

# REVISTA DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

---

LISBON LAW REVIEW



Homenagem ao Professor José de Oliveira Ascensão

ANO LXIV

2023

NÚMERO 1 | TOMO 3

REVISTA DA FACULDADE DE DIREITO  
DA UNIVERSIDADE DE LISBOA  
Periodicidade Semestral  
Vol. LXIV (2023) 1

LISBON LAW REVIEW

---

#### COMISSÃO CIENTÍFICA

Alfredo Calderale (Professor da Universidade de Foggia)  
Christian Baldus (Professor da Universidade de Heidelberg)  
Dinah Shelton (Professora da Universidade de Georgetown)  
Ingo Wolfgang Sarlet (Professor da Pontifícia Universidade Católica do Rio Grande do Sul)  
Jean-Louis Halpérin (Professor da Escola Normal Superior de Paris)  
José Luis Díez Ripollés (Professor da Universidade de Málaga)  
José Luís García-Pita y Lastres (Professor da Universidade da Corunha)  
Judith Martins-Costa (Ex-Professora da Universidade Federal do Rio Grande do Sul)  
Ken Pennington (Professor da Universidade Católica da América)  
Marc Bungenberg (Professor da Universidade do Sarre)  
Marco Antonio Marques da Silva (Professor da Pontifícia Universidade Católica de São Paulo)  
Miodrag Jovanovic (Professor da Universidade de Belgrado)  
Pedro Ortego Gil (Professor da Universidade de Santiago de Compostela)  
Pierluigi Chiassoni (Professor da Universidade de Génova)

---

#### DIRETOR

M. Januário da Costa Gomes

---

#### COMISSÃO DE REDAÇÃO

Paula Rosado Pereira  
Catarina Monteiro Pires  
Rui Tavares Lanceiro  
Francisco Rodrigues Rocha

---

#### SECRETÁRIO DE REDAÇÃO

Guilherme Grillo

---

#### PROPRIEDADE E SECRETARIADO

Faculdade de Direito da Universidade de Lisboa  
Alameda da Universidade – 1649-014 Lisboa – Portugal

---

#### EDIÇÃO, EXECUÇÃO GRÁFICA E DISTRIBUIÇÃO LISBON LAW EDITIONS

Alameda da Universidade – Cidade Universitária – 1649-014 Lisboa – Portugal

---

ISSN 0870-3116

---

Depósito Legal n.º 75611/95

Data: Julho, 2023

## TOMO 1

---

M. Januário da Costa Gomes  
13-44 Editorial

## ESTUDOS DOUTRINAIS

- 
- Alexandre Libório Dias Pereira  
47-56 Filtros de conteúdos digitais para infrações ‘óbvias’ aos direitos autorais?  
*Upload filters for copyright ‘obvious’ infringement?*
- 
- Alfredo Calderale  
57-83 *Posse pro-labore* e proprietà in Brasile tra conflitti sociali e tradizione giuridica portoghese  
*Posse pro-labore and property in Brazil between social conflict and portuguese legal tradition*
- 
- Ana Alves Leal | Tiago Fidalgo de Freitas  
85-133 Sobre a liquidação de fundações  
*On the liquidation of foundations*
- 
- André Moreira Simões  
135-181 Cláusulas MAC (“*Material Adverse Change*”) em contratos internacionais de M&A  
*Material Adverse Change (“MAC”) Clauses in International M&A Contracts*
- 
- António Barroso Rodrigues  
183-239 Em defesa da legítima defesa. Um olhar sobre os limites da justificação na dogmática civil moderna  
*In defence of self-defence. A glance at the limits of justification in modern civil dogmatics*
- 
- António Menezes Cordeiro  
241-276 Propriedade horizontal e alojamento local  
*Horizontal property and holiday rentals*
- 
- António Pedro Barbas Homem  
277-296 Legitimidade na revolução de 1820  
*The legitimacy of the 1820 Revolution*
- 
- Aquilino Paulo Antunes  
297-328 Mecanismos de incentivo à investigação e desenvolvimento de medicamentos: existe alternativa?  
*Mechanisms to encourage research and development of medicines: is there an alternative?*
- 
- Augusto Teixeira Garcia  
329-377 Marca: caducidade por não utilização séria e renovação  
*Trademark: Revocation for non-use and renewal*

- 
- 379-403 **Carlos Baptista Lobo | Daniel S. de Bobos-Radu**  
Uma arte de escribas e fariseus: nota sobre os limites da extensão da incidência do IRC aos rendimentos derivados da prestação de serviços jurídicos por entidades não residentes em território nacional  
*An art of scribes and Pharisees: remark on the limits of the Portuguese Corporate Income Tax liability of income derived from the provision of legal services by non-resident entities*
- 
- 405-442 **Carlos Blanco de Moraes | Mariana Melo Egídio**  
Da validade dos acordos de financiamento de contencioso por terceiros para a promoção de ações populares  
*On the validity of third-party litigation funding backing class action lawsuits*
- 
- 443-466 **Catarina Salgado**  
A arbitragem voluntária como meio de resolução extrajudicial de conflitos no direito angolano – alguns subsídios  
*Voluntary arbitration as a method for extrajudicial conflict resolution in Angolan law – some subsidies*
- 
- 467-495 **Daniel de Bettencourt Rodrigues Silva Moraes**  
A escolha de lei tácita: alguns problemas  
*Tacit choice of law: difficulties it raises*
- 
- 497-512 **Dário Moura Vicente**  
Desinformação, liberdade e responsabilidade  
*Disinformation, freedom and liability*
- 
- 513-554 **Diogo Costa Gonçalves**  
Relatório sobre a disciplina de Direitos de Personalidade  
*Personality Rights Academic Report*
- 
- 555-587 **Diogo Tapada dos Santos**  
Interpretação extensiva e analogia de normas excepcionais: reflexões a propósito da proibição do pacto comissório  
*Extensive interpretation and analogy of exceptional rules: reflections on the lex commissoria prohibition*
- 
- 589-634 **Eduardo Vera-Cruz Pinto**  
O pensamento jurídico analógico e a criação de Direito em Sociedades Digitais: o eterno retorno da analogia?  
*Analogical legal thinking and the creation of the Law in digital societies: the eternal return of analogy?*
- 
- 635-668 **Evaristo Mendes**  
Sociedades preliminares e sociedades em formação  
*Companies Before Incorporation*

---

**Filipe A. Henriques Rocha**  
669-708 A Arbitragem de litígios sobre dados pessoais  
*Arbitration of personal data disputes*

---

**Filipe de Arede Nunes**  
709-728 Nas vésperas da revisão constitucional de 1989: iniciativas e roteiros parlamentares  
*On the eve of the 1989 constitutional revision: parliamentary initiatives and routes*

## TOMO 2

---

**Flávio Tartuce**  
729-752 Os direitos da personalidade no código civil brasileiro. Diálogos com a doutrina do Professor José de Oliveira Ascensão  
*Personality rights in the Brazilian Civil Code. Dialogues with the doctrine of Professor José de Oliveira Ascensão*

---

**Francisco A. C. P. Andrade**  
753-771 Vícios de Vontade dos “agentes” de *Software*?  
*Software agent's defects of will?*

---

**Francisco Mendes Correia**  
773-800 O Direito natural na tradição aristotélico-tomista: esboço de uma defesa  
*A first attempt in the defense of Natural law in the Aristotelian-Thomistic Tradition*

---

**Francisco Paes Marques**  
801-826 Ação popular e *private enforcement*: nova vida europeia de um velho instituto nacional  
*Class actions and private enforcement: new European life of an old national legal remedy*

---

**Gonçalo Aleixo Nunes**  
827-884 Da penhora de direitos de crédito – em especial, as garantias de defesa do *debitor debitoris*, a execução concomitante e a legitimidade processual do exequente  
*The seizure of receivables – in particular, the guaranties of defence of the third debtor, the concurrent enforcement and the procedural legitimacy of the creditor*

---

**Henrique Marques Candeias**  
885-930 O abuso do direito de retenção. Exercício desproporcional do direito de retenção  
*The abuse of the right of retention. Disproportionate exercise of the right of retention*

---

**Hugo Ramos Alves**  
931-962 A desconsideração da personalidade coletiva em Oliveira Ascensão  
*Oliveira Ascensão and the disregard of the corporate veil doctrine*

---

**Isabel Alexandre**  
963-985 Reconhecimento e execução de acordos resultantes de mediação  
*Recognition and Enforcement of Mediated Settlements*

- 
- Isabel Graes**  
987-1027 As cartas de seguro na história do direito português: um instrumento de protecção do réu  
*The security charts in the History of the Portuguese Law: an instrument to protect the defendant*
- 
- Ivanildo Figueiredo**  
1029-1080 Registo dos direitos reais e da posse: Aspectos distintivos entre os sistemas de Portugal e do Brasil à luz da doutrina de José de Oliveira Ascensão  
*Registration of real rights and possession: Distinctive aspects between the systems of Portugal and Brazil based on the doctrine of José de Oliveira Ascensão*
- 
- J. P. Remédio Marques**  
1081-1115 Defesa preventiva e providências cautelares: a introdução, em Portugal, do “requerimento de protecção”, face ao possível decretamento de providência cautelar *inaudita altera parte* – A questão no quadro da propriedade intelectual  
*Preventive defense and interim injunctions: the introduction, in Portugal, of “protective letters”, in view of the possible award of an interim injunction without the prior contradictory of the same respondent (inaudita altera parte) – The issue in the context of intellectual property rights*
- 
- Jaime Reis**  
1117-1170 O penhor flutuante como penhor de universalidades: ensaio de fundamentação dogmática  
*The floating charge as a charge of universalities: an essay on its dogmatic foundations*
- 
- Joana Costa Lopes**  
1171-1206 Os desafios à tutela judicial civil do direito à imagem na era digital  
*The challenges to the judicial protection of the image right in the digital era*
- 
- João de Oliveira Gerales**  
1207-1248 Sobre o reconhecimento de decisões eclesíásticas em matéria matrimonial: o artigo 99.º do Regulamento Bruxelas II *ter* e a Concordata de 2004 entre a República Portuguesa e a Santa Sé  
*On Recognition of Ecclesiastical Judgments in Matrimonial Matters: Article 99 of the Brussels II ter Regulation and the 2004 Concordat Between the Portuguese Republic and the Holy See*
- 
- João Maurício Adeodato**  
1249-1260 Imprecisão da linguagem jurídica no exemplo do conceito de imperatividade (Em homenagem a José de Oliveira Ascensão)  
*Inaccuracy of legal language in the example of the concept of imperativity (In honor of José de Oliveira Ascensão)*
- 
- Jones Figueirêdo Alves**  
1261-1306 Pessoa como sujeito de direito e o Direito da Pessoa em suas moradas do ser: visões identitárias a partir de estudos doutriniais de Oliveira Ascensão  
*Person as subject of rights and the Personal Law in its being's abode: identitary perspectives based on doctrinal studies of Oliveira Ascensão*

- **Jorge Miranda**  
1307-1314 A Constituição e a língua  
*The Constitution and the portuguese language*
- **José Alberto Vieira**  
1315-1338 Oliveira Ascensão e a crítica ao conceito de relação jurídica  
*Oliveira Ascensão and the critique of the concept of legal relationship*
- **José Ferreira Gomes**  
1339-1378 A eficácia das declarações a pessoas coletivas  
*The effectiveness of declarations to legal persons*
- **José Luís Bonifácio Ramos**  
1379-1406 Alojamento Local e Condomínio  
*Airbnb or Short-Term Rental and Condominium*
- **Luourenço Vilhena de Freitas | Catarina Teles de Menezes**  
1407-1426 Pandemia Covid-19 e a Reposição do Equilíbrio Económico-Financeiro dos Contratos de Concessão  
*Covid-19 Pandemic and the Restoration of the Economic-Financial Balance of the Concession Contracts*
- **Luís de Lima Pinheiro**  
1427-1448 Direito aplicável, equidade e composição amigável na arbitragem  
*Applicable law, ex aequo et bono and amicable composition in arbitration*
- **Luís Manuel Teles de Menezes Leitão**  
1449-1468 O novo Regulamento Europeu 2022/2065 sobre os Serviços Digitais: o *Digital Services Act (DSA)*  
*The New European Regulation 2022/2065 on Digital Services: The Digital Services Act (DSA)*
- **M. Januário da Costa Gomes**  
1469-1501 “Supomos que esta descrição legal da situação é inaceitável”. Sobre a “sub-rogação dos credores” do repudiante na aceitação da herança e a interpretação disruptiva de José de Oliveira Ascensão  
*“We believe that such legal description of the situation is unacceptable”. On the “creditors subrogation” of the waivant in the acceptance of the inheritance and the disruptive interpretation of José de Oliveira Ascensão*

## TOMO 3

- **Manuel Carneiro da Frada**  
1503-1515 “Quando os lobos uivam...” – Sobre a tríplice tutela dos direitos subjectivos, a respeito de um trecho de Oliveira Ascensão (e de um acórdão da Relação de Coimbra sobre baldios)  
*“When wolves howl...” – On the triple protection of subjective rights, about an excerpt from Oliveira Ascensão (and a judgment of the Relação de Coimbra about the common land)*

- 
- Marco Caldeira**  
1517-1550 A colusão na contratação pública (em especial, a participação de empresas em relação de grupo): o “estado da arte” e perspectivas futuras  
*The bid-rigging in public procurement procedures (in particular, in regard to linked undertakings): the state of the art and future developments*
- 
- Margarida Silva Pereira**  
1551-1600 Ainda sem direito à identidade: as crianças na Gestação de Substituição segundo a (incompleta) Lei n.º 90/2021, de 16 de dezembro  
*Still no right to identity. Children of surrogacy under the (incomplete) Law n.º 90/2021, 16/12, which amended the Medically-Assisted Procreation Law*
- 
- Maria Raquel Rei**  
1601-1617 Mandato com vista a acompanhamento  
*Mandate to assist the vulnerable*
- 
- Marta Boura**  
1619-1662 A culpa do lesado e o abuso do direito. Considerações sobre a disfuncionalidade do exercício e o fundamento dogmático do instituto da culpa do lesado  
*The fault of the injured party and the abuse of right. Considerations on the dysfunctionality of the exercise and the dogmatic basis of the fault of the injured party*
- 
- Miguel de Lemos**  
1663-1688 Oliveira Ascensão, Direito Vivo e Pluralismo Jurídico em Água Branca – Entre *Factos* e *Mitos*: um Estudo de Sociologia Jurídica  
*Oliveira Ascensão, Living Law and Legal Pluralism in Água Branca – Between Facts and Myths: a Socio-Legal Study*
- 
- Miguel Teixeira de Sousa**  
1689-1702 Poderes do juiz no processo do trabalho: algumas notas  
*On the powers of the court in labor proceedings: some remarks*
- 
- Míriam Afonso Brigas**  
1703-1724 A Culpa como pressuposto da Acção de separação de pessoas e bens no Código Civil de 1867 – Breves notas  
*Guilt as a prerequisite for the Action of Separation of Persons and Property in the Civil Code of 1867 – Brief notes*
- 
- Nuno de Oliveira Garcia | Ana Paula Basílio**  
1725-1740 A tributação das mais-valias em IRS e o princípio da capacidade contributiva  
*Personal income tax on capital gains and the ability to pay principle*
- 
- Paula Costa e Silva | Nuno Trigo dos Reis**  
1741-1779 A morte de um comparte e o curioso caso da instância subjectivamente complexa: a lacuna oculta no art. 281.º CPC e a verdade do aforismo *nanos gigantum humeris*  
*The death of one of the defendants and the curious case of the subjectively complex proceedings: the hidden gap in art. 281 Civil Procedure Code and the truth of the aphorism nanos gigantum humeris*

- 
- Paulo Marques**  
1781-1822 Breves notas sobre a prestação de garantia idónea no processo de execução fiscal  
*Brief notes on the provision of adequate surety in tax enforcement proceedings*
- 
- Pedro de Albuquerque**  
1823-1876 A informação sensível a dar a administradores e membros do Conselho Geral e de Supervisão (em cenários de concorrência, efetiva ou potencial, na eventualidade de negação de autorização para o exercício de atividade concorrencial ou antes dessa autorização poder ser dada pelo órgão previsto)  
*The sensitive information to be given to directors and members of the General and Supervisory Board (in actual or potential competition scenarios, in the event of denial of authorisation to engage in competitive activity or before such authorisation can be given by the body envisaged)*
- 
- Pedro Romano Martinez**  
1877-1911 Direito de preferência e autonomia privada (Da preferência sucessiva)  
*Pre-emption rights and private autonomy (Of the successive pre-emption rights)*
- 
- Renata Oliveira Almeida Menezes**  
1913-1934 A proteção jurídica da memória do morto e a titularidade do interesse tutelado  
*The legal protection of the deceased memory and the ownership of the protected interest*
- 
- Ricardo Rodrigues de Oliveira**  
1935-1968 A nova identidade digital europeia. Uma primeira abordagem  
*The new European digital identity. A first approach*
- 
- Rui Pinto**  
1969-1991 A execução de condenações implícitas  
*The enforcement of implied condemnatory judgments*
- 
- Rui Soares Pereira | Daniela Rodrigues de Sousa**  
1993-2029 Sobre o levantamento da personalidade coletiva no domínio penal  
*On piercing the corporate veil in the criminal realm*
- 
- Silvio Romero Beltrão**  
2031-2045 O futuro dos direitos da personalidade: o valor da pessoa humana na sociedade  
*The future of personality rights: the value of human person in society*
- 
- Susana Antas Videira**  
2047-2078 Remuneração Adicional do Agente de Execução – Uma Interpretação fundada [também] em elementos genéticos ou lógico-históricos  
*Additional Remuneration for Enforcement Agents – An Interpretation Based [also] on Genetic or Logical-Historical Elements*

- **Teresa Quintela de Brito**  
2079-2122 Actuação “em nome ou por conta” e no “interesse directo ou indirecto” do ente colectivo, responsabilização penal da sociedade-mãe e (ir)relevância penal dos programas de *Compliance*  
*Acting “on behalf or for the account of” and in the “direct or indirect interest” of the collective entity, criminal liability of the parent company and criminal (ir)relevance of compliance programs*
- **Thomas Hoeren**  
2123-2140 Morreu Oliveira Ascensão – uma profunda vénia a um espírito livre  
*Oliveira Ascensão has died: a deep bow to a free spirit*
- **Tiago Henrique Sousa**  
2141-2169 A aquisição tabular na compra e venda executiva  
*Acquisition a non domino an execution sale*
- **Tong Io Cheng**  
2171-2198 A exploração de terrenos vagos e a *Radix Omnium Malorum*: Reflexões (esparsas e cingidas ao essencial) sobre a Legitimidade da Propriedade Privada  
*Vacant Land Exploitation and the Radix Omnium Malorum: Reflections (sparse and limited to the essentials) on the Legitimacy of Private Property*
- **Vítor Palmela Fidalgo**  
2199-2242 A responsabilidade dos intermediários e a violação do direito de marca: *quo vadis?*  
*Intermediaries’ liability and trademark infringement: quo vadis?*

## TESTEMUNHOS ACADÉMICOS

- **Maria João Estorninho**  
2245 Em memória do Professor Doutor Oliveira Ascensão
- **Paulo de Sousa Mendes**  
2247-2248 Em memória do Professor Doutor José de Oliveira Ascensão
- **Pedro Pais de Vasconcelos**  
2249-2251 Testemunho de um discípulo do Professor Oliveira Ascensão

# A nova identidade digital europeia

## Uma primeira abordagem

### *The new European digital identity* *A first approach*

Ricardo Rodrigues de Oliveira\*

“A sociedade que nos rodeia é uma sociedade tecnologicamente avançada. O homem, no seio dela, é uma mónada altamente vulnerável: as possibilidades de intromissão na vida de cada pessoa são hoje inúmeras e ameaçadoras”\*\*

**Resumo:** As instituições europeias adoptaram conclusões conjuntas com objectivos comuns de política pública e legislativa, para o ciclo 2020-2024, no sentido de aproveitar as transformações climáticas e digitais e tornar a União Europeia mais resiliente e autónoma. Uma das prioridades da Comissão decorrentes do diálogo legislativo trilateral é a revisão da Identidade Digital Europeia para permitir aos cidadãos terem apenas uma identificação virtual no acesso a bens e serviços, ao mesmo tempo que restitui o controlo sobre a divulgação dos dados pessoais. Este artigo pretende dar conta das principais mudanças contidas na proposta de 2021 de alteração do Regulamento (UE) n.º 910/2014, relativo ao quadro europeu para a identidade digital. É uma primeira

**Abstract:** The European institutions have adopted joint conclusions with common public policy and legislative goals for the 2020-2024 cycle to capitalise on the climate and digital transformations and to make the European Union more resilient and autonomous. One of the Commission’s priorities arising from the legislative trilogue is the review of the European Digital Identity to allow citizens to have only one virtual identification when accessing goods and services, while restoring control over the disclosure of personal data. This paper gives an account of the main changes comprised in the 2021 proposal to amend Regulation (EU) No 910/2014, on the European framework for the digital identity. It is a first approach, at a time when there is still limited

\* Professor auxiliar convidado e investigador contratado da Universidade Católica Portuguesa, Católica Research Centre for the Future of Law, Portugal. Investigador colaborador do Lisbon Public Law Research Centre da Faculdade de Direito da Universidade de Lisboa.

\*\* JOSÉ DE OLIVEIRA ASCENSÃO, *A dignidade da pessoa e o fundamento dos direitos humanos*, “Revista da Faculdade de Direito da Universidade de São Paulo”, volume 103, 2008, página 284.

abordagem, numa altura em que ainda há pouco debate doutrinal e não se conseguem aferir os efeitos destas modificações no mercado interno. Não obstante, parece pertinente dar a conhecer este desenvolvimento, especialmente pelo potencial impacto na vida dos utilizadores.

**Palavras-chave:** estratégia digital; União Europeia; identidade digital europeia; *e-wallet*; serviços de confiança.

doctrinal debate and it is not yet possible to gauge the effects of these modifications on the internal market. It seems pertinent, nevertheless, to make this development known, especially for the potential impact on the lives of users.

**Keywords:** digital strategy; European Union; european digital identity; e-wallet; trust services.

**Sumário:** Introdução; §1. A estratégia digital da Comissão; §2. Outros instrumentos jurídicos; §3. A identidade digital europeia; 3.1. A Directiva de 1999 e o quadro regulamentar de 2014; 3.2. A avaliação e a proposta de 2021; 3.3. Objectivos e harmonização; 3.4. Carteiras, atributos e certificados; 3.4.1. Conceito; 3.4.2. Atributos; 3.4.3. Sistema; 3.4.4. Segurança; 3.5. Serviços de confiança; 3.5.1. Identificação; 3.5.2. Assinaturas; 3.5.3. Selos; 3.5.4. Arquivos; 3.5.5. Livros-razão; 3.6. (Outras) garantias de segurança; Conclusões.<sup>\*\*\*</sup>

## Introdução

Não tive o privilégio de conhecer pessoalmente o Senhor Professor José de Oliveira Ascensão nem de ser seu aluno. O seu impacto na minha vida académica e na de tantos estudantes é, não obstante, incontornável. A leccionação da cadeira de Introdução ao Estudo do Direito na Faculdade de Direito da Universidade de Lisboa tinha como manual basilar, aquando da minha Licenciatura, a sua obra *O Direito. Introdução e teoria geral*<sup>1</sup>. Os demais livros e artigos eram, pelo menos na óptica dos alunos e com o devido respeito, complementares. Não sei se tal ainda sucede, mas quero acreditar que sim. Continua a ser um texto de referência, mesmo com tantos anos passados desde a primeira vez que adquiri a minha cópia. A obra e o seu autor são quase indissociáveis no ideário académico português, que

---

<sup>\*\*\*</sup> Lista das abreviaturas utilizadas: eIDAS: Regulamento relativo à Identificação Electrónica e aos Serviços de Confiança; EM: Estado-Membro da União Europeia; IA: Inteligência Artificial; IDE: Identidade Digital Europeia; JO: Jornal Oficial da União Europeia; PE: Parlamento Europeu; RGD: Regulamento Governação de Dados; RGPD: Regulamento Geral sobre a Protecção de Dados; RMD: Regulamento dos Mercados Digitais; RSD: Regulamento dos Serviços Digitais; UE: União Europeia.

<sup>1</sup> JOSÉ DE OLIVEIRA ASCENSÃO, *O Direito. Introdução e teoria geral*, 13.<sup>a</sup> edição, Coimbra, 2022.

empobreceu significativamente com o desaparecimento do Senhor Professor a 6 de Março de 2022.

Como pedido pelos organizadores da colectânea, o presente texto toca em alguns temas que o homenageado investigava, mormente que ver com o Direito da sociedade de informação e o Direito da União Europeia. De forma exploratória e não exaustiva, o estudo dá nota das principais propostas de revisão das normas europeias de 2014 sobre a Identidade Digital Europeia<sup>2</sup>, inserida na actual estratégia trilateral digital da UE, sobretudo na perspectiva do tratamento e garantia das informações pessoais dos cidadãos dos Estados-Membros. É uma reflexão doutrinária sobre um esboço legislativo que ainda tem um considerável caminho formal e material a percorrer, mas que poderá trazer diversas vantagens no domínio do mercado interno, bem como para a segurança e controlo, de *iure* e de facto, dos dados dos indivíduos. Para além da própria novidade da legislação, o interesse da investigação reside no facto de a IDE ser ainda relativamente desconhecida do ambiente doutrinário português, apesar de este estar cada vez mais atento às mudanças no campo dos dados pessoais e da ligação entre o Direito e a tecnologia.

O trabalho está organizado em três secções substantivas. A primeira enquadra e introduz à estratégia digital da Comissão, que faz parte dos objectivos políticos gerais que orientam a UE neste momento, no âmbito das prioridades para o hiato 2020-2024. A Comissão dialoga periodicamente com o Parlamento Europeu e o Conselho para desenhar estratégias a médio prazo, que depois materializa por meio de políticas e iniciativas específicas. A estratégia digital é uma das prioridades da actual Comissão e a sua concretização tem um impacto significativo no mercado interno e nas actividades desenvolvidas no espaço europeu.

São vários os projectos que estão a ser levados a cabo no campo digital, sendo que a segunda secção irá dar conta, de forma abreviada, do que de mais relevante está a ser feito à altura da escrita deste texto. Assim se compreenderá melhor o contexto em que a IDE está a ser revista e repensada. Uma das motivações mais palpáveis das instituições é que as normas aplicáveis ao panorama digital e à circulação de informação tenham um cunho marcadamente europeu. Há uma

---

<sup>2</sup> Este trabalho segue, em parte, na esteira de outro texto igualmente escrito em homenagem ao Senhor Professor José de Oliveira Ascensão, a saber MIGUEL PUPO CORREIA, Nota breve sobre o novo quadro legal europeu dos “serviços de confiança”, in *Estudos de direito intelectual em homenagem ao Prof. Doutor José de Oliveira Ascensão: 50 anos de vida universitária*, Dário Moura Vicente, Alexandre Dias Pereira e José Alberto Vieira (coord.), Coimbra, 2015, páginas 459-470.

axiologia própria, decorrente do Direito primário (constitucional, se se quiser), que a Comissão quer ver presente no mundo virtual, especialmente em face do lastro de acordos com países terceiros que nem sempre têm protegido os cidadãos europeus na extensão do previsto pelo Direito interno. Este cunho é evidente, desde logo, na diversidade e abrangência dos projectos – que vão desde a regulação da Inteligência Artificial até à gestão do espaço sideral – e a IDE não é excepção. Aliás, pelo contrário: a IDE e as suas revisões são um claro exercício de harmonização do Direito e de aprofundamento da integração europeia, revelando tanto a preocupação institucional em que os indivíduos estejam em pleno controlo dos seus dados pessoais como a vontade em concretizar as liberdades fundamentais de circulação e em aproximar a UE das pessoas.

A terceira secção vai ao cerne da investigação e trata, portanto, de explorar as mais recentes propostas de alteração e alargamento da IDE. Começa por visitar o quadro regulamentar de 2014 e as suas origens em 1999. Partindo da avaliação feita entre 2019 e 2021, a reflexão debruça-se, em seguida, sobre os aspectos essenciais da proposta para uma nova IDE, focando-se, em particular, nas carteiras digitais. A IDE é um projecto de continuidade mais do que de ruptura. Mas os desenvolvimentos tecnológicos permitiram uma sofisticação jurídica tão substancial que a proposta de Regulamento em cima da mesa é marcadamente mais robusta e inovadora do que os instrumentos que a antecederam. Só agora é que será possível afirmar que estamos perante uma verdadeira e segura identidade digital à disposição dos cidadãos europeus.

Este trabalho não tem pretensão de esgotar o tema, desde logo porque o novo quadro normativo ainda é uma proposta e está pouco discutido. Pretende-se, antes, apresentar esta matéria e levantar algumas questões sobre a digitalização da vida e do Direito – tal como o Senhor Professor José de Oliveira Ascensão gostava de fazer na sua investigação.

## §1. A estratégia digital da Comissão

A Comissão tem seis prioridades políticas para o período 2020-2024, que vão desde tornar a Europa no primeiro continente a atingir a neutralidade carbónica até à promoção de um estilo de vida europeu e assente nos valores fundamentais da UE<sup>3</sup>. Estas prioridades resultam de um diálogo institucional trilateral com o

---

<sup>3</sup> As prioridades estão elencadas sob títulos apelativos nos canais oficiais da UE. Estes são, na versão mais divulgada em Inglês (sendo que ainda não há uma tradução oficial em Português), *a European green deal, a Europe fit for the digital age, an economy that works for people, a stronger Europe in the*

PE e o Conselho. Pela primeira vez, em 2020, foram adoptadas conclusões conjuntas com objectivos comuns de política pública e legislativa. Para este ciclo, a ênfase foi colocada na recuperação dos efeitos provocados pela pandemia resultante da doença COVID-19 e no aproveitamento das oportunidades das “*twin climate and digital transformations*”<sup>4</sup> para revitalizar a Europa e torná-la estrategicamente mais autónoma de países terceiros.

Na parte relevante para esta reflexão, as conclusões priorizam a transição acelerada para uma sociedade mais digital, apostada na investigação, desenvolvimento e capacidade de inovação, em particular nos sectores da energia, computação de alta *performance* e IA. O documento sublinha ainda que a crise de saúde pública global antecipou a hiper-conectividade e a integração de novas tecnologias nas mais diversas áreas, como a educação, emprego, socialização e consumo. Mas também expôs as vulnerabilidades da UE, desde os riscos com a cibersegurança à insuficiente cobertura telemática de algumas regiões. Donde, as instituições decidiram que a posição da UE na economia global e a defesa dos valores europeus só poderiam ser garantidas através de soluções tecnológicas próprias e da afirmação da soberania digital da UE. Para tal, torna-se imperativo manter a aposta na protecção dos dados pessoais, desenvolvimento de tecnologia inovadora e melhoramento das infra-estruturas de suporte.

A 15 de Setembro de 2021, a Comissão propôs um Guião para a Década Digital<sup>5</sup> onde expôs mais concretamente as suas ambições a alcançar até 2030, designadamente na área das competências e da digitalização dos serviços. Com base numa anterior comunicação sobre orientações de digitalização<sup>6</sup>, o quadro governativo pretende que os EM cooperem para se alcançar um patamar relativamente semelhante de digitalização. O Guião prevê elementos como um “sistema de acompanhamento estruturado, transparente e partilhado (...) destinado [a] medir os progressos na consecução de cada uma das metas fixadas para 2030, incluindo indicadores-chave de desempenho”<sup>7</sup>, um relatório periódico de avaliação dos progressos, “[r]oteiros estratégicos plurianuais

---

*world, promoting our European way of life e a new push for European democracy. Veja-se As prioridades da Comissão Europeia* (consultado a 2 de Dezembro de 2022).

<sup>4</sup> *Joint Conclusions of the European Parliament, the Council of the European Union and the European Commission on Policy Objectives and Priorities for 2020-2024*, 17 de Dezembro de 2020 (consultado a 13 de Dezembro de 2022).

<sup>5</sup> Proposta de decisão do Parlamento Europeu e do Conselho que estabelece o programa para 2030 intitulado «Guião para a Década Digital» (COM(2021) 574 final 2021/0293 (COD), 15.9.2021).

<sup>6</sup> Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões ‘Orientações para a digitalização até 2030: a via europeia para a década digital’ (COM(2021) 118 final, 9.3.2021).

<sup>7</sup> *Estado da União: Comissão propõe um Guião para a Década Digital a fim de concretizar a transformação digital da UE até 2030*, 15 de Setembro de 2021 (consultado a 23 de Dezembro de 2022).

[com] as políticas e medidas adotadas ou planeadas”<sup>8</sup> e uma ferramenta que facilite a realização dos projectos plurianuais. A monitorização da digitalização e da evolução da capacitação dos EM, bem como a implementação dos roteiros, serão feitas através do denominado índice de digitalidade da economia e da sociedade, em utilização desde 2014<sup>9</sup>.

As instituições acordaram em objectivos claros mas ambiciosos de digitalização, pelo que o desígnio temporal até 2030 só poderá ser respeitado se trabalharem em conjunto. No seguimento daquelas primeiras conclusões e do Guião, surgiram declarações mais pormenorizadas a nomear as prioridades legislativas para os anos de 2021<sup>10</sup> e 2022. A de 2022 dispunha que um dos objectivos políticos basilares que deveria ter precedência nesse ano era preparar o continente para a era digital, assumindo a Europa a direcção global da produção de meios tecnológicos seguros, de confiança e antropocêntricos. O foco esteve nos serviços e mercados digitais, IA, dados pessoais e segurança das transmissões espaciais, almejando-se “melhorar a ciber-resiliência[,] promover uma economia dos dados dinâmica [e reforçar] ainda mais o investimento da Europa em capacidades de inovação e tecnológicas”<sup>11</sup>. Considerando o Guião, as ambições das conclusões conjuntas de 2020 e o facto de que a priorização da digitalização constava na declaração anual de 2021<sup>12</sup>, é expectável que esta continue a ser incluída como uma das prioridades legislativas na declaração de 2023 e nas subsequentes.

Estes desenvolvimentos levaram a que uma das prioridades para o intervalo actual seja a adopção pela Comissão de uma estratégia digital para a Europa. Esta estratégia pretende tornar o continente apto para a era moderna e empoderar as pessoas através de uma nova geração de tecnologias<sup>13</sup>. A necessidade de um plano desta natureza nasce do reconhecimento de que as tecnologias digitais estão a mudar a vida das pessoas e da ambição de fazer com que tal sirva tanto os cidadãos

---

<sup>8</sup> *Estado da União*. Alguns dos domínios de investimento dos primeiros projectos plurinacionais são as infra-estruturas de dados, processadores de baixo consumo, comunicações 5G, computação de alto desempenho, comunicações quânticas, competências digitais das pessoas e tecnologias *blockchain*.

<sup>9</sup> *The Digital Economy and Society Index (DESI)*, 16 de Setembro de 2022 (consultado a 23 de Dezembro de 2022).

<sup>10</sup> *Joint declaration of the European Parliament, the Council of the European Union and the European Commission ‘EU legislative priorities for 2021’*, 17 de Dezembro de 2020 (consultado a 13 de Dezembro de 2022).

<sup>11</sup> Declaração conjunta do Parlamento Europeu, do Conselho da União Europeia e da Comissão Europeia ‘Prioridades legislativas da UE para 2022’, 21 de Dezembro de 2021 (2021/C 514 I/01), página 2.

<sup>12</sup> *Joint declaration ‘EU legislative priorities for 2021’*, página 2.

<sup>13</sup> *Uma Europa preparada para a era digital*, 19 de Fevereiro de 2020 (consultado a 13 de Dezembro de 2022).

como as empresas. Aliás, a estratégia digital será instrumental para o sucesso das demais prioridades, nomeadamente para a utilização adequada dos recursos tecnológicos no combate às alterações climáticas.

A ideia da Comissão é que esta seja a década digital da Europa, sobretudo no sentido de se criarem padrões normativos europeus de utilização dos dados pessoais. Há já, nesse sentido, uma estratégia europeia para os dados<sup>14</sup>. Nota-se um propósito claro de aplicar às actividades desenvolvidas no território dos EM – independentemente da nacionalidade das empresas e dos operadores económicos – regras de matriz europeia e não, ou não apenas, normas de países terceiros, especialmente no que tenha que ver com o foro da resolução de litígios. Para além disso, espera-se que 80% da população europeia apresente competências digitais básicas até 2030, o que será crucial para que os cidadãos tenham um maior controlo sobre as respectivas informações pessoais, o seu tratamento e destino.

## §2. Outros instrumentos jurídicos

A estratégia digital assenta num conjunto de mecanismos político-legislativos que abrange diversas áreas tecnológicas e científicas. Esta investigação vai focar-se na identidade digital – a IDE, como referido – mas é relevante perceber o que está a ser feito ao mesmo tempo para se localizar esta proposta no seu contexto, assim se compreendendo melhor o alcance da visão da Comissão. Apesar de serem diversos os projectos em crescimento no seio da UE, serão apenas mencionados aqueles que mais impacto poderão ter nos dados pessoais dos cidadãos europeus.

Os dois instrumentos mais amplamente divulgados da estratégia digital são os Regulamentos Mercados Digitais<sup>15</sup> e Serviços Digitais<sup>16</sup>. Foram ambos propostos em Dezembro de 2020, tendo entrado em vigor a 1 e 16 de Novembro de 2022, respectivamente. O RMD pretende garantir um acesso aos mercados digitais mais justo, equilibrado e livre, regulando a actuação dos controladores de acesso. Para tal, elenca critérios para classificar as maiores e mais estabelecidas empresas

---

<sup>14</sup> Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões ‘Uma estratégia europeia para os dados’ (COM(2020) 66 final, 19.2.2020).

<sup>15</sup> Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho de 14 de Setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais) (JO L 265/1, 12.10.2022).

<sup>16</sup> Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de Outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais) (JO L 277/1, 27.10.2022).

e impor obrigações e restrições em favor do dinamismo concorrencial. Ser-lhes-á proibido, por exemplo, rastrear os utilizadores finais para além do necessário para a prestação de serviços essenciais e de lhes dirigir publicidade personalizada sem o seu consentimento expresso. De outro modo, aos utilizadores profissionais das plataformas será permitido aceder a todos os dados que gerem quando as utilizem. As coimas pecuniárias são avultadas e podem somar-se a medidas correctivas adicionais, mesmo de natureza não financeira. Já o RSD pretende melhorar a supressão de conteúdos ilegais na internet e aumentar a protecção dos direitos fundamentais dos utilizadores. Reforça, nesse sentido, os poderes de supervisão das plataformas e adopta diversas medidas, tais como um mecanismo colaborativo de sinalização de conteúdos que permite o contraditório, novas obrigações de rastreabilidade dos utilizadores empresariais para se combater a venda ilegal de produtos, a proibição de determinados anúncios que se dirijam a crianças ou que utilizem categorias sensíveis de dados ou a exigência de auditorias independentes a plataformas de grandes dimensões para aumentar a transparência das suas operações.

Também a IA é um campo de incidência regulatória crescente. Há já um conjunto de instrumentos normativos e de iniciativas que se poderão inclusivamente cruzar com a IDE, desde logo porque a leitura das informações electrónicas contidas nas carteiras digitais deverá ser feita por autómatos. O Plano Coordenado para a IA de 2018<sup>17</sup> tem permitido o progresso integrado das políticas nacionais e a revisão de 2021<sup>18</sup> adaptou-o às prioridades digitais e ambientais da Comissão. Um dos objectivos estratégicos é garantir que as tecnologias estão ao serviço das pessoas. Isto será alcançado através do primeiro quadro jurídico nesta matéria<sup>19</sup>, que virá, por exemplo, proibir o risco inaceitável e as ameaças aos cidadãos e restringir o risco elevado através de normas limitativas da liberdade e cognoscibilidade das ferramentas de IA, como quanto à classificação de exames, triagem de currículos em processos de recrutamento, atribuição de pontuação por risco em empréstimos bancários ou administração da justiça. Para além disso, a Comissão tem financiado vários projectos

---

<sup>17</sup> Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões 'Plano coordenado para a inteligência artificial' (COM(2018) 795 final, 7.12.2018).

<sup>18</sup> Apêndices à Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões 'Fomentar uma abordagem europeia da inteligência artificial' (COM(2021) 205 final, 21.4.2021).

<sup>19</sup> Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União (COM(2021) 206 final, 21.4.2021).

de IA nos mais diversos campos sociais, entre os quais a saúde e o combate à desinformação e notícias falsas<sup>20</sup>.

Em termos de utilização de informações em ambiente virtual, o desenvolvimento mais aparente reside na já referida estratégia europeia para os dados, que almeja fazer da UE um “modelo de sociedade capacitada pelos dados [onde] estes circulem livremente no [seu] interior (...) e em todos os setores, em benefício das empresas, dos investigadores e das administrações públicas”<sup>21</sup>. Tal será primeiramente concretizado através do Regulamento Governação de Dados<sup>22</sup>, que entrou em vigor a 23 de Junho de 2022 e que será aplicável a partir de 24 de Setembro de 2023. Será, muito provavelmente, crucial na implementação e sucesso da IDE visto almejar ao aumento da confiança na circulação de dados e à superação dos obstáculos técnicos à sua reutilização, bem como ao suporte de espaços de troca de dados em domínios estratégicos, envolvendo actores públicos e privados, como na saúde, energia, ambiente, mobilidade e Administração Pública. Este é o primeiro passo de uma infra-estrutura jurídica que se quer clara e justa, mas também prática e flexível, para permitir um mercado único de dados, baseado em competências europeias e numa sólida interoperabilidade interna (ancorada na capacidade de computação em nuvem), mas sem perder de vista a urgência de permitir que os utilizadores possam manter sempre os seus dados pessoais sob controlo. Ao mesmo tempo, o RGD pretende garantir um acesso cada vez melhor aos dados produzidos e recolhidos pelos dispositivos, tornando mais racionais e sustentáveis as decisões dos operadores económicos. Um segundo passo será dado com o Regulamento Dados<sup>23</sup>, proposto a 23 de Fevereiro de 2022, que complementarará o RGD com novas regras sobre a utilização e acesso a dados gerados nos diferentes sectores produtivos no seio da UE. Este instrumento determinará que os clientes possam mudar de prestador de serviços de processamento de dados em nuvem mais facilmente e até definir barreiras contra a divulgação não consentida das informações. Para além disso, pretende tornar mais transparente quem pode aceder a certos dados e em que condições o poderá fazer, nomeadamente no âmbito de serviços pós-venda e em circunstâncias excepcionais em que os organismos públicos precisem de aceder a dados detidos por privados.

---

<sup>20</sup> Comissão Europeia, *EU funded projects that use AI technology*, Abril de 2021.

<sup>21</sup> *Estratégia Europeia para os Dados* (consultado a 22 de Dezembro de 2022).

<sup>22</sup> Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de Maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados) (JO L 152/1, 3.6.2022).

<sup>23</sup> Proposta de Regulamento do Parlamento Europeu e do Conselho relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização (Regulamento Dados) (COM(2022) 68 final, 23.2.2022).

### §3. A identidade digital europeia

A 16 de Setembro de 2020, no seu discurso sobre o Estado da União, a presidente da Comissão, Ursula von der Leyen, disse, em Francês, que, “[d]e cada vez que uma aplicação ou um sítio Web nos pede que criemos uma nova identidade digital ou que nos registemos sem dificuldade através de uma grande plataforma, não fazemos a menor ideia do que efetivamente acontece aos nossos dados”<sup>24</sup>. A multiplicação de plataformas e arquivos que requerem dados pessoais para permitir o acesso a serviços virtuais ou o gozo de determinados bens faz igualmente multiplicar as *personas* que os indivíduos têm de criar em ambiente digital<sup>25</sup>. Tal amplifica os riscos de extravio, interferência ou divulgação indesejada dessas informações, especialmente considerando que boa parte dos serviços virtuais fornecidos por esses operadores de grandes dimensões dependem de sistemas de “single-sign-on”<sup>26</sup>, que não conseguem oferecer níveis adequados de segurança (garantia) às contas dos utilizadores. O cidadão acaba por não conseguir saber a dimensão da sua exposição *online* – desconhecimento esse que impede o controlo que se deve poder exercer sobre os dados pessoais a todo o momento.

Para além disso, ainda não é hoje possível à maioria dos cidadãos e residentes na UE trocar digitalmente, de forma transnacional, com um substancial nível de segurança dos dados e com custos administrativos reduzidos, informações relativas à sua identidade. A proposta de renovação da IDE vem tentar colmatar alguns destes aspectos, como a criação de demasiados perfis e contas de utilizador ou a falta de controlo sobre os dados, por forma a reduzir a insegurança e a exposição dos cidadãos em meios virtuais. Perante a crescente necessidade de sujeição a procedimentos de identificação e autenticação<sup>27</sup> para o acesso à prestação de serviços e aquisição de bens, sejam fornecidos por entidades públicas ou actores privados, uma das ideias-chave das alterações à IDE é substituir a fragmentação existente derivada do recurso a soluções nacionais díspares por uma harmonização técnica e jurídica que alcance

---

<sup>24</sup> *Discurso do Estado da União 2020*, 16 de Setembro de 2020 (consultado a 16 de Dezembro de 2022).

<sup>25</sup> De acordo com um inquérito recente do Eurobarómetro, 72% dos utilizadores gostariam de saber com maior detalhe como são tratados os seus dados pessoais quando acedem às suas contas em redes sociais e 63% dos cidadãos europeus querem uma identidade digital segura comum a todos os serviços virtuais. *Vide* Identidade Digital Europeia (consultado a 21 de Abril de 2023).

<sup>26</sup> MICHAEL KÜBACH, CHRISTIAN SCHUNCK, RACHELLE SELLUNG, e HEIKO ROSSNAGEL, Self-sovereign and decentralized identity as the future of identity management?, in *Open Identity Summit 2020*, Heiko Roßnagel, Christian Schunck, Sebastian Mödersheim e Detlef Hühnlein (eds.), Bona, 2020, página 36.

<sup>27</sup> ELIN WIHLBORG, *Secure electronic identification (eID) in the intersection of politics and technology*, “International Journal of Electronic Governance”, volume 6, número 2, 2013, páginas 143 e 144.

um sistema unificado, coeso e evolutivo de identificação pessoal a nível europeu. Este caminho não irá ficar estagnado com esta proposta nem deverá ficar tanto tempo sem revisão, desde logo porque o Direito está cada vez mais receptivo às mudanças técnicas e tecnológicas e visto que o legislador precaveu esse facto, como iremos ver. Em todo o caso, a harmonização jurídica dos meios de identificação pessoal já tem um relevante percurso histórico.

### 3.1. A Directiva de 1999 e o quadro regulamentar de 2014

Os primeiros passos da legislação da UE em termos de identidade virtual foram dados no campo das assinaturas digitais. Em Abril de 1997, a Comissão apresentou ao PE, Conselho, Comité Económico e Social e Comité das Regiões uma comunicação ampla relativa a uma potencial iniciativa em matéria de comércio electrónico<sup>28</sup>. Com base nesse texto, fez uma segunda comunicação, em Outubro, desta vez especificamente direccionada à melhoria da segurança e confiança das comunicações, mormente através de assinaturas digitais e técnicas de encriptação<sup>29</sup>. Instada pelo Conselho, a Comissão viria a concretizar as políticas apresentadas nestas comunicações dois anos depois, por meio de uma Directiva. O instrumento visava “facilitar a utilização das assinaturas electrónicas e contribuir para o seu reconhecimento legal. [Instituí-la, para isso,] um quadro legal comunitário para assinaturas electrónicas e para serviços de certificação, a fim de garantir o funcionamento adequado do mercado interno”<sup>30</sup>.

Quicá pelo seu escopo algo limitado, a Directiva vigorou em pleno até 2014, altura em que foi afastada por um Regulamento<sup>31</sup> que daria um salto manifesto em termos de identificação electrónica e segurança nas transacções, representando o primeiro esforço real de apresentar uma solução europeia de identificação pessoal

---

<sup>28</sup> Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões ‘Uma iniciativa europeia para o comércio electrónico’ (COM(97) 157 final, 16.4.1997).

<sup>29</sup> Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions ‘Ensuring security and trust in electronic communication. Towards a European framework for digital signatures and encryption’ (COM(97) 503 final, 8.10.1997).

<sup>30</sup> Artigo 1.º da Directiva 1999/93/CE do Parlamento Europeu e do Conselho de 13 de Dezembro de 1999 relativa a um quadro legal comunitário para as assinaturas electrónicas (JO L 13/12, 19.1.2000).

<sup>31</sup> Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de Julho de 2014, relativo à identificação electrónica e aos serviços de confiança para as transacções electrónicas no mercado interno e que revoga a Directiva 1999/93/CE (JO L 257/73, 28.8.2014).

interoperável<sup>32</sup>. Esta solução é herdeira de quase 20 anos de várias iniciativas financiadas pela UE, como o projecto-piloto STORK<sup>33</sup>. Com o Regulamento (UE) n.º 910/2014 (Regulamento eIDAS<sup>34</sup>), adoptado a 23 de Julho de 2014 e em vigor desde 1 de Julho de 2016<sup>35</sup>, o quadro regulatório das assinaturas digitais alargou-se para abranger selos e documentos electrónicos, bem como serviços de envio registado e autenticação de sítios na internet. Estabeleceu as condições para que as pessoas singulares e colectivas se possam identificar virtualmente nos EM, definindo ainda as normas que tornariam fiáveis os serviços relativos a transacções além-fronteiras e entre sectores de actividade<sup>36</sup>. O sistema regulamentar<sup>37</sup> – que se mantém em vigor à altura da escrita deste texto –, baseia-se numa infra-estrutura de notificações e reconhecimento mútuo que permite às autoridades nacionais confirmar, bem como rastrear, a identificação electrónica das pessoas quando circulem e comercializem no mercado interno.

---

<sup>32</sup> Apesar de alguns autores considerarem que a falta de publicitação aquando da sua discussão e adopção terá prejudicado o impacto potencial do Regulamento e a revolução digital consequente. Nesse sentido, PAUL POLAŃSKI, *Towards the single digital market for e-identification and trust services*, “Computer Law & Security Review”, volume 31, número 6, 2015, página 774.

<sup>33</sup> Acrónimo que se refere a *Secure idenTity acrOss boRders linKed* – um projecto que alcançou a edição 2.0 e que foi a base do Regulamento de 2014, bem como dos seus actos de implementação e especificações técnicas (*vide* a referência no considerando 16 do Regulamento (UE) n.º 910/2014). O seu objectivo era, precisamente, o de permitir o acesso sem barreiras legais e de semântica ou fronteiras a diversos sectores através de uma identificação digital multinacional, no sentido de facilitar a interoperabilidade com serviços públicos nas áreas dos negócios e da saúde, bem como a nível de *eLearning* ou *eBanking*. Este projecto criou as bases “towards borderless digital living and mobility in the EU”, de acordo com a página, já pouco usada, *STORK 2.0 Project*, 2 de Junho de 2020 (consultado a 5 de Janeiro de 2023). Para um estudo sobre este projecto e iniciativas similares, veja-se CARLOS RIBEIRO, HERBERT LEITOLD, SIMON ESPOSITO e DAVID MITZAM, *STORK: A real, heterogeneous, large-scale eID management system*, “International Journal of Information Security”, volume 17, número 5, 2018, páginas 569-585. Também relevante é ŽIVA STEPANČIĆ e BORKA JERMAN BLAŽIĆ, *Exploring European digital single market: User adoption and preferences for eID services*, “International Journal of Electronic Governance”, volume 10, número 4, 2018, página 383.

<sup>34</sup> eIDAS significando, no original Inglês, *electronic IDentification, Authentication and trust Services*.

<sup>35</sup> Mas com um conjunto de normas aplicáveis desde 17 de Setembro de 2014. Veja-se a alínea a) do número 2 do artigo 52.º do Regulamento (UE) n.º 910/2014.

<sup>36</sup> Artigo 1.º do Regulamento (UE) n.º 910/2014.

<sup>37</sup> Para um estudo pormenorizado do articulado do Regulamento, vejam-se, em geral, ALESSIO ZACCARIA, MARTIN SCHMIDT-KESSEL, REINER SCHULZE e ALBERTO GAMBINO (eds.), *EU eIDAS Regulation. Article-by-article commentary*, Baden-Baden, 2020, ou JOS DUMORTIER, *Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)*, in *EU regulation of e-commerce: A commentary*, Arno Lodder e Andrew Murray (eds.), 2.ª edição, Northampton, 2022, páginas 256-289.

### 3.2. A avaliação e a proposta de 2021

O artigo 49.º do Regulamento prevê uma cláusula de revisão, sendo que a Comissão ficou encarregue de analisar a sua aplicação e apresentar um relatório ao PE e ao Conselho até 1 de Julho de 2020. O estudo encomendado para avaliar a efectividade, eficácia, relevância e coerência do instrumento, para além do seu valor acrescentado, concluiu que o sistema eIDAS não permite que todos os cidadãos da UE tenham acesso a uma identidade digital plenamente segura e interoperável, sendo as falhas de segurança um dos aspectos mais prementes de revisão<sup>38</sup>, especialmente em face da entrada em vigor do Regulamento (UE) 2016/679<sup>39</sup>, comumente conhecido como Regulamento Geral sobre a Protecção de Dados. O procedimento de notificação foi descrito como complexo e demasiado lento, os protocolos de troca de dados e a implementação técnica não parecem oferecer uma experiência óptima para o utilizador, especialmente se o acesso for

---

<sup>38</sup> A este propósito, veja-se o estudo de ANTONIA RUSSO, GIANLUCA LAX, BAPTISTE DROMARD e MENAD MEZRED, *A system to access online services with minimal personal information disclosure*, “Information Systems Frontiers”, volume 24, 2022, páginas 1563-1575, em que os autores propõem um esquema baseado em tecnologia *blockchain* que respeita o Regulamento eIDAS, para permitir aos utilizadores ter maior controlo sobre os seus dados pessoais quando acedem a determinados serviços e celebram *smart contracts*. O exemplo utilizado é algo fortemente impactado pelo Regulamento: o aluguer de veículos automóveis. Só não conseguiram aditar ao estudo se haverá alguma mudança nos seus exemplos e na argumentação decorrente das alterações da proposta. Outras análises com propostas de melhoria do Regulamento baseadas em ensaios práticos podem ser encontradas em ÁLVARO ALONSO, ALEJANDRO POZO, ALDO GORDILLO, SONSOLES LÓPEZ-PERNAS, ANDRÉS MUNOZ-ARCENTALE, LOURDES MARCO e ENRIQUE BARRA, *Enhancing university services by extending the eIDAS European specification with academic attributes*, “Sustainability”, volume 12, número 3, 2020, páginas 770-789; DIANA BERBEARU, ANTONIO LIOY e CESARE CAMERONI, *On enabling additional natural person and domain-specific attributes in the eIDAS network*, “IEEE Access”, volume 9, 2021, páginas 134096-134121; ou LOURDES MARCO, ALEJANDRO POZO, GABRIEL HUECAS, JUAN QUEMADA e ÁLVARO ALONSO, *User-adapted web services by extending the eIDAS specification with functional attributes*, “International Journal of Environmental Research and Public Health”, volume 18, 2021, páginas 3980-4000. Em todo o caso, alguns autores também identificaram áreas em que o eIDAS estava particularmente bem preparado em termos de segurança para os objectivos a que se propunha, como em termos de transacções bancárias. Veja-se a investigação de NICOLAS BUCHMANN, CHRISTIAN RATHGEB, HARALD BAIER e CHRISTOPH BUSCH, *Towards electronic identification and trusted services for biometric authenticated transactions in the single euro payments area*, in *Annual Privacy Forum*, Bart Preneel e Demosthenes Ikononou (eds.), Berlim, 2014, páginas 172-190.

<sup>39</sup> Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE (Regulamento Geral sobre a Protecção de Dados) (JO L 119/1, 4.5.2016).

feito através de canais móveis, e o sistema tem pouca maleabilidade para suprir as necessidades dos diferentes sectores. Apesar de a parte relativa aos serviços de confiança estar consideravelmente melhor em relação à da Directiva, as diferenças que podem ocorrer na aplicação das normas entre EM pela falta de uniformização de critérios, algumas falhas de segurança e a falta de adaptabilidade a desenvolvimentos tecnológicos urge um melhoramento integrado e holístico do eIDAS. A recomendação do estudo entregue à Comissão foi a de se proceder à revisão do quadro regulamentar e à implementação de mudanças fundamentais<sup>40</sup>.

A Comissão anunciou a sua revisão a 19 de Fevereiro de 2020, como uma das principais acções no âmbito da construção do futuro digital da Europa. A sua intenção era “melhorar a sua eficácia, alargar as suas vantagens ao setor privado e promover a utilização de identidades digitais fiáveis por todos os europeus”<sup>41</sup>. O Conselho iria pressionar, em Outubro, para que o novo quadro regulatório de identificação electrónica segura fosse aplicável a toda a UE, incluísse assinaturas digitais e permitisse acesso a serviços públicos e privados transfronteiriços<sup>42</sup>.

Nesse sentido, foi avançada pela Comissão, em Junho de 2021<sup>43</sup>, uma proposta de Regulamento que modifica o quadro da IDE<sup>44</sup>. As alterações tencionam repensar a identificação individual, sobretudo no sentido de se implementar uma funcionalidade inteiramente nova. Pretende-se que cada cidadão, residente no território de um EM ou empresa com um critério de conexão ao espaço europeu tenha agregados numa base de dados única – uma carteira digital (*e-wallet* ou *mobile wallet*) – todos os seus elementos pessoais necessários para poder ser identificado ou autenticado<sup>45</sup> junto de serviços públicos e entidades privadas. Aliás, enquanto que o instrumento

---

<sup>40</sup> COMISSÃO EUROPEIA, *Evaluation study of the Regulation no. 910/2014 (eIDAS Regulation) SMART 2019/0046 Final Report*, Bruxelas, 2019, Executive summary.

<sup>41</sup> Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões ‘Construir o futuro digital da Europa’ (COM/2020/67 final, 19.2.2020), página 13.

<sup>42</sup> Conclusões da reunião extraordinária do Conselho Europeu (1 e 2 de Outubro de 2020) (EUCO 13/20 CO EUR 10 CONCL 6, 2.10.2020), página 6.

<sup>43</sup> *Comissão propõe uma identidade digital segura e de confiança para todos os europeus*, 3 de Junho de 2021 (consultado a 30 de Dezembro de 2022).

<sup>44</sup> Proposta de Regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (UE) n.º 910/2014 no respeitante à criação de um quadro europeu para a identidade digital (COM(2021) 281 final, 3.6.2021).

<sup>45</sup> Para uma análise de modelos de autorização e autenticação no eIDAS, veja-se DIANA BERBECARU, ANTONIO LIOY e CESARE CAMERONI, *Authorize-then-authenticate: Supporting authorization decisions prior to authentication in an electronic identity infrastructure*, in *Intelligent distributed computing XIII*, Igor Kotenko, Costin Badica, Vasily Desnitsky, Didier El Baz e Mirjana Ivanovic (eds.), volume 868, Cham, 2020, páginas 313-322.

de 2014 só permite conectar serviços públicos, uma das principais mudanças desta proposta é, precisamente, alargar a interoperabilidade para incluir fornecedores privados. A nova IDE permitirá o reconhecimento transversal em todo o território da UE da identidade daqueles que possam ser titulares de cartões nacionais de identificação civil ou documentos similares, sendo uma forma intuitiva e mais segura de controlar a informação partilhada, *online e offline*.

Como será desenvolvido em seguida, a proposta de revisão do Regulamento eIDAS é bastante ambiciosa no plano técnico. Está em causa nada menos do que a criação de uma solução tecnológica de identificação altamente segura e confiável que permita aos utilizadores partilhar um mínimo de dados possível para que lhes sejam prestados serviços públicos e privados através da sua identificação e autenticação, em todo o espaço europeu. Uma solução que passará por carteiras digitais que conterão os seus atributos pessoais e certificados, bem como pela redução da necessidade de emissão de credenciais para aumentar a privacidade individual e diminuir a exposição aos fornecedores dos serviços<sup>46</sup>. É, portanto, possível que decorram significativos atrasos na entrada em vigor da proposta, mormente se o legislador quiser aguardar por uma maior maturidade na definição de parâmetros e na testagem da tecnologia necessária ao funcionamento das carteiras.

### 3.3. Objectivos e harmonização

Esta revisão é um passo substancial num momento em que apenas 14% dos prestadores de serviços públicos básicos nos EM admitem a autenticação transfronteiriça com algum tipo de sistema de identificação digital<sup>47</sup> e somente 59% dos residentes podem aceder a estruturas de acesso confiáveis e seguras. Com a nova IDE, o acesso a serviços digitais será mais controlado e rastreável: por um lado, as entidades conseguirão mais rápida e facilmente confirmar a identidade individual, bem como a titularidade de atributos e o preenchimento de condições para obtenção de bens e serviços; por outro, os utilizadores poderão melhor compreender que elementos pessoais partilham, embora tal não signifique que terão de divulgar menos informação do que aquela que é divulgada actualmente.

De acordo com a exposição de motivos da proposta, há uma crescente procura de “soluções de identidade eletrónica (...) que ofereçam, ao setor público e privado,

---

<sup>46</sup> AMIR SHARIF, MATTEO RANZI, ROBERTO CARBONE, GIADA SCIARRETTA, FRANCESCO ANTONIO MARINO e SILVIO RANISE, *The eIDAS Regulation: A survey of technological trends for European electronic identity schemes*, “Applied Sciences”, volume 12, número 24, 2022, página 23.

<sup>47</sup> *Identidade Digital Europeia* (consultado a 16 de Dezembro de 2022).

ganhos de eficiência e um elevado nível de confiança em toda [a] UE. Esta procura surge da necessidade de identificar e autenticar utilizadores com um elevado nível de garantia<sup>48</sup>, sobretudo para agilizar o exercício das liberdades fundamentais de circulação e dos direitos relacionados com a iniciativa económica. Alguns exemplos dados pela Comissão em que a IDE poderá ser utilizada são a obtenção de certificados e comprovativos; a abertura de contas à ordem junto de entidades bancárias; a candidatura a instituições de ensino superior; a prescrição de medicamentos; o aluguer de viaturas automóveis e a sua condução; e, até mesmo, o *check-in* em instalações hoteleiras. Tendo os documentos digitalizados numa única carteira, os cidadãos poderão realizar diversas operações que requeiram alguma forma de identificação ou certificação precisando apenas de enviar ou revelar electronicamente esses documentos à entidade que os peça.

Alguns serviços já em funcionamento deverão ser integrados no sistema IDE, desde que o *software* consiga garantir a sua fiabilidade jurídica, certeza probatória e a segurança dos dados pessoais incluídos. Entre eles, contam-se a assinatura digital (*eSignature*), o carimbo horário (*eTimestamp*), o próprio cartão nacional de identificação (*eID*)<sup>49</sup>, o selo de garantia de autenticidade documental (*eSeal*) ou o serviço de entrega registada electrónica, também conhecido como recibo de recepção (de *e-mails* ou documentos).

A proposta (re)cria uma verdadeira identidade electrónica (um gémeo digital), cuja partilha dos dados pessoais é selectiva e deverá estar limitada às “necessidades do serviço específico solicitado”<sup>50</sup>. O utilizador estará mais atento ao que divulga e a quem o divulga. Ademais, criando-se uma arquitectura europeia única em que a difusão de informações é limitada e que substitui mecanismos locais, diminuem-se os riscos para a privacidade e protecção de dados inerentes à fragmentação. E qualquer optimização que se faça do sistema estará a contribuir todos os intervenientes, numa

---

<sup>48</sup> Secção 1 da exposição de motivos da Proposta.

<sup>49</sup> O primeiro esquema de identificação digital nacional a ser acessível aos demais EM foi o alemão, em utilização desde 29 de Setembro de 2018. Veja-se, a este propósito, NIKO TSAKALAKIS, SOPHIE STALLA-BOURDILLON e KIERON O’HARA, Data protection by design for cross-border electronic identification: Does the eIDAS interoperability framework need to be modernised?, in *Privacy and identity management. Fairness, accountability, and transparency in the age of big data*, Eleni Kosta, Jo Pierson, Daniel Slamanig, Simone Fischer-Hübner e Stephan Krenn (eds.), volume 547, Cham, 2019, página 256. Um modelo comparativo de diferentes arquitecturas de identificação virtual antecessoras dos sistemas actuais pode ser encontrado em ARMEN KHATCHATOUROV, MARYLINE LAURENT e CLAIRE LEVALLOIS-BARTH, Privacy in digital identity systems: Models, assessment, and user adoption, in *Electronic government*, Efthimios Tambouris, Marijn Janssen, Hans Jochen Scholl, Maria Wimmer, Konstantinos Tarabanis, Mila Gascó, Bram Klievink, Ida Lindgren e Peter Parycek (eds.), volume 13391, Cham, 2015, páginas 273-290.

<sup>50</sup> Secção 1 da exposição de motivos da Proposta.

abordagem transfronteiriça, ampla e multi-sectorial. Este tem sido, em bom rigor, um argumento recorrente aquando da apresentação de legislação europeia no âmbito do tratamento de dados. Tanto a Comissão como o PE têm, ao longo dos anos, apelado sistematicamente às vantagens que podem advir da uniformização pelo Direito da UE neste campo para justificar a substituição da malha de normas de origem nacional, ou, pelo menos, a sobreposição dessa malha por uma linguagem, axiologia e técnica harmonizadas a nível supra-nacional. Porém, em boa verdade, é um argumento que, apesar da solidez das vantagens para o mercado interno, não tem conseguido mascarar alguns inconvenientes e desconforto advindos da necessária *competence creep*.

O tratamento dos dados pessoais em todas as operações realizadas no âmbito da IDE deverá estar abrangido pelo RGPD – tal como o Regulamento eIDAS em vigor se refere<sup>51</sup> à Directiva 95/46/CE<sup>52</sup>. Não obstante, a proposta comporta um conjunto de garantias e pormenores específicos em matéria de protecção dos dados que serão assinalados nas secções seguintes<sup>53</sup>. Importa, nesse sentido, começar pelo cerne da proposta de Regulamento: a carteira digital.

### 3.4. Carteiras, atributos e certificados

O primeiro pagamento móvel por tecnologia *contactless* teve lugar em 1997, quando a Coca-Cola<sup>®</sup> instalou máquinas de venda automática em Helsínquia que aceitavam pagamentos por mensagem de texto<sup>54</sup>. Esta génese é bastante diferente do conceito actual de carteiras digitais, mas a evolução para sistemas de transacções electrónicas como os utilizados hoje em dia demorou menos de uma década. Em 2011, a Google<sup>®</sup> tornou-se a primeira grande empresa a oferecer um serviço de carteira digital. As *e-wallets* têm evoluído sobretudo por iniciativa do sector privado, que as utiliza para digitalizar e mobilizar recursos, bens, cartões ou bilhetes e facilitar a experiência dos clientes. As carteiras de IDE terão um funcionamento semelhante, servindo para compilar os atributos dos indivíduos e guardar os documentos necessários à sua identificação e autenticação.

---

<sup>51</sup> Número 1 do artigo 5.º do Regulamento (UE) n.º 910/2014.

<sup>52</sup> Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281/31, 23.11.1995).

<sup>53</sup> Atenção, porém, que este texto ainda não está na fase final de redacção, pelo que contém alguns erros, lapsos e incongruências que impedem a compreensão integral tanto da intenção do legislador como dos mecanismos normativos de utilização e protecção dos dados pessoais.

<sup>54</sup> *The History of E-Wallet* (consultado a 29 de Dezembro de 2022).

### 3.4.1. Conceito

O artigo 1.º da proposta introduz as carteiras digitais no objecto do Regulamento eIDAS, que também definirá os requisitos para a sua emissão pelos EM. A carteira digital é, simultaneamente, um produto e um serviço que “permitem ao utilizador armazenar dados de identidade, credenciais e atributos (...), com vista a fornecê-los a partes utilizadoras mediante pedido e a utilizá-los para autenticação, em linha e fora de linha”<sup>55</sup>. Servirá também para a criação de assinaturas e selos electrónicos, como partes integrantes da representação digital de cada indivíduo. De facto, os dados pessoais e os certificados podem ser combinados e utilizados de forma integrada nas carteiras para que os utilizadores acessem a bens e serviços com relativa conveniência, facilidade e segurança.

### 3.4.2. Atributos

Os atributos são “uma particularidade, característica ou qualidade de uma pessoa singular ou coletiva ou de uma entidade”<sup>56</sup>. Um novo Anexo VI permitirá compreender melhor este conceito, visto que enumera alguns<sup>57</sup> dos atributos que poderão constar das carteiras e ser verificados pelos prestadores (qualificados) de certificados electrónicos, a pedido dos utilizadores, através do contraste com fontes autênticas do sector público<sup>58</sup>. Eles são o endereço, idade, sexo, estado civil, composição do agregado familiar, nacionalidade, habilitações literárias e qualificações profissionais, bem como os respectivos títulos e licenças, autorizações específicas

---

<sup>55</sup> Parágrafo 42 do artigo 3.º da Proposta. Veja-se igualmente a alínea d) do artigo 1.º e o número 1 do artigo 2.º da Proposta.

<sup>56</sup> Parágrafo 43 do artigo 3.º da Proposta.

<sup>57</sup> O título do Anexo é ambíguo já que se refere a uma “lista mínima de atributos”.

<sup>58</sup> O número 1 do artigo 45.º-D da Proposta determina que os EM deverão garantir a adopção de medidas que permitam que os prestadores qualificados possam verificar a autenticidade dos atributos contidos no Anexo VI, por meios electrónicos, a pedido dos utilizadores, através da comparação dos certificados com fontes autênticas. O número 2 adita ainda que a Comissão deverá estabelecer “técnicas mínimas, as normas e os procedimentos no que respeita ao catálogo de atributos, aos sistemas de certificação de atributos e aos procedimentos de verificação referentes aos certificados electrónicos qualificados de atributos mediante um ato de execução relativo à implementação das carteiras”, no prazo de 6 meses após a entrada em vigor do Regulamento eIDAS. Relativamente à numeração do articulado, é de sublinhar que, na versão final para publicação, não haverá artigos alfanuméricos, como este artigo 45.º-D. Em todo o caso, este estudo está limitado ao texto actual da proposta – que existe em contraste com o Regulamento em vigor – e não pode antecipar a numeração final e exclusivamente numérica que será aprovada.

e dados financeiros e empresariais. Por outras palavras, atributos são as informações pessoais que poderão ser exibidas pelos seus titulares, sejam indivíduos ou representantes de pessoas colectivas, através das carteiras digitais, sempre que for requerida a sua identificação ou autenticação electrónicas.

A certeza do seu conteúdo pode ser confirmada com as tais fontes autênticas. Uma fonte é um “repositório ou sistema, sob a responsabilidade de um organismo do setor público ou de uma entidade privada, que contém os atributos relativos a uma pessoa singular ou colectiva e é considerado a fonte principal dessa informação ou reconhecido como autêntico pela legislação nacional”<sup>59</sup>. São fontes os arquivos onde se poderá obter a confirmação mais segura e o maior grau de certeza jurídica do teor (actualizado) dos atributos de cada pessoa singular ou colectiva. Pense-se, no caso nacional, por exemplo, nas bases de dados do Instituto dos Registos e Notariado, I.P.

Os mencionados prestadores de certificados que podem verificar a qualidade dos atributos – e seria importante que todas as entidades que emitem e tratam certificados (como diplomas, certidões ou licenças) possam ser consideradas como fornecedoras de certificados de atributos – terão de garantir a interoperabilidade dos certificados com as carteiras<sup>60</sup>, apesar de estarem limitados em certas acções em favor da confidencialidade e segurança dos dados aí contidos, tal como sucede para os próprios emissores das carteiras. Não podem combinar informações providas de outros serviços que prestem e devem prestá-los através de uma entidade jurídica autónoma. Para além disso, os dados pessoais devem ser “logicamente mantidos separados de outros dados detidos”<sup>61</sup>.

Uma das alterações que se repete na proposta tem que ver com a qualificação dos serviços e prestadores, e bem assim com os requisitos necessários a esse procedimento. Não será objecto especial de análise nesta recensão pelo (ainda) pouco relevo que tem, sobretudo visto que o novo Regulamento e os actos de execução da Comissão não estão em vigor<sup>62</sup>. Em todo o caso, importa perceber o que significa, visto que funciona como garante de maior certeza jurídica. No caso da certificação de atributos, esta pode ter lugar com base num documento (certificado) electrónico

---

<sup>59</sup> Parágrafo 46 do artigo 3.º da Proposta.

<sup>60</sup> Artigo 45.º-E da Proposta.

<sup>61</sup> Número 2 do artigo 45.º-F da Proposta. Veja-se, igualmente, os demais números.

<sup>62</sup> Espera-se que a qualificação dos serviços possa, pelo menos parcialmente, colmatar algumas fragilidades do Regulamento (UE) n.º 910/2014, nomeadamente no tratamento de dados sensíveis. Veja-se, a esse propósito, as sugestões de sobreposição do eIDAS com o projecto STORK 2.0 em ANTONIOS STASIS, LOUKIA DEMIRI e ELENI CHANIOTAKI, *eIDAS-electronic identification for cross border ehealth*, “International Journal of Reliable and Quality E-Healthcare”, volume 7, número 2, 2018, páginas 51-67.

ou num documento qualificado<sup>63</sup>. A diferença, que será semelhante nos casos dos serviços de confiança prestados no seio da IDE e que escusa a sua repetição, baseia-se nos certificados qualificados serem emitidos por um prestador qualificado e, no caso concreto, conterem os dados exigidos pelo Anexo V da proposta, a saber: i) a indicação de emissão como certificado electrónico qualificado de atributos; ii) os detalhes do prestador qualificado emissor, como o nome (para pessoas singulares) ou a designação e número de registo (pessoas colectivas); iii) a identificação do titular dos atributos; iv) os atributos a certificar; v) a validade do documento; vi) um código de identificação único e a indicação do sistema de certificação; vii) uma assinatura ou selo electrónicos; viii) o local onde pode ser consultado o certificado que valida esta assinatura ou selo; e ix) a informação de contacto dos serviços que podem atestar da validade do certificado qualificado.

O legislador europeu acrescentou ainda uma secção 9 ao capítulo III da proposta, relativo aos serviços de confiança (que veremos adiante), dedicada aos certificados de atributos. No essencial, cumpre dizer que se estabelece que estes certificados deverão ter todos os efeitos legais e ser admissíveis como meio probatório em juízo em pé de igualdade com documentos em suporte de papel, não podendo estas qualidades ser afastadas em razão do formato. Nesse sentido, também se prevê que os certificados sejam reconhecidos em todos os EM<sup>64</sup>. Porém, e salvo se os EM ou as Administrações Públicas o autorizarem, a apresentação de certificados de atributos não bastará quando o acesso a serviços electrónicos prestados por entidades públicas exigir aos utilizadores que se identifiquem e se autenticuem<sup>65</sup>.

### 3.4.3. Sistema

A secção I do capítulo II da proposta será agora dedicada às carteiras digitais, sendo inseridos quatro novos artigos e suprimido o actual artigo 6.º, sobre reconhecimento mútuo. É de notar que os EM deverão começar a emitir as carteiras até 12 meses depois da entrada em vigor do Regulamento, o que exigirá algum esforço técnico e financeiro, especialmente para garantir uma usabilidade sem erros e a exclusividade do controlo sobre os dados pelos utilizadores. É provável que o

---

<sup>63</sup> Parágrafos 44 e 45 do artigo 3.º da Proposta.

<sup>64</sup> Artigo 45.º-A da Proposta. Atenção que a proposta não modifica o artigo 46.º, sobre os efeitos legais dos documentos electrónicos. Nesse aspecto, mantém-se válida a opinião de que a proposta, tal como o Regulamento ainda em vigor, não vem tratar das noções de documento ou escrito, mantendo-as na esfera de cada Direito nacional, como entendem FRANCISCO ANDRADE e MARINA SILVA, *O documento electrónico: Suporte e formato*, “Revista da Ordem dos Advogados”, volume 3/4, 2021, páginas 604 e 609.

<sup>65</sup> Artigo 45.º-B da Proposta.

sucesso da implementação venha a depender de um acompanhamento sério da Comissão a vários níveis, como tecnológico, material, financeiro e de *know-how*<sup>66</sup>. Dependendo das rondas negociais e da preparação técnica dos países, também não será de estranhar que venha a ser necessária uma margem temporal e de discricionariedade de acção maior, sob pena de poderem ocorrer situações de incumprimento na execução inicial do Regulamento. Apesar das vantagens do sistema, não será aconselhável, porém, a aplicação de sanções se este incumprimento não se revelar excessivamente prolongado ou notoriamente negligente.

Dispõe a proposta de Regulamento que as carteiras servirão para:

“Pedir e obter de forma segura, armazenar, seleccionar, combinar e partilhar, de um modo que seja transparente e rastreável pelo utilizador, os dados legais de identificação pessoal e o certificado eletrónico de atributos necessários para se autenticar em linha e fora de linha, a fim de utilizar serviços públicos e privados em linha [e] [a]ssinar através de assinaturas eletrónicas qualificadas”<sup>67</sup>.

As carteiras providenciarão uma ferramenta de identificação, apresentação e diálogo – uma “interface comum”<sup>68</sup> – que ligará os utilizadores finais aos demais intervenientes,

---

<sup>66</sup> Em todo o caso, é de apontar que, quando avançou com a proposta de Regulamento eIDAS, a 3 de Junho de 2021, a Comissão também convidou os EM a trabalharem no sentido de se desenvolver uma caixa de ferramentas que incluísse uma arquitectura técnica e um quadro de referência, um conjunto de normas e especificações técnicas comuns e um conjunto de directrizes e boas práticas. Os resultados desta consulta servirão de base para a implementação do Regulamento, sendo o processo de desenvolvimento da caixa independente do processo legislativo. Até à escrita deste texto, um grupo de peritos já havia elaborado um esboço, com uma descrição sumária e resultados preliminares, do conceito e funcionamento das carteiras, os seus objectivos, o papel dos actores no sistema e os requisitos funcionais e não funcionais. A mais recente versão deste esboço data de Janeiro de 2023, denominando-se *The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework. The European Digital Identity Wallet Architecture and Reference Framework* (versão 1.0.0). Embora não seja obrigatório e seja um modelo em construção bastante abstracto que não permite ainda compreender como serão satisfeitos todos os requisitos técnicos, o esboço será a base para os actos de execução e actos delegados que decorrerão no seguimento da entrada em vigor das alterações ao Regulamento. Simultaneamente, a Comissão tem vindo a apoiar projectos-piloto em larga escala com tranches de co-financiamento até 50 milhões de euros para acelerar o desenvolvimento daqueles casos em que a utilização das carteiras digitais será prioritária, como no caso de pagamentos, atribuição de qualificações profissionais e certificados académicos, prestação de serviços de saúde ou atribuição de licenças e cartas de condução. Espera-se que estes projectos comecem a ser implementados ainda na primeira metade de 2023. Veja-se o *European Digital Identity Wallets: Commission publishes first technical Toolbox towards prototypes*, 10 de Fevereiro de 2023 (consultado a 21 de Abril de 2023).

<sup>67</sup> Número 3 do artigo 6.º-A da Proposta.

<sup>68</sup> Alínea a) do número 4 do artigo 6.º-A da Proposta.

como os fornecedores de serviços de confiança, emissores das carteiras e autoridades nacionais. A base é, de facto, a confiança<sup>69</sup>, sobretudo para que as Administrações Públicas não coloquem entraves à apresentação dos documentos electrónicos contidos nas carteiras porque podem confiar na sua origem e autenticidade, bem como na veracidade do seu conteúdo. As carteiras deverão servir para que os cidadãos da UE se possam identificar, fazer negócios, aceder a diversos serviços e interagir de forma tecnologicamente suave em todos os territórios dos EM, especificamente permitindo que os prestadores de serviços emitam certificados adicionáveis às carteiras, os utilizadores se identifiquem e vejam autenticados os seus dados e certificados de atributos e que a esses mesmos utilizadores sejam confirmadas as credenciais e atributos para acesso a bens e serviços, mesmo em modo *offline*. Estas credenciais são comprovativos “das capacidades, da experiência e do direito ou permissão de uma pessoa”<sup>70</sup>.

A autenticação sem acesso à internet poderá ser relevante em alguns sectores, como aqueles em que os serviços possam ser prestados presencialmente e cuja autenticação seja facilitada com códigos QR ou meios semelhantes, como na saúde<sup>71</sup>. Daí a importância de se garantir um nível elevado de segurança, desde logo no acesso a elementos críticos das carteiras. Para esses propósitos, as carteiras deverão ser aceites em todos os EM como meio de identificação, sempre que estes exijam uma “identificação eletrónica baseada num meio de identificação eletrónica e numa autenticação para aceder a um serviço em linha prestado por um organismo público”<sup>72</sup>. A intenção do legislador não podia ser mais clara: as carteiras digitais deverão ser aceites em qualquer situação que requeira a identificação virtual dos cidadãos. Mas isto aplicar-se-á também perante fornecedores de serviços privados, independentemente até de recorrerem a plataformas cujo acesso dependa de uma autenticação forte dos utilizadores (*i.e.*, baseada em múltiplos factores).

As carteiras digitais poderão ser requeridas em vários cenários, incluindo “nos domínios dos transportes, da energia, do[s] serviços bancários e financeiros, da segurança social, da saúde, da água potável, dos serviços postais, das infraestruturas digitais, da educação ou das telecomunicações”<sup>73</sup>. Desde que sejam emitidas de acordo com os requisitos de segurança do artigo 6.º-A, as carteiras serão métodos de

---

<sup>69</sup> O principal objectivo do Regulamento – que se mantém inequivocamente na proposta – é mesmo criar confiança no ambiente virtual, conforme afirmam JOZEF ANDRAŠKO e MATÚŠ MESARCIK, *Those who shall be identified: The data protection aspects of the legal framework for electronic identification in the European Union*, “TalTech Journal of European Studies”, volume 11, número 2, 2021, página 6.

<sup>70</sup> Parágrafo 52 do artigo 3.º da Proposta.

<sup>71</sup> Considerando 9 da Proposta.

<sup>72</sup> Número 1 do artigo 12.º-B da Proposta.

<sup>73</sup> Número 2 do artigo 12.º-B da Proposta. Veja-se, igualmente, o considerando 28.

identificação tão válidos como quaisquer outros já operáveis. Aliás, é inegável o propósito da Comissão não apenas de que se recorra a este novo instrumento em larga escala como o de o tornar no método subsidiário e preferencial de identificação no mercado interno, superando a fragmentação e os riscos que surgem de se ter diversos sistemas concorrentes em simultâneo. Não obstante, as carteiras irão conviver com muitos outros métodos de identificação durante algum tempo. Será interessante notar como é que os EM e os operadores irão lidar com o facto de terem de gerir sistemas concorrentes à medida que as carteiras europeias penetrarem no mercado interno, sendo que a Comissão não deve descurar os desafios de interoperabilidade que se colocarem nesta fase transitória<sup>74</sup>.

As carteiras assistirão igualmente no caso de ser requerida a autenticação perante plataformas virtuais de muito grande dimensão, fazendo-se aqui a ponte com o RSD<sup>75</sup>. Nestes casos, é de apontar que as plataformas deverão ser obrigadas a aceitar as carteiras caso os utilizadores o peçam mas os utilizadores não devem ser forçados a identificarem-se mediante as carteiras para usufruírem de serviços privados<sup>76</sup>. Este trecho comporta alguma expectativa quanto à reacção das plataformas e se procurarão implementar meios que prevejam a recolha e o arquivamento dos dados disponibilizados nas carteiras, e bem assim se respeitarão o princípio da minimização das informações. Isto porque as carteiras serão mesmo carteiras, ou seja, permitirão identificar o portador mas os dados aí incluídos permanecerão com o seu titular. Aliás, a alínea b) do número 4 do artigo 6.º-A afirma que as carteiras devem “[g]arantir que os prestadores de serviços de confiança de certificados qualificados de atributos não possam receber quaisquer informações sobre a utilização desses atributos”. O número 7 reforça a ideia, dizendo que o “utilizador tem pleno controlo sobre a carteira”, o que se concretiza de diferentes maneiras. Em primeiro lugar, o “emissor da carteira (...) não recolhe informações sobre a utilização (...) que não sejam necessárias para a prestação dos serviços”. Também não lhe é permitido combinar “os dados de identificação pessoal e quaisquer outros dados pessoais (...), salvo pedido expresso do utilizador”. E, para além

---

<sup>74</sup> Uma ideia apresentada por AMIR SHARIF et al., *The eIDAS Regulation*, página 24, seria a criação de um portão de identificação (*gateway*) entre a carteira europeia, os meios de identificação dos serviços públicos nacionais e os fornecedores de serviços. Os autores alertam, não obstante, para a necessidade de se aplicar o princípio de *privacy by design* para prevenir esse meio facilitador (*broker*) de permitir que se proceda à criação de perfis (*profiling*) dos utilizadores – algo que se poderia atingir com um “*blind broker architecture model*”. Sobre esse princípio aplicado ao actual Regulamento, vide NIKO TSAKALAKIS et al., *Data protection by design*, páginas 259 ss.

<sup>75</sup> Número 3 do artigo 12.º-B da Proposta.

<sup>76</sup> Considerando 28 da Proposta.

disso, os “dados pessoais relacionados com o fornecimento [das] carteiras (...) são conservados fisicamente e são logicamente separados de quaisquer outros dados detidos”, como mencionado anteriormente.

Para efeitos de monitorização deste novo sistema, os prestadores de serviços (partes utilizadoras, na linguagem da proposta) devem pedir para recorrer às carteiras. Para tal, “comunicam a sua intenção ao Estado-Membro onde estão estabelecid[os] para assegurar a conformidade com os requisitos aplicáveis à prestação de serviços”<sup>77</sup>, assim se garantindo uma maior protecção dos utilizadores contra sistemas fraudulentos, algum uso ilícito de dados, especialmente sensíveis, e o cumprimento da legislação europeia e nacional na matéria. Os EM têm a responsabilidade de criar um único instrumento de acesso e autenticação e as partes deverão autenticar-se com os seus dados pessoais para poderem utilizar os serviços de confiança<sup>78</sup>.

#### 3.4.4. Segurança

A questão da segurança está bem premente nos novos artigos 6.º-A a 6.º-C – a aditar, como se disse, à secção I do capítulo II do Regulamento. As carteiras deverão garantir um nível elevado de segurança dos processos de autenticação e dos dados pessoais, independentemente do tipo de armazenamento e tendo em consideração os graus de risco associados<sup>79</sup>, em particular quanto à sua “aplicação aos requisitos de prova e verificação da identidade, assim como à gestão e autenticação de meios de identificação electrónica”<sup>80</sup>. Aquelas deverão, em bom rigor, ser logo emitidas em observância a uma certa *safety by design*, por um sistema de identificação electrónica que observe um tal nível de garantia. Isto é densificado no artigo 8.º, que se mantém inalterado. Em suma, as carteiras terão de apresentar as mais rigorosas “especificações técnicas, normas e procedimentos conexos, nomeadamente controlos técnicos, cuja finalidade é evitar a utilização ou a alteração indevida da identidade”<sup>81</sup>.

---

<sup>77</sup> Número 1 do artigo 6.º-B da Proposta.

<sup>78</sup> Números 2 e 3 do artigo 6.º-B da Proposta.

<sup>79</sup> Considerando 11 da Proposta. Ainda nesse considerando, o legislador dá o exemplo da biometria (leitura de dados biométricos, como as impressões digitais) como um “método de identificação que oferece um elevado nível de confiança, sobretudo quando utilizado em combinação com outros elementos de autenticação”. Porém, continua, como a “biometria representa uma característica única de uma pessoa, o recurso à mesma requer medidas organizacionais e de segurança, proporcionais ao risco que esse tratamento pode implicar para os direitos e liberdades das pessoas singulares e em conformidade com o Regulamento (UE) 2016/679”.

<sup>80</sup> Alínea c) do número 4 do artigo 6.º-A da Proposta.

<sup>81</sup> Alínea c) do número 2 do artigo 8.º do Regulamento (UE) n.º 910/2014.

Sendo os EM responsáveis pela emissão das carteiras e pela criação das ferramentas de autenticação<sup>82</sup>, serão os fornecedores das ferramentas de validação para assegurar que a “autenticidade e validade [das carteiras] podem ser verificadas, (...) permitir às partes utilizadoras verificar se os certificados de atributos são válidos [e] permitir[-lhes] e aos prestadores qualificados de serviços de segurança verificar a autenticidade e validade dos dados de identificação pessoal atribuídos”<sup>83</sup>.

Se as carteiras tiverem sido certificadas – um procedimento voluntário que segue a avaliação de conformidade (obrigatória) e que substitui o processo de avaliação pelos pares, melhorando o potencial de eficiência e certeza do reconhecimento mútuo<sup>84</sup> –, presumir-se-á, segundo o número 1 do artigo 6.º-C, que respeitam todos os requisitos de cibersegurança do artigo 6.º-A. A certificação das operações de tratamento de dados levadas a cabo pelos EM faz-se no âmbito dos artigos 42.º e 43.º do RGPD. Isto é algo que deverá ser concretizado na redacção final, embora seja de apontar positivamente que já se preveja que instrumentos de execução da Comissão contemplarão um roteiro normativo para que os EM certifiquem a conformidade das carteiras com os requisitos de segurança de forma homogénea, garantindo um nível similar de segurança<sup>85</sup>. Isto é particularmente relevante, nomeadamente em prol da confiança entre as partes, desde logo porque a certificação

---

<sup>82</sup> E, claro está, pelos próprios sistemas de identificação electrónica que permitem accionar os protocolos de autenticação. O novo proémio do artigo 7.º, lido conjuntamente com o artigo 9.º, irá obrigar os EM a notificar a Comissão de “pelo menos um sistema de identificação electrónica que inclua, no mínimo, um meio de identificação”, no espaço de 12 meses desde a entrada em vigor das alterações ao Regulamento. Isto representa uma inovação em relação ao actual instrumento e cujo intuito é a disponibilização de mais e mais diversos meios de identificação para recurso dos vários EM. Um meio de identificação é definido, no parágrafo 2 do artigo 3.º, como “uma unidade material e/ou imaterial, incluindo carteiras europeias de identidade digital ou bilhetes de identidade na aceção do Regulamento (UE) 2019/1157, que contenha os dados de identificação pessoal e que seja utilizada para autenticação de um serviço em linha ou fora de linha”. O instrumento referido é o Regulamento (UE) 2019/1157 do Parlamento Europeu e do Conselho, de 20 de Junho de 2019, que visa reforçar a segurança dos bilhetes de identidade dos cidadãos da União e dos títulos de residência emitidos aos cidadãos da União e seus familiares que exercem o direito à livre circulação (JO L 188/67, 12.7.2019).

<sup>83</sup> Número 5 do artigo 6.º-A da Proposta.

<sup>84</sup> Sobre alguns problemas de aplicação do reconhecimento mútuo, veja-se JOZEF ANDRAŠKO, *Mutual recognition of electronic identification means under the eIDAS Regulation and its application issues*, “Ad Alta: Journal of Interdisciplinary Research”, volume 7, número 2, 2017, páginas 9-13.

<sup>85</sup> Números 2 e 4 do artigo 6.º-C da Proposta. Do mesmo modo, é de sublinhar a previsão, no número 4 do artigo 12.º-B, de que a Comissão encorajará e facilitará a “elaboração de códigos de conduta de autorregulação a nível da União (...) a fim de contribuir para a ampla disponibilidade e usabilidade de carteiras”, através de laços de cooperação e incentivos aos interessados. Diz-se ainda que os prestadores de serviços serão estimulados a “concluírem a elaboração dos códigos de conduta no prazo de 12 meses a contar da adoção do presente regulamento e a aplicá-los efetivamente no prazo de 18 meses”.

não é feita a nível centralizado na UE mas sim por “entidades acreditadas públicas ou privadas designadas pelos Estados-Membros”<sup>86</sup> – uma exigência que se foi consolidando a nível da certificação, e também de outros aspectos, no sentido de reforçar o controlo sobre os dados pelos utilizadores<sup>87</sup>, enquanto se assegura um grau de flexibilidade e proximidade. A emissão e certificação das carteiras, bem como o seu cancelamento, deverão ser comunicadas à Comissão, que publicará e manterá actualizada uma lista nesse sentido<sup>88</sup>, de acordo com os princípios da transparência e da publicidade.

Os EM e todas as entidades que causem danos às informações são objectivamente responsabilizáveis, na leitura combinada do número 8 do artigo 6.º-A da proposta com o (inalterado) artigo 11.º. Quanto à emissão e manutenção das carteiras, os EM terão de garantir a implementação de mecanismos contra a falsificação, roubo e extravio, entre outros, previstos em algumas alíneas do novo número 2 do artigo 24.º.

O legislador aditou ainda um artigo específico relativo à violação da segurança das carteiras. No novo artigo 10.º-A – que complementa o artigo 10.º, inalterado, sobre violações de segurança mais amplas – pode ler-se que, caso sejam comprometidas, mesmo que parcialmente, de maneira a que fique em risco a sua fiabilidade ou a de outras carteiras, o EM “emitente suspende, sem demora, a emissão, revoga a validade da carteira (...) e informa os outros Estados-Membros e a Comissão em conformidade”<sup>89</sup>. Esta suspensão só poderá prolongar-se por três meses, ao fim de cujo período a carteira deverá ser cancelada. Este hiato pode ser diminuído dependendo da gravidade da violação, que pode mesmo justificar a sua retirada imediata. Um dever contrário de restabelecimento e informação tem lugar, naturalmente, caso a violação seja corrigida.

### 3.5. Serviços de confiança

A proposta de novo artigo 1.º alarga o objecto do Regulamento para abarcar “o arquivo eletrónico e o certificado eletrónico de atributos, a gestão de dispositivos de criação de assinaturas e de selos eletrónicos à distância, e os livros-razão eletrónicos”,

---

<sup>86</sup> Número 3 do artigo 6.º-C da Proposta. Atenção, porém, que o número 6 desse mesmo preceito adita que a Comissão “fica habilitada a adotar atos delegados (...) no que diz respeito a estabelecer os critérios específicos a cumprir pelas entidades designadas”.

<sup>87</sup> AMIR SHARIF et al., *The eIDAS Regulation*, página 21.

<sup>88</sup> Veja-se o artigo 6.º-D da Proposta.

<sup>89</sup> Número 1 do artigo 10.º-A da Proposta. Veja-se, igualmente, os demais números.

para além das “assinaturas eletrónicas, os selos eletrónicos, os selos temporais eletrónicos, os documentos eletrónicos, os serviços de envio registado eletrónico e os serviços de certificados para autenticação de sítios Web”<sup>90</sup> previstos anteriormente<sup>91</sup>.

Todos estes são denominados por serviços de confiança – serviços virtuais prestados através da IDE, usualmente contra uma prestação pecuniária, e que serão, doravante, facilitados por meio das carteiras digitais, com a entrada em vigor da proposta. Uma alteração relevante é a patente no artigo 14.º, que permitirá à Comissão adoptar decisões de execução que confirmem a paridade dos requisitos aplicados aos prestadores de serviços de países terceiros<sup>92</sup> se apresentarem suficientes “quadros de confiança”<sup>93</sup>, em alternativa e complemento aos acordos de reconhecimento mútuo previstos no artigo 218.º do Tratado sobre o Funcionamento da UE<sup>94</sup>.

Não há muito a discutir ou a aprofundar relativamente às alterações às normas que têm que ver com os serviços de confiança existentes e mesmo quanto aos novos serviços disponibilizados no âmbito da IDE. O seu funcionamento é que trará uma riqueza ôntica que permitirá tecer juízos sobre o seu valor acrescentado, utilidade, eficácia e eficiência. Por ora, portanto, bastam alguns apontamentos breves. Antes disso, convém dizer que as alterações aos artigos 17.º, 18.º, 20.º e 21.º se devem à necessidade de se alinharem com as regras aplicáveis à segurança das redes de informação utilizadas na UE.

---

<sup>90</sup> Alínea c) do artigo 1.º da Proposta. Note-se também que, na versão actual do Regulamento, refere-se apenas “selos temporais” e tal foi alterado para “selos temporais eletrónicos”. Em todo o caso, parece que sempre se pretendeu falar em selos virtuais, pelo que não é uma modificação particularmente relevante. O parágrafo 16 do artigo 3.º da Proposta, relativo às definições, acrescenta estes novos serviços à lista de serviços de confiança abrangidos pelo Regulamento eIDAS. É, assim, modificada a alínea a) para incluir “certificados eletrónicos de atributos” e são aditadas as alíneas d) a f), que tornam em serviços de confiança o “arquivo eletrónico de documentos eletrónicos”, a “gestão de dispositivos de criação de assinaturas e de selos eletrónicos à distância” e o “registo de dados eletrónicos num livro-razão eletrónico”.

<sup>91</sup> Para um estudo interessante sobre a relação entre os selos temporais baseados em tecnologia *blockchain* e a versão actual do Regulamento, veja-se CHRISTOPH SORGE e MAXIMILIAN LEICHT, *Blockchain-based electronic time stamps and the eIDAS regulation: The best of both worlds*, “Scripted”, volume 19, número 1, 2022, páginas 61-87. Como referem os autores, não parece que as alterações da proposta venham modificar de forma substancial o funcionamento técnico ou influenciar as considerações legais que apresentam no estudo, mas será um pormenor a ter em atenção com o decorrer dos acontecimentos.

<sup>92</sup> Número 2 do artigo 14.º da Proposta.

<sup>93</sup> Considerando 20 da Proposta.

<sup>94</sup> Tratado sobre o Funcionamento da União Europeia (JO C 326/47, 26.10.2012).

### 3.5.1. Identificação

Um detalhe relevante na securitização da arquitectura da IDE e no acesso aos serviços é a previsão de que deverá haver uma só identidade por utilizador e uma só identificação pessoal. Isto significa que, por mais que o sistema seja interoperável e conjugue diferentes serviços de confiança com múltiplas funcionalidades – e, bem assim, haja diversos meios de identificação electrónica a actuar em simultâneo –, não deverá ser exigido aos utilizadores que criem várias contas e *personas* para beneficiar desta rede. Os dados pessoais inseridos no sistema deverão ser “combinados ou associados a uma conta existente pertencente à mesma pessoa”<sup>95</sup>.

Nessa senda, o legislador acrescentou um artigo 11.º-A que deixa claro que os EM devem assegurar uma identificação única dos cidadãos. Tal importa sobretudo quando a identificação é obrigatória, como no âmbito da saúde, serviços bancários ou processos judiciais. A cada utilizador será, inclusivamente, alocado “um identificador único e persistente”<sup>96</sup> para o conectar ao seu pedido de autenticação. Este identificador deve conter um conjunto mínimo de dados que permitam a identificação legal da pessoa. Até seis meses depois da entrada em vigor das alterações, os detalhes serão apurados pelos actos de execução que implementarem as carteiras. O desenho deste parâmetro deve ser feito com relativa cautela visto que pode criar riscos de privacidade consideráveis, especialmente se for possível, de algum modo, aos fornecedores de serviços seguir ou rastrear a actividade *online* dos utilizadores. A pseudonimização<sup>97</sup> emparelhada com o modelo de identificador poderá ser uma estratégia avisada a seguir<sup>98</sup>.

Os utilizadores autenticar-se-ão e acederão aos serviços de confiança através de contas de utilizador. É algo comum na gíria tecnológica e será levado a cabo, de preferência, através de uma autenticação forte – a “autenticação baseada na utilização de dois ou mais elementos (...) que são independentes, de tal forma que a violação de um deles não compromete a fiabilidade dos outros, e que foi concebida de modo a proteger a confidencialidade dos dados de autenticação”<sup>99</sup>.

A par desta identificação única, o novo artigo 12.º-C prevê que os EM reconheçam mutuamente os meios de identificação produzidos noutros EM para efeitos de acesso

<sup>95</sup> Parágrafo 55 do artigo 3.º da Proposta.

<sup>96</sup> Número 2 do artigo 11.º-A da Proposta. Veja-se, também, o número 3 e a alínea e) do número 4 do artigo 6.º-A.

<sup>97</sup> Para aprofundamento desta temática, atente-se no estudo de MIROSLAW KUTYŁOWSKI, LUCJAN HANZLIK e KAMIL KLUCZNIAK, Pseudonymous signature on eIDAS token – Implementation based privacy threats, in *Information security and privacy (part II)*, Joseph Liu e Ron Steinfeld (eds.), volume 9723, Cham, 2016, páginas 467-477.

<sup>98</sup> AMIR SHARIF et al., *The eIDAS Regulation*, página 24.

<sup>99</sup> Parágrafos 51 e 52 do artigo 3.º da Proposta.

e autenticação transfronteiriços a serviços prestados por entidades públicas – em concretização do princípio do reconhecimento mútuo no mercado interno e no sentido de se manterem eficazes as regras relativas às liberdades fundamentais. Não obstante, tal dependerá de que: i) esses meios constem da lista actualizada da Comissão de sistemas de identificação electrónica, prevista no artigo 9.º; ii) o nível de garantia a reconhecer seja, pelo menos, substancial<sup>100</sup> e seja igual ou superior ao requerido pelo EM que irá reconhecer; e iii) o acesso ao serviço *online* em questão por parte da entidade administrativa dependa de um nível de garantia substancial ou elevado.

Apesar de a validação dos serviços de confiança ser alargada expressamente apenas aos dados pessoais e aos certificados de atributos<sup>101</sup>, será de esperar que o mesmo acabe por suceder, nem que seja somente na vida prática, às demais funções dos serviços. A par disto, o artigo 12.º-A permitirá que se certifiquem os sistemas de identificação, à semelhança do que sucede com as carteiras digitais. Isto será feito por via de entidades designadas – cuja denominação e contactos devem ser dados a conhecer à Comissão, que os disponibilizará junto dos demais EM<sup>102</sup> – e somente se os sistemas cumprirem com os requisitos de segurança aplicáveis às carteiras no artigo 6.º-A, os níveis de garantia do artigo 8.º e as regras gerais de segurança do artigo 10.º.

### 3.5.2. Assinaturas

O novo parágrafo 14 do artigo 3.º vem modificar ligeiramente<sup>103</sup> a definição de certificado de assinatura, que passa de ser um “atestado eletrónico” para um

---

<sup>100</sup> Apesar de o número 2 do preceito abrir a possibilidade à aceitação pelos organismos públicos de meios de identificação electrónica com um nível de garantia baixo.

<sup>101</sup> Parágrafo 41 do artigo 3.º da Proposta.

<sup>103</sup> Mantém-se, com este tipo de alterações, um referencial que alguma doutrina tem defendido como positivo no Regulamento, que é o de se prever “uma abordagem tecnologicamente neutra da utilização de diferentes métodos de assinatura eletrónica, entendida em sentido lato”, nas palavras de FRANCISCO ANDRADE, *Identificação eletrónica, assinatura e serviço de confiança*, “UNIO – EU Law Journal”, volume 4, número 2, 2018, página 109. Veja-se, igualmente, NIKO TSAKALAKIS et al., *Data protection by design*, página 257. Esse referencial pode ser encontrado, em particular, na alínea a) do número 3 do artigo 12.º do Regulamento (UE) n.º 910/2014, que dispõe que “[o] quadro de interoperabilidade [procura] ser tecnologicamente neutro e não fazer discriminações em relação às soluções técnicas nacionais específicas utilizadas para a identificação eletrónica no Estado-Membro em causa”, e bem assim nos considerando 16 e 27. O primeiro refere que os requisitos técnicos de garantia “de prova da identidade para a emissão de certificados qualificados (...) deverão ser tecnologicamente neutros. Deverá ser possível satisfazer os requisitos de segurança necessários por meio de diferentes tecnologias” e o segundo considerando determina que “[o] presente regulamento deverá ser tecnologicamente neutro. Os efeitos legais que o presente regulamento produz deverão poder ser obtidos por qualquer meio técnico, desde que os requisitos do regulamento sejam cumpridos”.

“certificado eletrónico ou conjunto de certificados que associa os dados de validação da assinatura eletrónica a uma pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo”<sup>104</sup>. Ainda neste artigo, o parágrafo 23-A define o conceito, talvez desnecessariamente, de “[d]ispositivo qualificado de criação de assinaturas eletrónicas à distância [como] um dispositivo (...) em que um prestador qualificado de serviços de confiança cria, gere ou duplica os dados para a criação de uma assinatura eletrónica em nome de um signatário”<sup>105</sup>.

### 3.5.3. Selos

Tal como sucede relativamente às definições sobre as assinaturas, também o legislador vem agora definir os certificados de selos como certificados ou um conjunto de certificados<sup>106</sup> e aditar uma definição dos dispositivos qualificados de criação de selos à distância, que é em tudo igual à relativa às assinaturas, salvo que aqui não se presta o serviço em nome de um signatário mas “em nome do criador do selo”<sup>107</sup>.

### 3.5.4. Arquivos

O arquivo electrónico consistirá num “serviço que assegura a receção, o armazenamento, o apagamento e a transmissão de dados ou documentos eletrónicos para garantir a sua integridade, a exatidão da sua origem e as especificidades jurídicas durante o período de conservação”. Também poderá haver um serviço qualificado de arquivo, cuja definição se resume a ser “um serviço que satisfaça os requisitos estabelecidos no artigo 45.º-G”<sup>108</sup>. Mais valia não haver uma entrada específica para se definir os serviços qualificados de arquivo e esperemos que não seja incluída na versão final do Regulamento. É mais uma das definições vazias e remissivas que povoam o Direito da UE e que tendem a infectar as legislações nacionais sem razão substantiva aparente.

Em todo o caso, segundo esse artigo 45.º-G, tal como sucede quanto às demais normas relativas à qualificação de serviços<sup>109</sup>, um arquivo é qualificado por ser fornecido por “prestadores qualificados de serviços de confiança”. Neste caso,

---

<sup>104</sup> Parágrafo 14 do artigo 3.º da Proposta.

<sup>105</sup> Parágrafo 23-A do artigo 3.º da Proposta.

<sup>106</sup> Parágrafo 29 do artigo 3.º da Proposta.

<sup>107</sup> Parágrafo 23-B do artigo 3.º da Proposta.

<sup>108</sup> Parágrafos 47 e 48 do artigo 3.º da Proposta. Veja-se, igualmente, o considerando 33.

<sup>109</sup> Veja-se os artigos 34.º, relativo aos serviços qualificados de preservação de assinaturas qualificadas, e 40.º, quanto aos selos qualificados.

acrescenta-se ainda que estes prestadores recorrem a “procedimentos e tecnologias capazes de prolongar a fiabilidade dos documentos eletrónicos para além do prazo de validade tecnológica”<sup>110</sup>. Parece ser uma norma que precisará de alguma concretização no futuro.

### 3.5.5. Livros-razão

Esta última categoria de serviços de confiança<sup>111</sup> consiste num “registo eletrónico de dados inviolável, que assegura a autenticidade e integridade dos dados que contém, bem como a exatidão da sua data, hora e ordem cronológica”<sup>112</sup>. É o que permitirá, em boa medida, a rastreabilidade das operações de dados encetadas no sistema de IDE.

Como no caso dos certificados de atributos e, *mutatis mutandis*, no das carteiras, aos livros-razão não deverá ser afastada a sua eficácia jurídica e admissibilidade probatória pelo seu formato electrónico ou por não serem qualificados. Se forem qualificados, porém, beneficiarão “da presunção da singularidade e autenticidade dos dados que cont[êm], da exatidão da respetiva data e hora e da sua ordem cronológica sequencial”<sup>113</sup>.

Os livros-razão servem como comprovativo e “pista de auditoria imutável para a sequenciação de transações e registos de dados, salvaguardando a [sua] integridade”<sup>114</sup>. É uma técnica pertinente para controlar a cadeia de circulação das informações, pois que agrega a validação temporal, a sequenciação e a garantia do originador dos dados, de forma semelhante ao caso das assinaturas. Ademais, permite uma governação menos centralizada e, conseqüentemente, uma maior cooperação dos envolvidos. O caminho percorrido no fluxo interoperável dos dados é assim assimilável e demonstrável com relativa facilidade, não se exigindo provas adicionais para se confirmar que determinadas informações foram produzidas por certas fontes ou divulgadas junto de certas entidades. Assim se facilita o trilho probatório

---

<sup>110</sup> Primeiro parágrafo do artigo 45.º-G da Proposta.

<sup>111</sup> Não há nada de particularmente relevante a mencionar relativamente à autenticação de sítios na internet e à gestão de dispositivos, pelo que não serão exploradas neste texto.

<sup>112</sup> Parágrafo 53 do artigo 3.º da Proposta. Algumas vantagens podem ser encontradas no considerando 34, que menciona que o livro-razão electrónico cria “uma pista de auditoria fiável para a origem de mercadorias no comércio transfronteiriço, apoia a proteção dos direitos de propriedade intelectual, dota os mercados da eletricidade de uma maior flexibilidade, fornece a base para soluções avançadas de identidade autossobereana e apoia serviços públicos mais eficientes e transformadores”.

<sup>113</sup> Artigo 45.º-H da Proposta.

<sup>114</sup> Secção 3 da exposição de motivos da Proposta.

ao utilizador que alegue a violação dos seus direitos à privacidade ou à protecção de dados. Mas também se reduzem os custos das empresas e se agiliza a supervisão e a regulação por parte das autoridades nacionais e europeias.

A chave para o sucesso deste serviço será, uma vez mais, a harmonização europeia que permita o reconhecimento dos livros-razão em todos os EM. Os livros-razão permitirão compreender melhor o respeito por normas de diversos sectores (incluindo a comunicação social, indústria transformadora de recursos naturais, serviços públicos e actuação governamental, seguros e pensões ou transportes) e facilitar negociações complexas, especialmente no âmbito de instrumentos financeiros e bancários. Também poderão ser um activo essencial na verificação do cumprimento das regras do Direito da UE sobre o tratamento de dados pessoais.

### 3.6. (Outras) garantias de segurança

Um apontamento final é devido quanto a dois aspectos complementares de segurança que irão acrescer ao estabelecido na proposta e no RGPD. Logo no artigo 3.º é dito que as carteiras poderão exibir uma marca de confiança, que consistirá numa “indicação de um modo simples, reconhecível e claro de que uma carteira de identidade digital foi emitida em conformidade com o presente regulamento”<sup>115</sup>. Isto parece assemelhar-se aos selos de qualidade e higiene recorrentes durante a pandemia de COVID-19<sup>116</sup>. Poderá representar algum conforto visual mas é sempre questionável a irrepetibilidade destes símbolos e fica por saber se haverá suficiente fiscalização e controlo da sua aposição.

De outro tanto, é de apontar também a alteração ao artigo 18.º, sobre assistência mútua entre as entidades de supervisão dos EM. A proposta de norma está epigrafada como assistência mútua e cooperação, sendo que o seu número 1 dispõe que as entidades supervisoras não apenas “cooperam tendo em vista o intercâmbio de boas práticas [mas também de] informações relativas à prestação de serviços de confiança”. Esta modificação segue na esteira da economia de escala de haver um único sistema europeu de identidade digital e do facto de que, em consequência, todas as melhorias que tiverem lugar beneficiarão todos os interessados. É ainda

---

<sup>115</sup> Parágrafo 49 do artigo 3.º da Proposta.

<sup>116</sup> Como foi o caso do selo *Clean & Safe Portugal*, criado a 24 de Abril de 2020, pelo Turismo de Portugal, I.P., para certificar o cumprimento de requisitos de higiene e limpeza pelas empresas e estabelecimentos a actuar no país para prevenção e controlo dessa e de outras infecções. Veja-se *Clean & Safe Portugal* (consultado a 27 de Dezembro de 2022).

acrescentado um preceito a instruir os supervisores e as autoridades nacionais competentes a trabalharem em conjunto para “assegurar que os prestadores de serviços de confiança cumprem os requisitos estabelecidos no presente regulamento e na Diretiva [SRI 2]”<sup>117</sup>, sendo que as autoridades nacionais devem verificar o cumprimento, exigir o saneamento de irregularidades e obrigar à notificação<sup>118</sup> de todos os incidentes relevantes.

## Conclusões

Esta breve nótula teve como intuito dar a conhecer a estratégia digital da UE e, em especial, a proposta de melhoramento da IDE, um dos objectivos político-legislativos da Comissão que poderá ter um visível impacto na vida e na condução dos negócios dos cidadãos da UE. Para tal, o texto foi dividido em três partes substantivas. A primeira apresentou a estratégia e o propósito valorativo que decorre do diálogo institucional. A segunda secção deu conta de três eixos da estratégia que estão a correr ao mesmo tempo que a IDE e que com ela se interligam. Finalmente, o último trecho explorou a IDE através do prisma das principais propostas de alteração ao Regulamento (UE) n.º 910/2014.

Uma modificação crucial consiste na introdução de carteiras digitais que visarão permitir a representação pessoal dos indivíduos em ambiente virtual para a obtenção de bens e serviços prestados pelas Administrações Públicas nacionais e por entidades privadas. Esta alteração é secundada pelo alargamento do número de serviços de confiança que serão prestados através da IDE. Parece ser uma pequena revolução técnico-legislativa mas o seu potencial para facilitar e tornar mais cómodas as actividades das pessoas e das empresas é considerável, bem como para reforçar a competitividade do tecido empresarial europeu. É um mecanismo potencialmente sem retorno na agilização do mercado interno e na digitalização da vida em sociedade. E é, ao mesmo tempo, um feliz passo de integração europeia e superação da fragmentação inerente às diferenças entre países, culturas e ambientes tecnológicos.

---

<sup>117</sup> Número 4 do artigo 18.º da Proposta. A “Diretiva [SRI 2]” é, hoje, a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333/80, 27.12.2022).

<sup>118</sup> Este tipo de procedimentos de notificação em caso de acesso indevido e eventual comprometimento das informações tende a estar presente nos diversos instrumentos jurídicos da área, como sublinha SAMSON YOSEPH ESAYAS, *The role of anonymisation and pseudonymisation under the EU data privacy rules: Beyond the ‘all or nothing’ approach*, “European Journal of Law and Technology”, volume 6, número 2, 2015, página 12.

Isto deve-se também ao facto de que não é um instrumento tendente à estagnação. Enquanto que, em 2014, se previu uma análise do Regulamento até 1 de Julho de 2020, as exigências de responsabilização (*accountability*) político-legislativa hodiernas já não comportam prazos tão dilatados. Donde, a Comissão deverá escrutinar a execução do novo eIDAS e apresentar, ao PE e ao Conselho, um relatório no espaço de 24 meses após a sua entrada em vigor. Pela novidade da matéria, propõe-se que o relatório contenha:

“[U]ma avaliação da disponibilidade e usabilidade dos meios de identificação, incluindo as carteiras (...) e [afira] se todos os prestadores privados de serviços em linha que dependem de serviços de identificação eletrónica de terceiros para a autenticação de utilizadores devem ser obrigados a aceitar a utilização dos meios de identificação eletrónica notificados e da carteira europeia de identidade digital”<sup>119</sup>.

Não obstante, é natural que surjam hesitações quanto à colocação de tanta informação pessoal em dispositivos que podem ser acedidos tanto em modo *online* como *offline*. Apesar da robustez das legislações europeia e nacionais sobre a protecção de dados, os riscos securitários estão sempre latentes e são sempre significativos, tendo um lado insidioso de serem difíceis de conhecer e compreender na sua total extensão antes de ter lugar uma violação ou comprometimento das informações. Novas tecnologias comportam sempre novos riscos, por mais que consigamos antecipar muitos deles.

Por outro lado, também é questionável se a própria razão de ser das carteiras digitais e desta nova IDE é legítima, válida ou, simplesmente, aceitável. A verdade é que este mecanismo surge pela necessidade crescente de identificação pessoal para aceder à prestação de serviços. E é compreensível que tal cause controvérsia. Tanto mais que pode conjecturar-se se não estará a ser desenhado um novo incitamento à difusão de dados pessoais e à liberalização das razões pelas quais os fornecedores de serviços pedirão acesso aos atributos dos cidadãos. Não é oculta a inclinação das entidades para pedirem autenticações e a partilha de dados perante permissões ou vazios legais, o que tem redundado numa cada vez maior exposição pública dos indivíduos. Está para se ver o grau de transtorno do direito à privacidade que causará esta evolução da IDE<sup>120</sup>, mesmo que os prestadores de serviços não procedam a qualquer recolha das informações; *rectius*, a qualquer recolha suspeita das informações.

---

<sup>119</sup> Número 2 do artigo 49.º da Proposta.

<sup>120</sup> NORA SCHREIER, ROBIN RENWICK e TINA EHRKE-RABEL, *The digital avatar on a blockchain: e-Identity, anonymity and human dignity*, “Austrian Law Journal”, volume 2021, número 2, 2021, página 213.