aos interessados a sua consulta permanente através do sítio *web* do órgão competente, permitindo-se a sua participação, também permanente, na realização dos atos e diligências;

143. O Regulamento EIDAS revogou o regime das assinaturas eletrónicas constante do Decreto-Lei n.º 290-D/99, de 2/8, salvo na parte que respeita à prova mediante documentos eletrónicos;

144. O Regulamento EIDAS criou um sistema de indentificaçao eletrónica no espaço da União Europeia, que confere o direito aos cidadãos de um Estado Membro a utilizar um só meio de identificação em todos os Estados Membros, quando ele possua um nível de garantia elevado ou igual ao do outro Estado Membro, criando também um regime de interoperabilidade entre os sistemas dos vários Estados;

145. Esse regime deve também aplicar-se na utilização pelos cidadãos nacionais em todos os serviços eletrónicos da administração pública portugueses, bem como das empresas.

Bibliografia

Aboso, G. E. (2017). *Derecho Penal Cibernético. La Cibernética y el Derecho Penal en la Moderna Sociedad de la Información y la Tecnologia de la Comunicación*. Euros Editores, S. R. L. Buenos Aires.

Almeida. M. A. (2015). *Teoria Geral do Direito Administrativo. O Novo Regime do Código do Procedimento Administrativo, 3.ª Edição*. Edições Almedina. Coimbra.

Almeida D'Eça, F. (2009). *Registos On Line, 2.ª Edição Revista e Actualizada*. Edições Almedina, S. A. Coimbra.

Amaral, D. F. (2001). *Curso de Direito Administrativo, Volume II*. Edições Almedina, Coimbra.

Amaral, D.F., Caupers, J.; Claro, J.M., Raposo, J., Garcia, M.G.D; Vieira, P.S., Silva, V.P. (2005). *Código do Procedimento Administrativo Anotado, com Legislação Complementar*. 5.ª Edição", Livraria Almedina. Coimbra.

Andrade, F. C. P. (2003). *A Assinatura Dinâmica Face ao Regime Jurídico das Assinaturas Electrónicas*. Scientia Jurídica, Tomo LIII, n.º 299, 2004.

Andrade, F. C. P. (2003). *Contratação Electrónica e Recurso a Sistemas Multi-Agentes: questões de representação e responsabilidade*. http://wiki.di.uminho.pt/twiki/pub/Research/Doutoramentos/SDDI2005/Francisco Andrade.pdf

Barlow, J.P. (1996, February 8). *A Declaration of the Independence of Cyberspace*. Acedido a 11 de maio 2016, em: https://www.eff.org/cyberspace-independence.

Barret, N. (2006). *The Binary Revolution – The history and Development of the Computer*. Weidenfeld & Nicolson. London.

Baygual, F.A. (2002). El Protocol SET. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., *Régimen Jurídico de Internet*. La Ley. Madrid.

Bazin, P. (2008). An Outline of the French Law on Digital Evidence. *Digital Evidence and Electronic Signature Law Review*. Vol 5, pag. 180 e 182.

Bennasar, A. J. (2010). La Validez del Documento Electrónico y su Eficácia en Sede Procesal. Lex Nova. Valladolid.

Berry, W. (1990). Why I am not going to buy a computer. Acedido a 17/2/2016 em: http://www.jesusradicals.com/uploads/2/6/3/8/26388433/computer.pdf

Bessio, I. P. (2015). "Prueba Documental Electrónica en el Processo Jurisdicional: Estamos Listos?". Fodertics 3.0. Estúdios Sobre Nuevas Tecnologias e Justícia. Editorial Comares. Granada.

Binder, N. B. (2016). Weg frei für vollautomatisierte Verwaltungsverfahren in Deutschland. http://www.foev-speyer.de/files/de/downloads/Jusletter-IT_22.09.2016.pdf.

Birnhack, M.D. e Elkin-Koren, N. (Summer 2003). *The Invisible Handshake: The Reemergence of the State in the Digital Environment*. Virginia Journal of Law and Technology. University of Virginia. Acedido a 11/5/2016, em: http://www.vjolt.net/vol8/issue2/v8i2_a06-Birnhack-Elkin-Koren.pdf.

Blanco, C. L. e López, L.A. (2004). El Uso de la Firma Electrónica por las Administraciones Públicas: Nuevos Modelos de Relación de Calidad en la Gestión Pública. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.

Blanco, M. D.R. (2007). Las Nuevas Tecnologías en la Futura Ley de Contratos del Sector Público. Em: Parra, A.M (dir). e Lebrón, M.J.G (Coord). *Derecho Patrimonial e Tecnología*". Marcial Pons, Ediciones Jurídicas. Madrid.

Blasco, J.A. (2005). Qué es Internet. Em: Mexía, P.G (Director). *Principios de Derecho de Internet*. 2.ª Edição, Tirant lo Blanch, Valencia.

Boadilla, R.H., Belenguer, J.A., Pintos, J.A., Elorza, I.D. Eganha, J.M.H., Peso, J.A.M.V., Moliner, A.P.G., Torres, E.P., Soria, D.R. e Fornos, A.Z.R., (2004). *Comentarios a la Nueva Ley General Tributaria*. Thomson, Aranzadi, Navarra.

Bochenski, I. M., (1976). *Historia de la Lógica Formal*. Editorial Gredos, Madrid.

Calviño, R.C., (2008). *Servicios de Certificación de Firma Electrónica y Libre Competencia.* Editorial Comares, Granada.

Calvo-Sotelo, A.C. e Coello, M.C.L., (2002). La Firma Electrónica. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., *Régimen Jurídico de Internet*. La Ley. Madrid.

Cantos, J.M.A. (2004). El Control de Calidad de los Servicios de Certificación y de los Productos de Firma Electrónica. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.

Caramés, J.G. (2005). La Administración Electrónica. Em: Mexía, P.G (Director). *Principios de Derecho de Internet*. 2.ª Edição, Tirant lo Blanch. Valencia.

Carrillo, M.C., (2012). *El Pago Electrónico en Internet: Estructura Operativa e Régimen Jurídico*. Thomson Reuters, Aranzadi. Pamplona.

Carron, C.F. (2010). Empleo de las Nuevas Tecnologías en el Proceso Civil Francés: Algunas Ideas Generales. Em: Motilla. C.S. (Coordinadora). *Presente y Futuro de la e-Justicia en Espanha y la Unión Europea*. Thomson Reuters, Aranzadi. Pamplona.

Casado, E.G., (2005). *Notificaciónes Telemáticas y Otros Médios de Notificación Administrativa en el Procedimiento Administrativo Comúm*. Editorial Bosch, Barcelona.

Casamento, G. e Hatfield, P. (2009). The Essential Elements of an Effective Electronic Signature Process. *Digital Evidence and Electronic Signature Law Review*. Vol 6: pag. 84.

Castells, M., (2004). *A Galáxia Internet - Reflexões Sobre a Internet, Negócios e Sociedade*. Fundação Calouste Gulbenkian, Lisboa.

Cecílio, L. R. (2015) "Política Criminal el el Ciberespacio: Crítica al Concepto de Crimen Informático". *Fodertics 3.0. Estúdios Sobre Nuevas Tecnologias e Justícia. Editorial Comares*. Granada.

Clarizia, R. (1988) *Informática e Conclusione del Contratto*. 1ª edición, Colección Diritto dell"informática 5. Milán.

Correia, M. P. (1999). Comércio Eletrónico: Forma e Segurança. *As Telecomunicações e o Direito da Sociedade da Comunicação.* Coimbra.

Correia, M. P. (2000). As certificações digitais: factura e assinatura. *Privacidade e comércio electrónico*. Comissão Nacional de Protecção de Dados.

Correia, M. P. (1999). *Assinatura Electrónica e Certificaçao Digital*. http://www.apdi.pt/wp-content/uploads/2016/10/8-ARTIGO_ASSINATURA_ELETRONICA_CERTIFICACAO_DIGITAL.pdf

Cremades, J. (2002). Cultura y Internet: Una Nueva Revolución. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., *Régimen Jurídico de Internet*. La Ley. Madrid.

Dan Kaminsky. (2015). *Dan Kaminsky, hacker y experto en seguridad online: "Internet tiene siete llaves y yo tengo una*. Consulta a 26/5/2015. Em: http://www.huffingtonpost.es/2015/08/03/kaminski-seguridad-online_n_7924008.html

Delgado, I.M. (2005). Las Notificaciones Administrativas Telemáticas. Em: Moraleda, J.P., *Administraciones Públicas e Nuevas Tecnologías*. Editorial Lex Nova. Valladolid.

Díaz, J.J.O. (2008). *La Firma y el Contrato de Certificación Electrónicos.* Thomson – Aranzadi. Pamplona.

Eggers, W.D. (2005). *Governing 2.0 - Using Technology to Improve Education, Cut Red Tape, Reduce Gridlock, and Enhance Democracy*. Roman & Littlefield Publishers, Inc. Maryland.

Entralgo, P.L. (1983). *Teoría y Realidad del Otro.* Alianza Editorial. Madrid.

Fernández, F.U. (2004). Efectos Jurídicos de la Firma Electrónica: La Emisión de Actos Administrativos «On Line». Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.

Fraile, G; (1978). *Historia de la Filosofía, vol. III – Del Humanismo a la Ilustración.* Biblioteca de Autores Cristianos, Madrid.

Friedman, T.L. (2005). *O Mundo é Plano - Uma História Breve do Século XXI*. Actual Editora, Lisboa.

Gálvez, J.F.P. (2007). Incidencia de las Nuevas Tecnologías en el Procedimiento Administrativo Español. Em: Parra, A.M (dir). e Lebrón, M.J.G (Coord). *Derecho Patrimonial e Tecnología*. Marcial Pons, Ediciones Jurídicas. Madrid.

Garcia, M.G.F.P.D. (1994). *Da Justiça Administrativa em Portugal. Sua Origem e Evolução*. Universidade Católica Editora. Lisboa.

Garnacho, A.R. (2002). *Sistema de Certificación: La Firma y el Certificado Digital. Regimen Jurídico de Internet*. Editorial La Ley. Madrid.

Gassen, D. (2008). Introducing and Working With Electronic Signatures in Mass Applications: Notaries And The German Commercial Register. *Digital Evidence and Electronic Signature Law Review.* Vol 5, pag. 68.

Giannantonio, E. (1986). *Trasferimenti Elettronici dei Fondi e Autonomia Privata*. Univ. di Salerno, A. Giuffré. Milano.

Gil, M.I.L. (2003). Modificaciones del Régimen Jurídico Administrativo del Empleo Masivo de Nuevas Tecnologías. En Particular el caso de la Agencia Estatal de Administración Tributaria. Em: Ros, R.M. e Gallego, M.L.M., *Derecho de Internet - La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*. Thomson, Aranzadi, Navarra.

Gil, M.I.L. (2004). Los Interesados en el Procedimiento: La Problemática de las Personas Jurídicas. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.

Gil, P.G. (2004). La Representación por Medios Electrónicos. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.

Goldsmith, J. (1997). *Against Cyberanarchy.* Acedido a 20 de maio de 2014 em: http://groups.csail.mit.edu/mac/classes/6.805/articles/goldsmith-against-cyberanarchy.html.

Gonçalves, F.; Alves, M..J.; Vieira, V.M.F; Gonçalves, R.M.; Correia, B. e Gonçalves, M.V. (2016). *Novo Código do Procedimento Administrativo Anotado e Comentado, 3.ª edição*. Edições Almedina, S.A. Coimbra.

Gonçalves, P. (1997). O Acto Administrativo Electrónico. *Scientia Jurídica, Revista de Direito Comparado Português e Brasileiro, Tomo XLVI*. N.º 265/267, Universidade do Minho: pag. 47 a 95.

González, N. R. (2007). La Utilización de las Nuevas Tecnologías en las Relaciones Entre las Administraciones Públicas y los Ciudadanos (En Particular, Registros Telemáticos y Notificaciones Telemáticas): Hacia un Cambio de Modelo. *Revista Española de Derecho Administrativo, n.º 133, Enero - Marzo* 2007. Editorial Thomson – Civitas. Navarra.

Gragera, M.L.D. (2002). Normativa Aplicable a la Firma Electrónica (Directiva 99/93/CE y Real Decreto-Ley 14/1999)". Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., *Régimen Jurídico de Internet*. La Ley. Madrid.

Gutiérrez, R.M. (2009). *Administración Pública Electrónica*. Civitas, Thomson Reuters, Editorial Aranzadi. Pamplona.

Guzmán, A.M. (2004). Criptografía de Clave Pública Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.

Habermas, J. (2003). *Teoría de la Acción Comunicativa*. Santillana Ediciones Generales. Madrid.

Hellman, M. e Diffie, W. (1976). New Directions in Cryptography. Consultado a 14/10/2015 em: http://www-ee.stanford.edu/~hellman/publications/24.pdf.

Jiménez, A.Z. (2004). El Régimen de Responsabilidad en el Uso de la Firma Electrónica. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.

Kirk, G. S., Raven, J. E. (1979). *Os Filósofos Pré-Socráticos,* Fundação Calouste Gulbenkian. Lisboa.

Kloos, C.D.e Rubio, C.G. (2002). História de Internet. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., *Régimen Jurídico de Internet*. La Ley. Madrid.

Kneale, W. e Kneale, M. (1980). *O Desenvolvimento da Lógica*. 2.ª edição, Fundação Calouste Gulbenkian, Lisboa.

Kracmar, H., Bjorn-Andersen, N. e O' Callaghan, R. (1995). *EDI in Europ*, John Wiley & Sons. Chichester.

Kudruavtseva, O.I. (2008). The Use of Electronic Digital Signatures in Banking Relationships in the Russian Federation. *Digital Evidence and Electronic Signature Law Review*. Vol 5.

Larisma, S. (2004) "Contratação Electrónica". O Comércio Electrónico e m Portugal. *O Quadro Legal e o Negócio*. https://www.anacom.pt/streaming/manual_comercio_elec.pdf?contentId=178219&field=ATTACHED_FILE.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C.; Postel, J.R., Lawrence G., Wolff, S. (1989). *Una breve historia de Internet*. Cuadernos Novática, Fevereiro de 1989 e Fevereiro de 1990. Acedido a 15/3/2016 em: http://www.ati.es/DOCS/internet/histint/.

Llovet, E.G. (2002). Acreditación. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., *Régimen Jurídico de Internet*. La Ley. Madrid.

López, M.J.L. (2009). *Criptografía y Seguridad en Computadores, Versión 4-0,7,53*. Universidad de Jaén. Consultado a 2014/07/03 em: http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.Lcripto;

Mahillo, S.R.R. (2004). La Seguridad de los Protocolos Criptográficos. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.

Marques, G. e Martins, L. (2006). *Direito da Informática, Lições de Direito da Comunicação, 2.ª Edição Refundida e Atualizada.* Edições Almedina, S. A. Coimbra.

Malsipica, S.G. (2004). Notificaciones Telemáticas. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.

Más, F.J.G. (2003). Firma Electrónica y Seguridad Jurídica Preventiva. Novedades Introducidas por la Ley 24/2001, de 27 de Diciembre, de Medidas Fiscales,

Administrativas e del Orden Social. Em: Ros, R.M. e Gallego, M.L.M., *Derecho de Internet - La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*. Thomson, Aranzadi, Navarra.

Más, F.J.G. (2004). *Comercio y Firma Electrónicos. Análisis Jurídico de los Servicios de la Sociedad de la Información*. 2.ª Edição, Editorial Lex Nova. Valladolid.

Maurer, H. (2011). *Derecho Administrativo. Parte General*. Marcial Pons. Ediciones Jurídicas y Sociales, S.A. Madrid.

Mundet, J.R.C.P. e Peña, F.M. (2006). *Información y Documentación Administrativa*. 2.ª Edição; Editorial Tecnos. Madrid.

Munhoz, J.M.A., Mercado, F.G.G, Delgado, J.M.G, Espinosa, J.I.M.M, Bedoya, M.D.R.M, González, M.R., Gandasegui, F.S., Labelha, J.I.V. (2004). *Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo*. 3.ª edição, Thomson Aranzadi. Navarra.

Nadal, A.G. (2001). *La Ley de Firma Electrónica.* 2.ª edição, Civitas Ediciones, SL. Madrid.

Nadal, A.G. (2009). *Comentarios a la Ley 59/2003 de Firma Electrónica*. 2.ª edição, Civitas Aranzadi, Thomson Reuters. Pamplona.

Oliveira, M.E., Gonçalves, P.C. e Amorim, J. P. (2006) *Código do Procedimento Administrativo Comentado*; 2.ª Edição, Livraria Almedina. Coimbra.

Olmeda, A.P. (2007). *La Actividad Administrativa Efectuada por Medios Electrónicos – A Propósito de la Ley de Acceso Electrónico a las Administraciones Públicas*, Thomson, Aranzadi. Pamplona.

Ortega, R.R. (2007). *El Expediente Administrativo - De los Legajos a los Soportes Electrónicos*. Thomson, Aranzadi. Navarra.

Ortiz, R.I., (2000). *Derecho de la Contratación Electrónica*. Civitas Ediciones. Madrid.

Paniagua, E. L., (2010). *Fundamentos de Derecho Administrativo. Del Derecho del poder al Derecho de los ciudadanos. 2.ª edición*. Colex Editorial. Universidad Nacional de Educación a Distância. Madrid.

Parra, A.M. (2002). Ley Modelo de la CNUDMI/UNCITRAL para las Firmas Electrónicas. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., *Régimen Jurídico de Internet*. La Ley. Madrid.

Patrão, A. (2012). *Assinaturas Eletrónicas, Documentos Eletrónicos e Garantais Reais. Reflexões Sobre a Viabilidade de Constituição de Garantias Imobiliárias por Meios Electrónicos à Luz da Lei Portuguesa*. Revista do Centro de Estudos de Direito do Ordenamento, do Urbanismo e do Ambiente.

Perales, J.M.A.M. (2005). La Nueva Administración Pública Electrónica, Las Relaciones Electrónicas Entre la Administración y el Ciudadano. Especial Referencia a la Firma Electrónica. Em: Moraleda, J.P., *Administraciones Públicas e Nuevas Tecnologías*. Editorial Lex Nova. Valladolid.

Pires, J.M.F., Bulcão, G., Vidal, J.R. e Menezes, M.J. (2015), *Lei Geral Tributária Comentada e Anotada.* Livraria Almedina. Coimbra.

Pires, J.M.F. (2016). *Lições de Impostos Sobre o Património e do Selo*. 3.ª Edição, Livraria Almedina. Coimbra.

Pozo, J.D.S. e Sonseca, M.A.M. (2004). Empleo de la Firma Electrónica en el Seno de las Administraciones Públicas: Derecho Comparado. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.

Ramalho, D. S. (2017). *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Edições Almedina. S. A. Coimbra.

Reiniger, T.S. (2008). The Proposed International E-Identity Assurance for Electronic Notarization. *Digital Evidence and Electronic Signature Law Review*. Vol 5: pag.78.

Rivero, D.C. (Mayo 2005). Análisis de los Antecedentes del Concepto de Firma Electrónica Como Equivalente de la Firma Manuscrita. *Revista de Contratación Electrónica*. N.º 60, pág. 99.

Rivero, D.C. (2006). *La Firma Electrónica Reconocida - Análisis de los Requisitos del Artículo 3,3 de la Ley 59/2003, de 19 de Diciembre, de Firma Electrónica*. Colegios Notariales de España. Madrid.

Rocha, M. L. (1999); *A assinatura electrónica Uma Via Portuguesa "Original"?*

http://www.asf.com.pt/winlib/cgi/winlibimg.exe?key=&doc=10038&img=961.

Rocha, M. L.; Correia, M. P.; Rodrigues, M. F.; Andrade, M. A.; Amorim, P. P.; Carreiro, H. J.; Cabrita, L. (2008). *Leis da Sociedade da Informação. Comércio ELetrónico*. Coimbra Editora, Coimbra.

Roques-Bonnet, M.C. (2010). *Le Droit. Peut'il Ignorer la Révolution Numérique?*. Michalon Éditions. Paris.

Rodrigues, B. S. (2009). *Direito Penal Especial. Tomo I. Direito Penal Informático-Digital*. Coimbra Editora Limitada. Coimbra.

Rodrigues, D. (2015, 9 de julho). *A identificação Biométrica: Ficção e Realidade*. Público, pag 34.

Rodriguez, M.A.D. (2004). *Manual de Derecho Informático*., Thomson – Aranzadi. Navarra.

Rodriguez, M.A.D. (2005). *La Seguridad en las Transacciones electrónicas: La Firma Electrónica.* Universidad Pontificia Comillas. Madrid.

Rodriguez, M.A.D. (1999). La Liberalización del Mercado de las Telecomunicaciónes: Una Perspectiva Desde la Ética. Em: *As Telecomunicações e o Direito na Sociedade da Informação*. Instituto Jurídico da Comunicação, Faculdade de Direito da Universidade de Coimbra. Coimbra.

Rodriguez-Margariños, F.G. (2008). *La Administración de Justicia Digitalizada. Una Necesidad Inaplazable.* Ediciones Experiencia. Barcelona.

Ruggieri, F. (2008). Comments on the Italian 'Code For Digital Administration. *Digital Evidence and Electronic Signature Law Review*, Vol 5: pag 29 a 38.

Ruíz, C.B. (2006). *La Contratación Electrónica.* 3.ª Edição. Editorial Dykinson. Madrid.

Sampaio, J. M. G. (2010). *A Prova por Documentos Particulares. Na Doutrina, na Legislação e na Jurisprudência. 3.ª Edição Atualizada e Ampliada*. Edições almedina, S. A. Coimbra.

Sánchez, O.G. (2010). La Incidencia de la Ley de la Firma Electrónica en el Valor Probatorio de los Soportes Informáticos. Mucho Ruido y Pocas Nueces. Em: *Presente y Futuro de la e-Justicia en Espanha y la Unión Europea*. Thomson Reuters, Aranzadi, Pamplona.

Seng, D. (2008). The Singapore Electronic Transactions Act and the Hong Kong Eletctronic Transactions Ordinance. *Digital Evidence and Electronic Signature Law Review*. Vol 5.

Silva, V. M. P. D. P. (2003). *Em Busca do Acto Administrativo Perdido (reimpressão)*. Livraria Almedina. Coimbra.

Sousa, L. F. P. (2017). *O valor Probatório do Documento Eletrónico no Processo Civil, 2.ª Edição*. Edições Almedina, S. A. Coimbra.

Sousa, M.R. (1992). Regime do Ato Administrativo. Direito e Justiça, Volume VI. Lisboa.

Stallings, W. (2011). *Cryptography and Netwook Security, Principles and Practice*. 5.ª Edição, Pearso Education, Pearson Hall. New York.

Tormo, S.S. (2004). Utilización de la Firma Electrónica en la Administración Española I: La Agencia Estatal de la Administración Tributaria. Em: Ministerio de Economia. *Administración Electrónica y Procedimiento Administrativo*. Real Casa de la Moneda. Madrid.

Tossi, E. (2010). *Codice del Diritto Dell'Informatica e Di Internet*. 7.ª Edição, Celt, Casa Editrice La Tribuna. Piacenza.

Ubao, L.G.E. (2003). La Firma Electrónica. Em: Ros, R.M. e Gallego, M.L.M., *Derecho de Internet - La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*. Thomson, Aranzadi, Navarra.

Urdanoz, T. (1978). *História de la Filosofia, vol. VI*. Biblioteca de Autores Cristianos. Madrid.

Vadell, L. M. B. (2015). La Valoración de la Prueba Electrónica. *Fodertics 3.0. Estúdios Sobre Nuevas Tecnologias e Justícia*. Editorial Comares. Granada.

Lima, F.A.P., Varela, J.M.A. (1984). *Código Civil Anotado, Volume I, 3.ª Edição Revista e Actualizada*. Coimbra Editora. Coimbra.

Velasco, M.M.P e Castejón, J.C. (2002). Regulación Versus Autorregulación en Internet y los Nuevos Servicios de Comunicación. Em: Cremades, J., Ordonhez, M.F.A., Illescas, R., *Régimen Jurídico de Internet*. La Ley. Madrid.

Velásquez, R.R., Sau, C.R. e Muñoz, R.M. (2004). *La Firma Electrónica - Aspectos Legales e Técnicos*. Ediciones Experiencia. Barcelona.

Venâncio, P. D. (2015). Delitos Contra la Integridad de los Datos Informáticos y Sistemas Informáticos en el Convénio del Consejo de Europa Sobre la Ciberdelincuencia". *Fodertics 3.0. Estúdios Sobre Nuevas Tecnologias e Justícia*. Editorial Comares. Granada.

Viesca, M.I.H. (2001). La Firma Electrónica en la Regulación Española: Valoración Crítica. Em: Viesca, M.I.H. e Villa, D.R.V., *Los Prestadores de Servicios de Certificación en la Contratación Electrónica*, Aranzadi Editorial, Elcano. Navarra.

Villar-Pallasí, J.L. (2009). *Implicaciones Jurídicas de Internet*. Acedido a 15 de Junho de 2009, em: http://www.dominiuris.com/boletines/doctrinal/villar.htm.

Wolf, H.; Bachof, O; Stober, R. (2006). *Direito Administrativo, Volume I*. Fundação Caloust Gulbenkian. Lisboa.

Relatórios e Estudos de Organizações Internacionais

ITU. (2008). *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*; ITU-T Recommendation X.500; International Telecommunication Union, ITU-T Rec. X.500 (11/2008). Consulta a 26/11/2015. Em: file:///C:/Users/jp01918/Downloads/T-REC-X.500-200811-S!!PDF-E.pdf.

ITU. (2010). *International Telecommunication Union (ITU).* Consulta a 26/11/2015. Em: file:///C:/Users/jp01918/Downloads/T-REC-X.509-201210-I!!PDF-E.pdf

ITU. (2012). *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*; Recommendation ITU-T X.509, International Telecommunication Union; Rec. ITU-T X.509 (10/2012). Consulta a 26/11/2015. Em: em file:///F:/jp01918/UCP2/EDI/T-REC-X.509-201210-I!!PDF-E.pdf.

ITU. (2012). *Entity authentication assurance framework*; Recommendation ITU-T X.1254, International Telecommunication Union; SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY. Cyberspace security – Identity management. Consulta a 26/11/2015. Em: file:///C:/Users/jp01918/Downloads/T-REC-X.1254-201209-I!!PDF-E.pdf.

MISMO. (2009). *The Mortgage Industry Standards Maintenance Organization Engineering Guideline"; MEG0006 Versioning and Release Schedule*. 1/13/2009 8:48 AM. Consulta a 26/5/2015. Em: http://www.mismo.org/Guidelines/EngineeringGuidelines(MEGS).htm.

Montreal Protocols. (1999). *Convention For The Unification Of Certain Rules For International Carriage By Air*. Consulta a 15/3/2016. Em: http://nasamer.ku.edu.tr/sites/nasamer.ku.edu.tr/files/mevzuat/conventions/montreal-convention.pdf.

OCDE. (1998). *A Global Action Plan for Electronic Commerce. Prepared by Business with Recommendations for Governments; Business and Industry Advisory Committee* to the OECD (BIAC). Consulta a 15/1/2016. Em: http://www.witsa.org/papers/globecom.htm, páginas 15 e 16.

OCDE. (2005). *The Use of Authentication Across Borders in OECD Countries*. OECD Working Party on Information Security and Privacy. DSTI/ICCP/REG(2005)4/FINAL; 24-Nov-2005.

UNCITRAL. (1984). A/CN.9/250 and Add.1 to 4. Draft Legal Guide on Electronic Funds Transfers: Report of the Secretary-General. Em: *Yearbook of the United Nations Commission on International Trade Law.* Volume XV. New York.

UNCITRAL. (1985). A/CN.9/265. *Legal Value of Computer Records - Report of the Secretary-General*; United Nations Commission on International Trade Law Eighteenth Session. Vienna.

UNCITRAL. (1985). A/CN.9/266Add.1. *Draft Legal Guide on Electronic Funds Transfers, Chapter on Finality of Funds Transfer, Report of the Secretary – General*. New York.

UNCITRAL. (1985). A/CN.9/266Add.2. *Draft Legal Guide on Electronic Funds Transfers, Chapter on Finality of Funds Transfer, Report of the Secretary – General*. New York.

UNCITRAL. (1991). A/CN.9/344. Report of the Working Group on International Payments on the Work of its Twenty-Second Session, 26 November – 7 December 1990. Em: *Yearbook of the United Nations Commission on International Trade Law*. Volume XXII. Vienna

UNCITRAL. (1991).A/CN.9/350. *Legal Issues of Electronic Data Interchange. Electronic Data Interchange: Report of the Secretary-General*. Yearbook of the United Nations Commission on International Trade Law, Vol. XXII, páginas 409 a 427. New York.

UNCITRAL. (1992). A/CN.9/221. *Electronic Funds Transfer, Report of the Secretary-General*. New York.

UNCITRAL. (1992). A/CN.9/WG.IV/WP.53. *Working Paper Submitted to the Working Group on International Payments at its Twenty-Fourth Session: Possible Issues to be Included in the Programme of Future Work on the Legal Aspects of EDI: Note by the Secretariat*. Yearbook of the United Nations Commission on International Trade Law. Vol. XXIII", páginas 365 a 382. New York.

UNCITRAL. (1992). A/CN.9/360. *Report of The Working Group on International Payments on The Work Of Its Twenty-Fourth Session*. United Nations Commission on International Trade Law, Vienna

UNCITRAL. (1993). A/CN.9/373. *Report of the Working Group on Electronic Data Interchange (EDI) on the Work of its Twenty-Fifth Session. 4 - 15 January 1993*.

United Nations Commission on International Trade Law, 9 March 1993. New York

UNCITRAL. (1993). A/CN.9/387. *Working Group on Electronic Data Interchange (EDI) on the Work of its Twenty-Sixth Session,11/12 October 1993*. United Nations Commission on International Trade Law. Vienna

UNCITRAL. (1994). A/CN.9/WG.IV/WP.60. *Working Paper Submitted to the Working Group on Electronic Data Interchange at its Twenty-Seventh Session: Revised Articles of Draft Uniform Rules on the Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Data Communication: Note by the Secretariat*". New York.

UNCITRAL. (1994). A/CN.9/406. *Report of the Working Group on Electronic Data Interchange (EDI) on the Work of its Twenty -Eighth Session*. United Nations Commission on International Trade Law. Vienna

UNCITRAL. (1995). A/CN.9/WG.IV/WP.64. *Working Paper Submitted to the Working Group on Electronic Data Interchange (EDI) at its Twenty-Ninth Session. Draft Guide to Enactment of the UNCITRAL Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Communication: Note by the Secretariat*. "Yearbook of the United Nations Commission on International Trade Law, 1995, Vol. XXVI", páginas 157 a 171. New York.

UNCITRAL. (1995). A/CN.9/407. *Report of the Working Group on Electronic Data Interchange (EDI) on the Work of its Twenty-Ninth Session*. United Nations Commission on International Trade Law, Twenty-Eighth Session. Vienna.

UNCITRAL. (1995). A/CN.9/409. *Draft Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Communication. Compilation of Comments by Governments and International Organizations*. United Nations Commission on International Trade Law, Twenty-Eight Session. Vienna

UNCITRAL. (1996). *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce*". United Nations publication Sales No.: E.99.V.4, ISBN 92-1-133607-4. New York.

UNCITRAL. (1996). A/CN.9/421. *Report of the Working Group on Electronic Data Interchange (EDI) on the Work of its Thirtieth Session*. United Nations Commission on International Trade Law; Twenty-ninth Session. Vienna

UNCITRAL. (1996). A/CN.9/426. *Electronic Data Interchange. Guide to Enactment of the UNCITRAL Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Communication. Report of the Secretary-General*. United Nations Commission on International Trade Law. Twenty-Ninth Session. New York.

UNCITRAL. (1996). A/CN.9/WG.IV/WP.69. *Electronic Data Interchange. Note by the Secretariat". United Nations Commission on International Trade Law. Working Group on Electronic Data Interchange*. Thirtieth session. Vienna

UNCITRAL. (1996). A/CN.9/WG.IV/WP.71. *Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues. Note by the Secretariat*. United Nations Commission on International Trade Law; Working Group on Electronic Commerce; Thirty-first session. New York

UNCITRAL. (1997). A/CN.9/437. *Report of the Working Group on Electronic Commerce on the Work of its Thirty-First Session*". United Nations Commission on International Trade Law, Thirtieth sesión. New York

UNCITRAL. (1997). A/CN.9/WG.IV/WP.73. *Draft Uniform Rules on Electronic Signatures; United Nations Commission on International Trade Law*. Working Group on Electronic Commerce, Thirty-Second Session. Vienna.

UNCITRAL. (1998). A/CN.9/446. *Report of the Working Group on Electronic Commerce on the Work of its Thirty-Second Session*. United Nations Commission on International Trade Law Thirty-first Session. New York

UNCITRAL. (1998). A/CN.9/WG.IV/WP.76. *Draft Uniform Rules on Electronic Signatures, Note by the Secretariat.* United Nations Commission on International Trade Law, Working Group on Electronic Commerce; Thirty-third sesión. New York.

UNCITRAL. (1998). A/CN.9/WG.IV/WP.77. *Proposal by the United States of America. Note by the Secretariat*. United Nations Commission on International

Trade Law; Working Group on Electronic Commerce; Thirty-third session, New York.

UNCITRAL. (1999). A/CN.9/454. *Report of the Working Group On Electronic Commerce on the Work of its Thirty-Third Session*. United Nations Commission on International Trade Law; Thirty-second sesión. New York.

UNCITRAL. (1999). A/CN.9/457. *Report of the Working Group on Electronic Commerce on the Work of its Thirty-Fourth Session*. United Nations Commission on International Trade Law; Thirty-second session. Vienna.

UNCITRAL. (1999). A/CN.9/465. *Report of the Working Group on Electronic Commerce on the Work of Its Thirty-Fifth Session.* United Nations Commission on International Trade Law, Thirty-third session. Vienna

UNCITRAL. (1999). A/CN.9/WG.IV/WP.84. *Draft Uniform Rules on Electronic Signatures. Note by the Secretariat*. United Nations Commission on International Trade Law. Working Group on Electronic Commerce, Thirty-sixth sesión. New York.

UNCITRAL. (2000). A/CN.9/467. *Report of the Working Group on Electronic Commerce on the work of its thirty-sixth sesión.* United Nations Commission on International Trade Law Thirty-third sesión. New York

UNCITRAL. (2000). A/CN.9/WG.IV/WP.86/Add.1. *Electronic Signatures. Draft Guide to Enactment of the UNCITRAL Uniform Rules on Electronic Signatures. Note by the Secretariat.* Working Group on Electronic Commerce Thirty-seventh sesión. Vienna.

UNCITRAL. (2000). A/CN.9/483. *Report of the Working Group on Electronic Commerce on the work of its thirty-seventh session*. United Nations Commission on International Trade Law Thirty-fourth sesión. Vienna.

UNCITRAL. (2001). A/CN.9/WG.IV/WP.88. *Electronic Signatures, Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures. Note by the Secretariat.* United Nations Commission on International Trade Law Working Group on Electronic Commerce Thirty-eighth sesión. New York.

UNCITRAL. (2001). A/CN.9/WG.IV/WP.91. *Legal aspects of electronic commerce Possible future work in the field of electronic contracting: an analysis of the United Nations Convention on Contracts for the International Sale of Goods Note by the Secretariat*. United Nations Commission on International Trade Law Working Group on Electronic Commerce Thirty-eighth sesión. New York.

UNCITRAL. (2001). A/CN.9/493. *Electronic Signatures, Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures. Note by the Secretariat.* United Nations Commission on International Trade Law Thirty-fourth sesión. Vienna.

UNCITRAL. (2003). A/CN.9/WG.IV/WP.104. *Legal aspects of electronic commerce. Electronic contracting: background information. Note by the Secretariat*. United Nations Commission on International Trade Law Working Group IV (Electronic Commerce), Forty-second sesión. Vienna.

UNCITRAL. (2003). A/CN.9/WG.IV/WP.104/Add.3. *Legal aspects of electronic commerce. Electronic contracting: background information. Note by the Secretariat, Addendum*. United Nations Commission on International Trade Law Working Group IV (Electronic Commerce), Forty-second sesión. Vienna.

UNCITRAL. (2003). A/CN.9/546. *Report of the Working Group on Electronic Commerce on the work of its forty-second sesión*. United Nations Commission on International Trade Law Thirty-seventh sesión. New York.

UNCITRAL. (2005). A/CN.9/578/Add.9. *Draft Convention on the Use of Electronic Communications in International Contracts Compilation of comments by Governments and international organizations Addendum*. United Nations Commission on International Trade Law Thirty-eighth sesión. Vienna.

UNCITRAL. (2005). A/CN.9/578/Add.10. *Draft Convention on the Use of Electronic Communications in International Contracts. Compilation of comments by Governments and international organizations Addendum.* United Nations Commission on International Trade Law Thirty-eighth sesión. Vienna.

UNCITRAL. (2005). A/CN.9/578/Add.15. *Draft Convention on the Use of Electronic Communications in International Contracts. Compilation of comments by*

Governments and international organizations Addendum. United Nations Commission on International Trade Law Thirty-eighth sesión. Vienna.

UNCITRAL. (2006). A/CN.9/608. *Legal Aspects of Electronic Commerce. Explanatory Note on the Convention on the Use of Electronic Communications in International Contracts. Note by the Secretariat*. United Nations Commission on International Trade Law; Thirty-ninth sesión. New York.

UNCITRAL. (2006). A/CN.9/608/Add.1. *Legal aspects of electronic commerce Explanatory Note on the Convention on the Use of Electronic Communications in International Contracts. Note by the Secretariat. Addendum*. United Nations Commission on International Trade Law; Thirty-ninth sesión. New York.

UNCITRAL. (2006). A/CN.9/608/Add.2. *Legal aspects of electronic commerce Explanatory Note on the Convention on the Use of Electronic Communications in International Contracts. Note by the Secretariat. Addendum*. United Nations Commission on International Trade Law; Thirty-ninth sesión. New York.

UNCITRAL. (2006). A/CN.9/608/Add.3. *Legal aspects of electronic commerce Explanatory Note on the Convention on the Use of Electronic Communications in International Contracts. Note by the Secretariat. Addendum*. United Nations Commission on International Trade Law; Thirty-ninth sesión. New York.

UNCITRAL. (2007). A/CN.9/630. *Possible future work on electronic commerce. Comprehensive reference document on elements required to establish a favourable legal framework for electronic commerce: sample chapter on international use of electronic authentication and signature methods. Note by the Secretariat*. United Nations Commission on International Trade Law; Fortieth session. Vienna.

UNCITRAL. (2007). A/CN.9/630/Add.1. *Possible future work on electronic commerce. Comprehensive reference document on elements required to establish a favourable legal framework for electronic commerce: sample chapter on international use of electronic authentication and signature methods. Note by the Secretariat. Addendum*. United Nations Commission on International Trade Law; Fortieth session. Vienna.

UNCITRAL. (2007). A/CN.9/630/Add.2. *Possible future work on electronic commerce. Comprehensive reference document on elements required to establish a favourable legal framework for electronic commerce: sample chapter on international use of electronic authentication and signature methods. Note by the Secretariat. Addendum*. United Nations Commission on International Trade Law; Fortieth session. Vienna.

UNCITRAL. (2007). A/CN.9/630/Add.3. *Possible future work on electronic commerce. Comprehensive reference document on elements required to establish a favourable legal framework for electronic commerce: sample chapter on international use of electronic authentication and signature methods. Note by the Secretariat. Addendum*. United Nations Commission on International Trade Law; Fortieth session. Vienna.

UNCITRAL. (2007). A/CN.9/630/Add.4. *Possible future work on electronic commerce. Comprehensive reference document on elements required to establish a favourable legal framework for electronic commerce: sample chapter on international use of electronic authentication and signature methods. Note by the Secretariat. Addendum*. United Nations Commission on International Trade Law; Fortieth session. Vienna.

UNCITRAL. (2007). A/CN.9/630/Add.5. *Possible future work on electronic commerce. Comprehensive reference document on elements required to establish a favourable legal framework for electronic commerce: sample chapter on international use of electronic authentication and signature methods. Note by the Secretariat. Addendum*. United Nations Commission on International Trade Law; Fortieth session. Vienna.

UNCITRAL. (2011). A/CN.9/WG.IV/WP.115. *Legal issues relating to the use of electronic transferable records. Note by the Secretariat*. United Nations Commission on International Trade Law Working Group IV (Electronic Commerce); Forty-fifth sesión. Vienna.

UNCITRAL. (2012). A/CN.9/WG.IV/WP.118/Add.1. *Legal issues relating to the use of electronic transferable records (continued). Note by the Secretariat. Addendum*.

United Nations Commission on International Trade Law Working Group IV (Electronic Commerce); Forty-sixth sesión. Vienna.

UNCITRAL. (2013). A/CN.9/797. *Report of Working Group IV (Electronic Commerce) on the work of its forty-eighth session (Vienna, 9-13 December 2013)*. United Nations Commission on International Trade Law Forty - seventh sesión. New York.

UNCITRAL. (2014). A/CN.9/804. *Report of Working Group IV (Electronic Commerce) on the work of is forty-ninth session (New York, 28 April-2 May 2014)*. United Nations Commission on International Trade Law Forty – seventh sesión. New York.

UNCITRAL. (2014). A/CN.9/WG.IV/WP.130. *Draft provisions on electronic transferable records Note by the Secretariat.* United Nations Commission on International Trade Law Working Group IV (Electronic Commerce) Fiftieth sesión. Vienna.

UNCITRAL. (2015). A/CN.9/WG.IV/WP.132. *Draft provisions on electronic transferable records Note by the Secretariat*. United Nations Commission on International Trade Law Working Group IV (Electronic Commerce) Fifty-first sesión. New York.

UNCITRAL. (2015). A/CN.9/854. *Possible future work in the area of electronic commerce - legal issues related to identity management and trust services. Proposal by Austria, Belgium, France, Italy and Poland. Note by the Secretariat*. United Nations Commission on International Trade Law Forty-eighth sesión. Vienna.

União Europeia. (1989). *TEDIS - The Legal Position of the Member States With Respect to Electronic Data Interchange. Final Report*". Commission of the European Communities. Bruxells.

União Europeia. COM(1998) 297 final. *Proposta de Directiva do Parlamento Europeu e do Conselho Relativa a um Quadro Comum para as Assinaturas Eletrónicas (Apresentada pela Comissão), Comissão das Comunidades Europeias Bruxelas*, 13.05.1998. Bruxells.

União Europeia. 98/C 157/01. *Parecer do Comité Económico e Social sobre a «Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões: Garantir a Segurança e a Confiança nas Comunicações Eletrónicas — Contribuição para a Definição de um Quadro Europeu para as Assinaturas Digitais e a Cifragem*. Jornal Oficial das Comunidades Europeias, 25.5.98. Bruxells.

União Europeia. (COM(97)0503 C4-0648/97). *Resolução sobre a Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões intitulada "Garantir a segurança e a confiança nas comunicações eletrónicas - contribuição para a definição de um quadro europeu para as assinaturas digitais e a cifragem*. Jornal Oficial nº C 292 de 21/09/1998 p. 0217. Bruxells.

União Europeia. COM(2006) 120 final. *Relatório da Comissão ao Parlamento Europeu e ao Conselho Relatório sobre o funcionamento da Directiva 1999/93/CE relativa a um quadro legal comunitário para as assinaturas eletrónicas*. Comissão das Comunidades Europeias. Bruxelas.

União Europeia. COM(2009) 7806. *Commission Decision of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (notified under document COM(2009) 7806).* (Text with EEA relevance), Official Journal of the European Union, 20.10.2009. Bruxells.

União Europeia. COM(2010)245 final. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Uma Agenda Digital para a Europa*. Comissão Europeia 19.5.2010. Bruxelas.

União Europeia. COM(2010) 171 final. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Realização de um espaço de liberdade, de segurança e de justiça para os cidadãos europeus. Plano de Acção de aplicação do Programa de Estocolmo*. Comissão Europeia, 20.4.2010. Bruxelas.

União Europeia. COM(2011) 882 final. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Dados Abertos. Um Motor de Inovação, Crescimento e Governação Transparente*. Comissão Europeia, 12.12.2011. Bruxelas.

União Europeia. COM(2011) 942 final. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões um Enquadramento Coerente para Reforçar a Confiança no Mercado Único Digital do Comércio Eletrónico e dos Serviços em Linha*. Comissão Europeia Bruxelas, 11.1.2012. Bruxells.

União Europeia. COM(2012) 179 final. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Uma Estratégia Para a Contratação Pública Eletrónica*. Comissão Europeia, 20.4.2012. Bruxelas.

União Europeia. SWD(2012) 136 final. *Commission Staff Working Document Executive Summary of the Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market*; European Commission, 4.6.2012. Brussels.

União Europeia. 2012/C 229/01. *Parecer do Comité Económico e Social Europeu sobre «O mercado digital como motor de crescimento» (parecer exploratório)*. Comité Económico e Social Europeu, 481.ª Sessão Plenária, de 23 e 24 de Maio de 2012. Jornal Oficial da União Europeia, 31/7/2012. Bruxells.

União Europeia. COM(2012) 238 final. *Proposta de Regulamento do Parlamento Europeu e do Conselho Relativo à Identificação Eletrónica e aos Serviços de Confiança para as Transações Eletrónicas no Mercado Interno.* Comissão Europeia, Bruxelas, 4.6.2012. Bruxells.

União Europeia. *Parecer do Comité Económico e Social Europeu sobre a «Proposta de regulamento do Parlamento Europeu e do Conselho relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno*. Jornal Oficial da União Europeia, 15/11/2012, página C 351/74. Bruxells.

União Europeia. *Mercado único digital competitivo - a administração pública em linha como força motriz. Resolução do Parlamento Europeu, de 20 de abril de 2012, sobre um mercado único digital competitivo - a administração pública em linha como força motriz*. Jornal Oficial da União Europeia, 7.9.2013, C 258 E/65. Bruxells.

União Europeia. (2014/C 182/02). *Plano de Ação Plurianual 2014-2018 Sobre Justiça Eletrónica Europeia.* Jornal Oficial da União Europeia 14.6.2014. Bruxells.

União Europeia. *Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust Service Provider status information.* Consulta a 16/3/2016 em: disponível em http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ts_102231v010201p&RGW.doc

Documentos Normativos

Council of Europe. (1981). *Recommendation No. R (81) 20, of the Committee of Ministers to Member States on the Harmonisation of Laws Relating to the Requirement of Written Proof And to the Admissibility of Reproductions of Documents And Recordings on Computers*. (Adopted by the Committee of Ministers on 11 December 1981 at the 341st meeting of the Ministers' Deputies). Consulta a 15/11/2014. Em: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=600958&SecMode=1&DocId=674076&Usage=2.

CMI. (1965). *Convention on Facilitation of International Maritime Traffic*. Consulta a 26/5/2015. Em: http://www.ifrc.org/Docs/idrl/I258EN.pdf.

CMI. (1999). *CMI Rules for Electronic Document Interchange (EDI)*. Appendix A, 13 Octobber 1999, Consulta a 15/3/2016. Em: http://web.uct.ac.za/depts/shiplaw/cmi/cmirules.htm.

Código Civil.

Código Comercial;

Código do Procedimento Administrativo.

Código de Procedimento e de Processo Tributário.

Código de Processo Civil.

Código do Registo Predial.

Código dos Valores Mobiliários

Convenção do Conselho da Europa sobre a Cibercrime. Disponível em http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Decreto-Lei n.º 149/83, de 5 de abril.

Decreto-Lei n.º 176/88, de 18 de maio.

Decreto-Lei n.º 16/93, de 23 de janeiro.

Decreto-Lei n.º 184/98, de 6 de Julho.

Decreto-Lei n.º 135/99, de 22 de abril.

Decreto-Lei n.º 290-D/99, de 2 de Agosto.

Decreto-Lei 14/99, de 17 de Setembro.

Decreto-Lei n.º 146/2000, de 18 de julho.

Decreto-Lei n.º 234/2000, de 25 de Setembro.

Decreto-Lei n.º 62/2003, de 3 de abril.

Decreto-Lei n.º 7/2004, de 7/7.

Decreto-Lei n.º 112/2006, de 9 de junho.

Decreto-Lei n.º 116-A/2006, de 16 de junho.

Decreto-Lei n.º 238/2006, de 20 de dezembro.

Decreto-Lei n.º 53-A/2006, de 29 de dezembro.

Lei n.º 7/2007 de 5 de fevereiro.

Decreto-Lei n.º 116/2008, de 4 de julho.

Decreto-Lei n.º 88/2009, de 9 de abril.

Decreto-Lei n.º 113/2011, de 29 de novembro.

Decreto-Lei n.º 160/2013 de 19 de novembro.

Decreto-Lei n.º 73/2014, de 13 de maio.

Decreto-Lei n.º 214-G/2015, de 2 de outubro.

Diretiva 1999/93/CE, de 13/12/1999.

Lei Geral Tributária.

Norma ISO/IEC DIS 29115

Portaria n.º 375/2003, de 10 de maio.

Portaria n.º 331-B/2009, de 30 de março.

Portaria n.º 280/2013, de 26 de agosto.

Portaria n.º 189/2014, de 23 de setembro.

Portaria n.º 289-B/2015, de 17 de setembro.

Portaria n.º 280/2013, de 25 de outubro.

Regulamento (UE) n.º 910/2014, de 23/7/ 2014.

SET. (1997). SET Secure Electronic Transaction Specification Book 1: Business Description; Version 1.0; May 31, 1997. Consulta a 26/11/2015. Em: http://www.maithean.com/docs/set_bk1.pdf.

UNCITRAL. (1985). *United Nations Commission on International Trade Law Recommendation on the Legal Value of Computer Records*. New York.

UNCITRAL. (1987). *UNCITRAL Legal Guide on Electronic Funds Transfer*. United Nations publication Sales No. E.87.V.9 ISBN 92-1-133299-0 A/CN.9/SERB/1, V.87-84017-July 1987. New York.

UNCITRAL. (2002). *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*. United Nations Publication, Sales No. E.02.V.8, ISBN 92-1-133653-8. New York.

UNCITRAL. (2007). *United Nations Convention on the Use of Electronic Communications in International Contracts*. United Nations Commission on International Trade Law; United Nations. New York.

UNCITRAL. (2007). *United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea*; United Nations Commission on International Trade Law; United Nations. Vienna.

UNCITRAL. (2009). *Promoting Confidence in Legal Issues on International Use of Electronic Authentication and Signature Methods.* United Nations Commission on International Trade Law; United Nations. Vienna.

Regulamento de Execução (UE) 2015/806, da Comissão, de 22 de maio de 2015.

Regulamento de Execuçao (UE) 2015/1501 da Comissão, de 8 de Setembro de 2015;

Regulamento de Execuçao (UE) 2015/1502 da Comissão, de 8 de Setembro de 2015;

Decisão de Execuçao (UE) 2015/1505 da Comissão, de 8 de Setembro de 2015;

Decisão de Execuçao (UE) 2015/1506 da Comissão, de 8 de Setembro de 2015;

Decisão de Execuçao (UE) 2016/650 da Comissão, de 25 de abril de 2016;

Decisão da Comissão, de 7 de julho de 2014, que alterou o Rgeulamento Interno (2004/563/CE Euratom;