Proteção de Dados Pessoais nas Comunicações Eletrónicas: O papel da CNPD e da ANACOM

MARGARIDA VIANA GUARDA DE OLIVEIRA

Dissertação de Mestrado em Direito Administrativo
sob orientação da Prof. Doutora Margarida Couto

Outubro de 2015

Lisboa

LISTA DE ACRÓNIMOS

AdC	Autoridade da Concorrência
ANACOM	Autoridade Nacional de Comunicações
Art.	artigo
Cap.	capítulo
CNPD	Comissão Nacional de Proteção de Dados
cf.	Conferir
ENISA	*European Union Agency for Network and Information Security*
ICP	Instituto de Comunicações de Portugal
ICO	*Information Commissioner's Office*
LPDP	Lei da Proteção de Dados Pessoais (Lei n.º 67/98, de 26 de outubro)
LCE	Lei das Comunicações Eletrónicas (Lei n.º 5/2004, de 10 de fevereiro)
RFID	*Radio Frequency Identification*
TEDH	Tribunal Europeu dos Direitos do Homem
TJUE	Tribunal de Justiça da União Europeia
i.e.	isto é
infra	ver abaixo
n.º	número
op. cit.	obra já citada anteriormente do mesmo autor

ÍNDICE

I. INTRODUÇÃO

A presente dissertação tem por objeto um tema de relevância contemporânea, da qual emerge a atual sociedade de informação. Todo o progresso técnico, aliado à desmaterialização do detentor da informação, é simultaneamente "fonte de libertação e de servidão"[1]. Os desafios colocados pelo avanço da tecnologia e a constante vontade de acompanhar os sucessivos progressos informáticos despertaram a importância de proteger cada cidadão dos riscos inerentes a este universo cibernético. Na verdade, e como nunca antes, vigora hoje uma dicotomia repartida entre a necessidade de proteção de valores como a intimidade da vida privada e claro desejo de dispor de uma Administração Pública transparente, na qual possamos confiar.

Por conseguinte, dada a exponencial evolução das tecnologias relacionadas com as comunicações eletrónicas e as crescentes exigências legítimas das autoridades competentes, revela-se indispensável a construção de sistemas de informação capazes de reunir as características fundamentais para garantir a segurança da informação, nas vertentes de confidencialidade, integridade e disponibilidade da informação.

Em razão do seu caráter multidisciplinar, o presente estudo traduz-se num enfoque polivalente repartido essencialmente entre duas matérias: as comunicações eletrónicas e a proteção de dados pessoais.

Uma vez que a captação de comunicação de informação é cada vez mais suportada em meios digitais, pretendem estas linhas, num primeiro plano, analisar o enquadramento histórico do próprio setor das comunicações eletrónicas. De seguida, será apresentado um breve estudo sobre o aparecimento da autoridade responsável pela regulação do setor, ANACOM, até aos dias de hoje. Este capítulo, intitulado por "Comunicações Eletrónicas", terminará com o regime jurídico em vigor, com especial destaque para a Lei das Comunicações Eletrónicas.

Num segundo plano, deslocaremos o debate para o regime da proteção de dados pessoais. Aí analisaremos o conceito de dados pessoais, remetendo posteriormente para o regime subjacente à nossa Lei Fundamental. Tendo o legislador optado por delegar o controlo

[1] JOSÉ GARCIA MARQUES, "Telecomunicações e proteção de dados", *in As Telecomunicações e o Direito na Sociedade da Informação – Actas do Colóquio organizado pelo IJC em 23 e 24 de Abril de 1998,* Coimbra, Instituto Jurídico da Comunicação, 1999.

e a fiscalização do processamento de dados pessoais na CNPD, faremos uma breve apresentação deste organismo, encerrando o capítulo com alguns dos princípios inerentes ao tratamento de dados pessoais.

Por fim, será analisado o regime legal, em matéria de proteção de dados, subjacente às duas entidades, com especial incidência na Lei relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas. Para esta investigação gnosiológica, estudaremos, afinal, o caso dos *data breaches* à luz dos vários diplomas que sobre eles versam.

Esta foi a esquematização que, de entre várias possíveis, considerámos mais adequada ao tratamento global da proteção de dados pessoais no setor das comunicações eletrónicas, sem descurar a análise mais detalhada de algumas questões que julgámos essenciais.

II. COMUNICAÇÕES ELETRÓNICAS

II.1. DA REGULAÇÃO

II.1.1. Evolução do setor das Comunicações Eletrónicas

Em Portugal, até à revisão da conhecida "Lei de Delimitação de Setores", ocorrida em 1997, o acesso à atividade das telecomunicações encontrava-se vedado a empresas de natureza privada.

O início do processo de liberalização do setor das telecomunicações ocorre em 1989 e foi impulsionado pela Lei n.º 88/89, de 11 de setembro. A chamada Lei de Bases do Estabelecimento, Gestão e Exploração das Infraestruturas e Serviços de Telecomunicações determinou que o acesso à atividade das telecomunicações, com exceção dos serviços complementares da rede básica e dos serviços de valor acrescentado, ficaria sujeito ao regime de vedação relativa ou à reserva de controlo. Assim, o acesso por parte da iniciativa privada ficou condicionado à detenção, pelo setor público, da maioria do capital social do operador de telecomunicações.

Nos idos anos 80, a realidade existente no nosso país assemelhava-se à restante presente na generalidade dos Estados-Membros da União Europeia, resultante da simbiose entre a atividade de prestação de serviços de telecomunicações e o desenvolvimento e a exploração das infraestruturas de telecomunicações, estando esta atividade a cargo do setor público, que por sua vez asseguraria a respetiva gestão e exploração[2]. Após sucessivas reorganizações empresariais, a plena liberalização do setor das comunicações eletrónicas só terminou com a Lei n.º 91/97, de 1 de agosto, a qual consagrou, nos artigos 7º e 11º, o princípio da liberalização das telecomunicações de acordo com a legislação aplicável[3].

Cumpre salientar que o processo de liberalização não implicou, necessariamente, a retirada de influência do poder do Estado, uma vez que é possível conciliar o desenvolvimento da atividade pelos operadores do setor com a aplicação de amplas e eficazes

[2] Com exceção do Reino Unido, onde passaram a operar duas empresas em regime de duopólio a partir de 1981. Ver SÉRGIO GONÇALVES DO CABO, *Regulação e concorrência no Setor das Comunicações Eletrónicas*, Almedina 2009, pág. 208.
[3] Por sua vez, a Lei n.º 91/97 revogou a anterior Lei n.º 88/89, de 11 de setembro

atitudes interventivas estatais, através da atribuição de regras para os setores de atividade objeto de regulação, a par da criação de entidades dotadas de independência total, não só perante a Administração, como também face aos próprios regulados capazes de executarem com sucesso as tarefas que lhes são cometidas por lei, como autoridades de visível prestígio e de reconhecimento social.

Contudo, é apenas com o Decreto-Lei n.º 415/98, de 31 de dezembro, que, ao transpor a Diretiva 97/33/CE, do Parlamento Europeu e do Conselho, de 30 de junho, respeitante à interligação no setor das telecomunicações, é finalmente atribuído ao Instituto de Comunicações de Portugal (ICP) a função de "autoridade reguladora nacional" [4].

Entre aqueles e outros diplomas legais, em conjunto com a Lei de Bases de 1997, é edificado o quadro regulamentar do setor das comunicações eletrónicas até ao aparecimento da Lei das Comunicações Eletrónicas.

II.1.2. Regulação setor – a autoridade reguladora

Resultante do impulso da Comissão Europeia e da iniciativa dos Estados-Membros, o movimento de privatização e de liberalização conduziu à transformação do modo de prestação de alguns serviços infraestruturais e exigiu, em simultâneo, alterações profundas no respetivo quadro regulatório.

Atividades como as telecomunicações ou a distribuição de energia tornaram-se áreas de atuação para todos os agentes económicos com envergadura para o respetivo empreendimento. É no quadro da abertura quase total à concorrência que surgiu de modo visível e com crescente peso no ordenamento jurídico-económico, o conceito de regulação, como uma nova forma relacional entre o Estado, munido do seu poder de autoridade, e a economia.

O processo deu origem à densificação, em alguns casos, da regulação setorial tendo sido concebidas novas entidades de natureza setorial com funções especializadas, sob a forma de autoridades reguladoras. Estas entidades passaram a supervisionar cada setor, salvaguardando a interconexão entre todos os seus elementos. A regulação setorial assume

[4] O Decreto-Lei também prevê o regime de interligação entre redes públicas de telecomunicações num ambiente de mercados abertos e concorrenciais, com vista a permitira interoperabilidade de serviços de telecomunicações de uso público, e determina os princípios gerais aplicáveis à numeração.

como papel principal a substituição da concorrência e defende que a sua intervenção é indispensável para atingir resultados aceitáveis.

A figura das autoridades reguladoras independentes[5] é apresentada na Europa Continental no contexto mais amplo das autoridades administrativas independentes[6]: correspondem a autoridades administrativas independentes com funções de regulação económica ou financeira e partilham características essenciais, tais como a natureza administrativa, a independência orgânica e funcional, a neutralidade política da gestão e a imparcialidade, ou seja, estão dotadas de um poder-dever para valorar e ponderar os diferentes interesses em jogo, não privilegiando ou discriminando qualquer deles.

As autoridades reguladoras independentes estão inseridas naquilo que a maioria da doutrina designa por "administração independente"[7], uma vez que estão somente limitadas pela lei e sujeitas apenas a controlo judicial. O sistema jurídico português determina, contudo, que nem todas as autoridades administrativas providas de funções de regulação partilham de características como a independência orgânica e funcional, assumindo, por isso, a natureza de institutos públicos na vertente tradicional.

A crescente atribuição de competências das autoridades com incidência não só setorial como também transversal salientou a necessidade de implementar um modelo de articulação que permitisse o aproveitamento do desempenho de cada uma delas, de modo prevenir e resolver eventuais conflitos de competência e complementar as suas atribuições[8].

II.1.2.1 Quadro Institucional - ANACOM

Ao contrário do que seria de prever, a liberalização do setor das telecomunicações deu origem à sua maior regulação. A especificidade técnica do setor das comunicações, aliada às suas constantes inovações, impõem diariamente a existência de um amplo espaço para a

[5] Comummente designadas pela doutrina por agências reguladoras, de inspiração anglo-saxónica, ou "autoridades administrativas independentes", de inspiração francesa. Quanto ao aqui utilizado, ver FERNANDA MAÇÃS e VITAL MOREIRA, *Autoridades Reguladoras Independentes - Estudo e Projeto de Lei-Quadro*, Coimbra, Coimbra Editora, 2003.

[6] Sobre a evolução da regulação desde a sua origem veja-se CARDOSO, José Lucas, *Autoridades Administrativas Independentes e Constituição*, Coimbra, Coimbra Editora, outubro de 2002,
Pág. 42.

[7] CARLOS SANTOS, EDUARDA GONÇALVES e LEITÃO MARQUES defendem, contudo, a integração das autoridades reguladoras independentes na Administração indireta, in, *Direito da Economia*, Lisboa, AAFDL, 2001, pág. 145.

[8] A título de exemplo ver o Acordo de Cooperação entre a ANACOM, cuja atividade incide sobre a regulação setorial, e a AdC, que versa sobre a regulação transversal, de 26 de setembro de 2003.

intervenção ordenadora da autoridade de regulação e, consequentemente, a necessidade de garantir um regime que a habilite de instrumentos que lhe confiram flexibilidade, não só no plano jurídico-material, mas ao nível do regime económico-financeiro e dos contratos de aquisição de bens e serviços.

A evolução do regime jurídico e a constante reestruturação do setor das comunicações deu origem à criação de um organismo público de supervisão e regulação do setor - Instituto de Comunicações de Portugal (ICP).

O aparecimento no plano jurídico nacional desta entidade, separada organicamente do Governo, tem início na década de oitenta, através do artigo 7º do Decreto-Lei n.º 188/81, de 2 de julho[9]. Regido por princípios gerais das comunicações, o ICP foi concebido como um organismo integrado na administração indireta do Estado[10], destinado a apoiar o Governo no âmbito das comunicações e a exercer funções de gestão do espaço radielétrico, de homologação de equipamentos e materiais e de fiscalização de operadores, funções estas que outrora se encontravam atribuídas ao operador público, os Correios e Telecomunicações de Portugal.

Foi nesse pressuposto que a regulação e a supervisão do setor das comunicações eletrónicas foi posteriormente entregue ao ICP-Autoridade Nacional de Comunicações, por via dos seus Estatutos aprovados pelo Decreto-Lei n.º 309/2001, de 7 de dezembro[11]. Esta autoridade prolongou a personalidade jurídica do ICP[12] e teve como principal objetivo dotar a instância de maior poder de intervenção no mercado do setor, ou seja, dos correios e telecomunicações, face à autoridade anteriormente existente. Esta reforma permitiu a inserção do ICP numa nova categoria designada por "autoridades reguladoras independentes". O ICP-ANACOM surge com diferente orgânica, com maior independência face ao poder político, e munida de um leque de atribuições e competências inerentes à sua função de controlo.

Uma década após a aprovação do Decreto-Lei n.º 309/2001, entraram em vigor a 1 de abril de 2015 os novos estatutos da autoridade reguladora, através do Decreto-Lei n.º 39/2015,

[9] Os seus Estatutos só foram aprovados dois anos mais tarde, pelo Decreto Regulamentar n.º 70/83 de 20 de julho.
[10] Distingue-se da atividade direta, pois esta é "exercida por serviços integrados na pessoa coletiva Estado, ao passo que a administração indireta do Estado é uma atividade que, embora desenvolvida para realização dos fins do Estado, é exercida por pessoas coletivas públicas distintas do Estado" ver FREITAS DO AMARAL, *Curso de Direito Administrativo*, 3ª edição, vol. I, Lisboa, Almedina, 2006, pág. 228.
[11] Revogado pelo Decreto-Lei n.º 39/2015, de 16 de março, à exceção dos artigos 3.º e 5.º, este último na parte em que mantém em vigor o n.º 3 do artigo 28.º do Decreto-Lei n.º 283/89, de 23 de agosto.
[12] Cf. art. 1º, n.º 2, do Anexo ao Decreto-Lei n.º 309/2001, de 7 de dezembro.

de 16 de março, os quais alteraram a designação de ICP-ANACOM para apenas Autoridade Nacional de Comunicações.

Depois de conjugadas prerrogativas de direito público, indispensáveis para o desempenho dos seus poderes de autoridade, com a eficiência do direito privado, porquanto intervém num setor em diária mutação, concebeu-se a ANACOM como pessoa coletiva de direito público, dotada de autonomia financeira[13]. Dispõe de um poder normativo genérico para elaborar e aprovar regulamentos nos casos previstos na lei e quando se mostrem indispensáveis ao exercício das suas atribuições, e ainda, uma vez responsável pela aplicação e fiscalização do cumprimento das leis aplicáveis ao setor das comunicações, de um poder sancionatório, estando os operadores obrigados a colaborar com a autoridade no exercício dos poderes de fiscalização e a prestarem todas as informações solicitadas pela ANACOM. Na verdade, sem poderes para se impor, a regulação careceria de sentido.

Do vasto conjunto de atribuições prosseguidas pela ANACOM, atribuímos especial relevância à obrigação de "contribuir para garantir um elevado nível de proteção dos dados pessoais e da privacidade"[14], atribuição esta sem previsão legal nos anteriores estatutos.

Embora a Lei das Comunicações Eletrónicas (LCE) não pretenda regular o tratamento de dados pessoais, a preocupação pela proteção dos assinantes e utilizadores dos serviços prestados pelos operadores no setor encontra-se normativamente consagrado no seu artigo 27º, n.º 1, al. g), o qual prevê que as empresas que oferecem redes e serviços de comunicações eletrónicas poderão estar sujeitas à obrigação de "proteção dos dados pessoais e da privacidade (…) em conformidade com a legislação aplicável à proteção de dados pessoais e da privacidade". De modo a acautelar o pleno exercício das suas funções, este preceito remete para o regime geral em matéria de tratamento de dados pessoais constante da Lei n.º 67/98, de 26 de outubro, e para o regime especial aplicável às comunicações eletrónicas, assegurada pela Lei n.º 41/2004, de 18 de agosto. Funcionam como elementos complementares, sem substituir ou revogar matéria do setor em análise.

[13] A independência financeira resulta, nomeadamente, das taxas que a ANACOM está devidamente autorizada a cobrar aos regulados, convertidas em receitas, como património próprio da autoridade (art. 37º e 38º dos Estatutos).
[14] Art. 8º, n.º1, al. k), do Decreto-Lei n.º 39/2015, de 16 de março.

II.1.3. Enquadramento jurídico

A criação de um mercado concorrencial no setor das telecomunicações resultou de inspirações europeias, determinantes no processo de liberalização do setor. Para tal, foram elaboradas normas destinadas à regulamentação dos parâmetros essenciais, de modo a permitir a entrada de novos operadores no mercado e a garantir não só a concorrência efetiva como a obediência dos operadores a normas comuns.

É na sequência da conhecida *Revisão 99* que surge um novo ciclo regulatório, o "pacote regulamentar de 2002", posteriormente revisto em 2009, constituído por "diretivas da segunda geração": uma diretiva quadro[15] e quatro diretiva específicas - a diretiva autorização, a diretiva acesso, a diretiva serviço universal e a diretiva relativa ao tratamento de dados e à privacidade no setor das comunicações eletrónicas[16]. Vislumbrando a construção de um mercado único, a diretiva-quadro tipificou um conjunto de procedimentos, de forma a assegurar a aplicação harmonizada do quadro regulamentar em toda a União Europeia, e estabeleceu uma moldura regulamentar comum para as redes e serviços de comunicações eletrónicas.

Neste contexto foi então aprovada a Diretiva 2002/21/CE, de 7 de março de 2002[17], a qual estipula as atribuições de autoridades reguladoras nacionais de forma a garantir a harmonia e a coerência das práticas dos diversos Estados-Membros em matéria de redes e serviços de comunicações eletrónicas. Adicionalmente, este diploma define ainda na alínea c) do artigo 2.º, o conceito de "serviço de comunicações eletrónicas" como correspondentes ao *serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações eletrónicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão,*

[15] Diretiva 2002/12/CE, de 5 de março de 2002, do Parlamento Europeu e do Conselho.

[16] Diretiva 2002/20/CE do Parlamento Europeu e do Conselho relativa à autorização de redes e serviços de comunicações eletrónicas, Diretiva 2002/19/CE do Parlamento Europeu e do Conselho respeitante ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos, Diretiva 2002/22/CE do Parlamento Europeu relativo ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas e Diretiva 2002/58/CE do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas – esta última foi posteriormente alterada pelas Diretivas 2006/24/CE e pela Diretiva 2002/58/CE do Parlamento Europeu e do Conselho respeitante à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

[17] Posteriormente alterada pela Diretiva 2009/140/CE, de 25 de novembro de 2009, com objetivo de colmatar incoerências até aí existentes a nível da aplicação de medidas pelas autoridades reguladoras nacionais

excluindo os serviços que prestem ou exerçam controlo editorial sobre conteúdos transmitidos através de redes e serviços de comunicações eletrónicas; excluem-se igualmente os serviços da sociedade da informação, tal como definidos no artigo 1.º da Diretiva 98/34/CE que não consistam total ou principalmente no envio de sinais através de redes de comunicações eletrónicas.

Já relativamente ao ordenamento jurídico português, a LCE - Lei n.º 5/2004 de 10 de fevereiro- veio consagrar o regime jurídico aplicável às redes e serviços de comunicações eletrónicas e aos serviços conexos, bem como veio definir as competências a autoridade reguladora nacional neste domínio[18].

Embora a LCE tenha sido alvo de diversas alterações[19], foi a sexta, por via da Lei n.º 51/2011, de 13 de setembro, que teve especial impacto a nível da proteção de dados pessoais. Resultante da transposição da Diretiva 2009/136/CE, do Parlamento Europeu e do Conselho, de 25 de novembro[20], a Lei n.º 51/2011 incidiu praticamente sobre todos os grandes temas objeto de regulação, dando origem à reforma da LCE, através da introdução de um conjunto de prerrogativas destinadas à proteção de dados, como reforço da defesa do utilizador final. Por forma a aplicar maior transparência nas condições comerciais apresentadas pelas empresas que oferecem redes e serviços de comunicações eletrónicas, implementou medidas obrigatórias aos prestadores dos referidos serviços, nomeadamente quanto aos elementos a constar nos contratos celebrados com os consumidores. Assim, impôs a obrigação de previsão de medidas que o fornecedor poderá adotar na sequência de incidentes relativos à segurança ou à integridade da rede, ou para reagir perante ameaças ou situações de vulnerabilidade, bem como medidas de proteção do assinante contra riscos para a segurança pessoal, privacidade e dados pessoais[21].

Cumpre evidenciar que esta lei aditou ainda o capítulo V, epigrafado «Segurança e integridade das redes e serviços», composto pelos artigos 54.º-A a 54.º-G, de acordo com o qual as empresas devem garantir as devidas "medidas técnicas e organizacionais adequadas à prevenção, gestão e redução dos riscos para a segurança das redes e serviços visando, em

[18] A Lei n.º 5/2004 revogou a Lei n.º 91/97, de 1 de agosto (Lei de Bases das Tecnologias).
[19] A LCE foi alterada pelos seguintes diplomas legais: Lei n.º 82-B/2014, de 31/12, DL n.º 35/2014, de 07/03, Lei n.º 42/2013, de 03/07, Lei n.º 10/2013, de 28/01, Lei n.º 51/2011, de 13/09, Lei n.º 46/2011, de 24/06), DL n.º 258/2009, de 25/09, DL n.º 123/2009, de 21/05, Lei n.º 35/2008, de 28/07, DL n.º 176/2007, de 08/05).
[20] Esta Diretiva alterou as Diretivas 2002/22/CE e 2002/58/CE, bem como o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação defesa do consumidor.
[21] Art. 48º, n.º 1, al. o) e n) da LCE.

especial, impedir ou minimizar o impacte dos incidentes de segurança nas redes interligadas, a nível nacional e internacional, e nos utilizadores"[22], bem como, ao abrigo do disposto no artigo 54.º-B, notificar a Autoridade Reguladora Nacional, ora ANACOM, das "violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e serviços".

Embora o Lei originária já previsse na al. c), do n.º 4 do artigo 5º a obrigação imposta às empresas para assegurarem um elevado nível de proteção dos dados pessoais e da privacidade de defesa dos interesses dos cidadãos, esta reforma legislativa realçou, de modo claro e evidente, a necessidade de preservar a segurança nas redes e nos serviços e de reforçar as competências regulatórias atribuídas à ANACOM.

[22] Art. 54º-A, n.º 1 da LCE.

III. DA PROTEÇÃO DE DADOS PESSOAIS

III.1. Enquadramento histórico

Os direitos fundamentais consubstanciam o reflexo da sociedade onde o Homem convive em cada época, resultantes das necessidades historicamente impostas. Na linha de PEDRO FERREIRA, tais direitos exercem uma "função de escudo protetor determinados em cada contexto sócio-político"[23]. Na realidade, a vida privada, conjugada com as liberdades fundamentais numa sociedade participada, existe desde a origem dos tempos.

Na sociedade pré-industrial, os documentos respeitantes às relações pessoais eram limitados a uma parte da vida das pessoas e apenas existentes numa pequena elite reinante. A rotina diária não era documentada de forma escrita, e, uma vez que a maioria das relações pessoais decorria da proximidade, era extremamente fácil obter informações de cada cidadão. Todavia, com o modelo de produção industrial, tornou-se necessário e imprescindível criar ferramentas para o próprio planeamento da vida diária, como auxiliares de memória, através de um registo dos factos e acontecimentos do quotidiano. Na realidade, os motivos que conduziram à aprovação das primeiras leis sobre proteção de dados, prendem-se com o facto de as novas tecnologias, sob forma de tratamento eletrónico de dados, possibilitarem um acesso mais fácil e generalizado a informações pessoais, do que os tradicionais e anteriores procedimentos. O crescente levantamento de dados foi uma consequência gradual da diminuição do sentido das ligações pessoais, representado como uma reação lógica da perda de confiança entre as pessoas[24].

O processo de armazenamento, documentação e uso de informações pessoais transformou-se numa condição *sine qua non* para a formação da nossa sociedade moderna.

A nível europeu, é a partir da década de 70 que começam a surgir as primeiras preocupações em regular a proteção contra os sistemas de informação automatizada que se apresentassem como perigos de intromissão indevida na vida privada[25]. Inicialmente na Alemanha, depois na Suécia e França, começaram a aparecer as primeiras atividades

[23] PEDRO FERREIRA, *A Proteção de Dados Pessoais na Sociedade de Comunicação - Dados de Tráfego, Dados de Localização e Testemunhos de Conexão*, Lisboa, O Espírito das Leis, 2006, pág. 71.
[24] Neste sentido, REGINA LINDEN RUARO, DANIEL PIÑEIRO RODRIGUEZ, BRUNIZE FINGER " O Direito à Proteção de Dados Pessoais e a privacidade" , *in Revista da Faculdade de Direito da Universidade Federal do Paraná*, Curitiba, n.53, 2011, pág. 143.
[25] AMADEU GUERRA, *Lei Proteção de Dados Pessoais*, "Direito da Sociedade de Informação", Vol. 2, Faculdade de Direito de Lisboa, Coimbra, Coimbra Editora, pág. 146.

legislativas focadas no controlo do processamento de dados por organismos públicos e na defesa dos direitos fundamentais dos cidadãos, enquanto "autogarantias" das sociedades democráticas.

Devido ao crescimento do fluxo transfronteiriço de dados, a Recomendação de 1981 deu origem à Convecção n.º 108, aprovada pelo Comité de Ministros em 28 de janeiro e respeitante à "Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados Pessoais". O aumento exponencial da utilização de dados pessoais e a consequente urgência em harmonizar o mercado único entre os vários Estados-Membros, impulsionou a União Europeia a regular a matéria da proteção de dados pessoais, tendo sido publicada, em 24 de janeiro de 1995, a Diretiva 95/46/CE relativa à "proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados".

De modo a proteger as informações pessoais de um tratamento e uso abusivos, a diretiva estipulou um conjunto de princípios reguladores do tratamento de dados pessoais automatizados e não automatizados, aplicáveis ao responsável pelo tratamento. Para tal, consagrou, no seu artigo 7º, o princípio do consentimento[26], segundo o qual tratamento dos dados pessoais ficaria dependente, regra geral, do consentimento inequívoco do titular dos dados.

A contínua evolução das tecnologias de informação, com particular ênfase no início do século XXI, tornou cada vez mais imperiosa a necessidade de proteger a informação para que a sua utilização inadequada não viesse a servir interesses ilegítimos e atentatórios dos direitos, liberdades e garantias dos cidadãos[27]. Foi a necessidade de definir um enquadramento jurídico equilibrado e ajustado à realidade que levou a União Europeia a adotar a Diretiva 2002/58/CE, e 17 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, que elenca as condições em que os Estados-Membros podem restringir os direitos e obrigações dos prestadores dos serviços de comunicações para salvaguardar a segurança nacional, a defesa, a segurança pública, de modo

[26] Grupo de Trabalho do Artigo 29º esclarece que o requisito essencial do consentimento "é que a declaração ou o ato signifique claramente o acordo do titular dos dados relativamente ao tratamento dos dados pessoais que lhe dizem respeito". Ver GRUPO DE TRABALHO DO ARTIGO 29º PARA A PROTEÇÃO DE DADOS, Parecer 08/2012, que presta um contributo suplementar o debate sobre a reforma em matéria de proteção de dados, Adotado em 5 de outubro de 2012, WP197. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_pt.pdf.

[27] ANA VAZ, "Segurança da Informação, Proteção da Privacidade e dos Dados Pessoais", *in Noção e Defesa*, verão 2007, N.º 117 - 3.ª Série, pág. 35

a prevenir e investigar infrações penais ou a utilização ilegítima das comunicações eletrónicas[28].

Esta Diretiva regula o período de conservação dos dados recolhidos no âmbito das comunicações eletrónicas: dados de tráfego e de localização. Os dados de tráfego só podem ser conservados pelo período necessário para concretizar a transmissão da comunicação, pelo que depois deverão ser eliminados ou tornados anónimos. Todavia, do conjunto de dados que incorporam os dados de tráfego podem ser armazenados e tratados os necessários para efeitos de faturação, e até quando a fatura puder ser legalmente contestada ou o pagamento reclamado. Os dados de localização, regra geral, só podem ser trabalhados se forem anónimos. Porém, o utilizador das redes de comunicação pode consentir na recolha e tratamento desses dados, devendo ser mantidos na medida do necessário e pelo período estritamente indispensável para a prestação de serviços de valor acrescentado. É de notar que a Diretiva 2006/24/CE, de 15 de março de 2006, veio alargar o prazo de conservação de dados de tráfego e de localização. Estabeleceu a obrigação de conservar determinados dados, elencados no seu artigo 5º, pelo prazo não inferior a seis meses e não superior a dois anos.

Já a Lei n.º32/2008, de 17 de julho, que transpôs a Diretiva 2006/24/CE, delimita no seu artigo 6º que os dados devem ser conservados pelo período de um ano a contar da conclusão da transmissão.

III.2. Do conceito de Dados Pessoais

Na linha do previsto no artigo 2º da diretiva 95/46/CE, "dados pessoais" equivalem a qualquer informação relativa a uma pessoa singular identificada ou identificável, qualificando-se como tal não só uma informação que diretamente identifica uma pessoa, como também o conjunto de informações que a possam identificar, através de um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.

[28] Após os atentados terroristas de Madrid, foi aprovada uma nova Diretiva sobre a matéria (Diretiva 2006/24/CE) que, restringindo embora alguns direitos no âmbito da proteção dos dados pessoais e da privacidade, vem criar melhores condições para se utilizarem os dados das comunicações no combate à criminalidade e ao terrorismo.

Contudo, a materialização do direito à proteção de dados pessoais, enquanto direito tecnologicamente determinado, apenas surge com o aparecimento da tecnologia. De modo a colmatar a até aí ausente consagração e proteção jurídica, foram tidos em apreço três princípios essenciais: privacidade, liberdade de expressão e sigilo das comunicações[29].

Importa referir que o conceito acimo referido de dados pessoais corresponde a uma noção ampla que se manteve em todo o processo legislativo. O objetivo das regras contidas na diretiva é, afinal, a proteção das pessoas singulares. O artigo 1.º, quer da Diretiva 95/46/CE quer da Diretiva 2002/58/CE, espelha de modo evidente a finalidade de proteção da liberdade e dos direitos fundamentais das pessoas singulares, especialmente o direito à vida privada. Na linha do defendido pelo Grupo de Trabalho instituído pelo artigo 29.º da Diretiva 95/46/CE[30], este objetivo corresponde a um elemento fundamental a ter em consideração na interpretação e aplicação das regras vigentes, que poderá ser determinante para determinar a forma de aplicação das normas aos inúmeros casos em que os direitos das pessoas singulares não estão efetivamente em risco, podendo, porventura, prevenir contra qualquer outra interpretação das regras[31].

Uma vez consagrada uma noção ampla de dados pessoais, a aplicação das regras tem de ser cautelosa e restringir a necessidade da sua imposição às situações contempladas pelo legislador. Este, por outro lado, através das derrogações materiais estipuladas no artigo 3.º da Diretiva, conjugadas com os Considerandos 26 e 27, demonstra o modo de aplicação do regime deste regime. Uma vez que o tratamento eletrónico de dados corresponde a um meio de acesso mais célere aos dados pessoais face ao anteriormente existente, a Diretiva, ao abrigo do Considerando 27, pretendeu proteger as formas de tratamento que tipicamente apresentam um maior risco de "acesso fácil aos dados pessoais". Por sua vez, o tratamento de dados não automatizado só está sujeito ao regime estabelecido pela Diretiva se os dados fizerem parte de um sistema de arquivo ou quando se destinam a fazer parte desse sistema[32].

---

[29] Sobre a consagração do direito PEDRO FERREIRA**,** *op. cit.*, pág. 194.

[30] Ou Grupo de Trabalho de Proteção de Dados da União Europeia. Doravante "Grupo de Trabalho", "Grupo do Artigo 29.º" ou, simplesmente, "Grupo". Corresponde a um órgão consultivo europeu independente em matéria de proteção de dados e privacidade, cujas funções se encontram previstas no artigo 30º da Diretiva que o institui.

[31] Neste sentido, GRUPO DE TRABALHO DO ARTIGO 29º PARA A PROTEÇÃO DE DADOS, Parecer n.º 4/2007 sobre o conceito de dados pessoais, Adotado em 4 de julho, 01248/07/PT, WP 136. Disponível em: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

[32] Art. 3º n.º 1 da Diretiva 95/46/CE. O Considerando 26 da Diretiva prevê outra limitação geral à aplicação da proteção de dados nos casos em meios de identificação da pessoa em questão para tratamento dos dados não são "suscetíveis de serem razoavelmente utilizados".

A Lei de Proteção de Dados Pessoais, resultante da transposição desta Diretiva para o ordenamento jurídico português, consagrou no artigo 3º, al. a) uma definição idêntica à da Diretiva, tendo ainda acrescentado que a informação pode constar em qualquer suporte, nomeadamente som ou imagem.

Dada a diversidade entre os Estados-Membros sobre parâmetros essenciais do conceito de "dados pessoais" contido na Diretiva, que poderia eventualmente afetar o correto funcionamento do atual quadro de proteção de dados em contextos diferentes, o Grupo de Trabalho elaborou o Parecer n.º 4/2007, 20 de junho, sobre o conceito de dados pessoais, concluindo que o mesmo assenta em quatro pilares fundamentais: "qualquer informação", "relativa a", "identificada ou identificável" e "pessoa singular".

Em primeiro lugar, o conceito de "qualquer informação" dá imediatamente origem a uma interpretação ampla da noção de "dados pessoais". Evidencia a vontade do legislador em consagrar um conceito alargado de dados pessoais, incluindo assim qualquer tipo de declarações sobre a pessoa, não só de cariz "objetivo", tal como a presença de determinada substância no sangue dessa pessoa, como também informações de natureza subjetiva, como opiniões ou avaliações[33]. Ademais, não é necessário que a informação obtida e objeto de tratamento seja verdadeira ou comprovada para que seja englobada no conceito de "dados pessoais". Na verdade, as regras de proteção de dados preveem inclusivamente a possibilidade de a informação ser incorreta, estando o titular do dado provido do direito de a avaliar e contestá-la através dos meios apropriados[34].

Ao segundo elemento, "relativa a", considerado crucial, está subjacente a ideia de que a informação pode ser considerada como "relativa" a uma pessoa quando recai sobre a mesma[35]. No âmbito da questão da proteção de dados suscitada pelos dispositivos RFID[36], o Grupo de Trabalho realizou um Parecer no qual analisou quando é que a informação pode ser

[33] Este último tipo de declarações constitui uma parte considerável do tratamento de dados pessoais em setores como a banca, para avaliação da fiabilidade dos requerentes de empréstimos, dos seguros ou o emprego – significando, nestes casos, que o utilizador é um requerente fiável, não sendo previsível que morra em breve ou que é um bom trabalhador e, por isso, merece ser promovido. GT identifica alguns exemplos Parecer 4/2007, adotado em 20 de junho, do Grupo de Trabalho do Artigo 29º nº WP 105, pág. 6. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pt.pdf.

[34] Subjacente o princípio da retificação. Ver infra subcapítulo *III.4.1.1*

[35] Embora esta relação seja fácil de apurar na maior parte dos casos, existem situações em que as informações inicialmente apresentadas reportam-se a objetos, processos ou eventos e não ao titular dos dados.

[36] RFID corresponde a uma tecnologia utilizada para identificar, localizar e gerenciar produtos, documentos, animais ou pessoas, sem contacto nem a necessidade de um campo visual e resulta da evolução do sistema de código de barras: ao invés do feixe de luz para capturar dados, a tecnologia RFID utiliza a frequência radio com maior alcance.

admitida como "relativa" a uma pessoa. Aí aferiu que os dados reportam-se "a uma pessoa se se referirem à identidade, características ou comportamento de uma pessoa ou se tal informação for utilizada para determinar ou influenciar a forma como essa pessoa é tratada ou avaliada"[37]. Para tal, na linha do defendido pelo GT no Parecer 4/2007, terão de constar os elementos "conteúdo", "finalidade" ou "resultado", de modo a concluir que o tal dado é "relativo a" uma pessoa, sendo estas condições alternativas e não cumulativas.

Como terceiro elemento, a Diretiva exige ainda que a informação seja relativa a uma pessoa singular "identificada ou identificável"[38]. Resumidamente, considera-se que as informações contêm dados sobre uma pessoa se essa pessoa estiver identificada nessas informações, ou se essa pessoa, embora não esteja identificada, estiver descrita nessas informações de forma que seja possível descobrir quem é a pessoa em causa através de pesquisas adicionais. O TEDH tem afirmado repetidamente que o conceito de "dados pessoais" é idêntico ao previsto não só na CEDH, como na Convenção 108, especialmente no que respeita à exigência de serem relativos a pessoas singulares identificadas ou identificáveis[39]. Por sua vez, são normalmente os "identificadores" que permitem chegar a tal conclusão, pois apresentam uma relação relativamente próxima com a pessoa em questão. A Diretiva na definição de "dados pessoais" refere-se a esses "identificadores" no artigo 2.º quando estabelece que uma pessoa singular é todo aquele que "possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

Por último, o quarto elemento prende-se com a "pessoa singular" enquanto ser humano titular de dados pessoais. Quanto a este parâmetro o direito à proteção dos dados

[37] Ver GRUPO DE TRABALHO DO ARTIGO 29º PARA A PROTEÇÃO DE DADOS, nº WP 10, *Documento de trabalho sobre questões relativas à proteção de dados no âmbito da tecnologia RFID*, adotado em 19 de janeiro de 2005, p. 8. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf

[38] A definição surge na LCE como tecnicamente mais adequada face à anterior Lei 10/91, já que, de acordo com o seu art. 2º e no seguimento do estabelecido na Convenção 108 do Conselho da Europa, seria identificável a pessoa cuja identificação não envolvesse custos ou prazos desproporcionados. Certo é admitir que esta definição poderia desencadear uma total arbitrariedade na determinação do que seja pessoa identificável, e por sua vez do que corresponda a um dado pessoal.

[39] Neste sentido, ver TEDH, acórdão *Amann c. Suíça* de 16 de fevereiro de 2000, queixa n.º 27798/95. Trata-se de um caso em que o TEDH considerou que o armazenamento de dados sobre uma chamada a telefónica de natureza profissional para o requerente estava relacionado com a vida privada deste, tendo sublinhado que o termo «vida privada» não podia ser objeto de uma interpretação restritiva, sobretudo porque o respeito pela vida privada abrangia o direito de estabelecer e desenvolver relações com outros seres humanos e concluiu que tinha havido uma violação do artigo 8.º da CEDH.

pessoais é universal, já que ao abrigo do disposto no artigo 6.º da Declaração Universal dos Direitos do Homem, "todas as pessoas têm o direito a serem reconhecidas como sujeitos perante a Lei". Além disso, segundo o Parecer do Grupo do Artigo 29.º, apenas as pessoas vivas estão protegidas pela legislação europeia sobre proteção de dados [40].

III.3. Consagração constitucional

O regime da proteção dos dados pessoais em Portugal foi desenvolvido a par do crescimento internacional do tratamento jurídico nesta matéria.

A Constituição de 1838 foi das primeiras a fazer referência ao direito à privacidade, ao estatuir no seu artigo 16º o direito à inviolabilidade do domicílio dos cidadãos, o qual dita os termos em que uma intromissão na vida privada do indivíduo era considerada justificada face aos deveres do Estado e do indivíduo[41]. Por sua vez, a Constituição de 1933 determina que a inviolabilidade do domicílio de cada cidadão e o sigilo da sua correspondência constituem um direito e garantia individual[42]. Já em 1976, a CRP, em conjunto com o direito à identidade pessoal, consagrou o direito à reserva da vida privada[43] e familiar, remetendo para a lei a consagração das garantias contra a utilização de informações relativas à vida privada e familiar.

Reconhecido em finais do séc. XIX, o direito à privacidade surgiu com uma certa antecipação face à comercialização informacional. A privacidade[44] foi objeto de análise pioneira no estudo de Samuel Warren e Louis Brandeis, intitulado *The right to privacy: the*

[40] O parecer discute igualmente a interação com dados sobre pessoas mortas, nascituros e pessoas coletivas. Ver Parecer 4/2007 do Grupo de Trabalho do Artigo 29.º, cit., pp. 23-25.
[41] O artigo 16º da CRP prevê expressamente que "a casa do cidadão é inviolável", só podendo nela entrar terceiros se tiverem consentimento, em caso e socorro, reclamação feita de dentro ou "para aboletamento de tropa, feito por ordem da competente autoridade".
[42] Artigo 8º, n.º6 da CRP de 1933.
[43] O primeiro instrumento jurídico internacional a consagrar o direito à reserva da vida privada foi a Declaração Universal dos Direitos do Homem, em 1948, através do 12º ("Ninguém sofrerá intromissões arbitrárias na sua vida privada…"). Na Europa, o direito à reserva da vida privada foi consagrado pela primeira vez na Convenção Europeia dos Direitos do Homem consagrou, em 4 de novembro de 1950. No seu artigo 8º n.º1 pode-se ler que "toda a pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência".
[44] A privacidade foi defendida por SEABRA LOPES como um valor essencialmente urbano e "porventura até elitista". O Autor recorre à descrição do ambiente vivido nas aldeias, no qual a necessidade de privacidade e de reserva da vida privada não subsiste, porquanto, para além de nelas existir um forte sentido de comunidade e consequente entreajuda nas dificuldades, prevalece um "sentimento de partilha dos bons e dos maus momentos que não é compatível com o desconhecimento do que se passa em casa de cada um". Ver J. DE SEABRA LOPES, "A proteção da privacidade e dos dados pessoais na sociedade da informação" in *Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa*, Lisboa, Universidade Católica de Lisboa, 1ª Edição, 2002, pág. 779.

implicit made explicit[45], de 1890, o qual consagrou o *right to be let alone* como direito a ser-se deixado sozinho, ou melhor, o direito a ser-se deixado em paz, defendendo a proteção de pensamentos, emoções e sensações. De acordo com os Autores, cada indivíduo tem o direito de determinar quando é que os pretende revelar, não podendo ser obrigado a fazê-lo. Caso o indivíduo decida revelar essas informações, estas continuam na sua disponibilidade, podendo controlar a publicidade dada às mesmas[46].

Na esteira de GOMES CANOTILHO e VITAL MOREIRA, o direito à privacidade nasceu como subespécie dos direitos de personalidade, e foi configurado como uma verdadeira proibição de acesso e de divulgação, destinado a preservar a intimidade em todas as suas vertentes.

Emergido historicamente da defesa da privacidade, o direito à proteção de dados pessoais encontra-se previsto na nossa Constituição da República desde 1976[47], tendo desde então assumido inquestionável relevância jurídica[48]. Portugal foi um dos primeiros países a reconhecer e consagrar constitucionalmente o direito à proteção de dados pessoais como independente do direito à privacidade. Integrado pelo nosso legislador constitucional nos direitos fundamentais sob o artigo 35º, foi-lhe reconhecida a devida força e dignidade, de modo a proibir que o legislador ordinário, não obstante a admitida existência do direito, o desprovesse das suas características essenciais. Ao determinar que a proteção dos dados pessoais será acautelada por via de uma "entidade Administrativa independente"[49], assegura que a lei ordinária terá de sucumbir e respeitar o direito em causa por via da forçada

[45] Defenderam no seu Artigo pela primeira vez, abertamente e de forma incisiva, o reconhecimento do direito à privacidade e à reserva da vida privada, como um direito das famílias, alegando para tal "*Gossip ir no longer the resource of ilde and the vicious, but has become a trad*e". Disponível em: http://www.english.illinois.edu/-people/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

[46] BRANDEIS, LOUIS D., WARREN, SAMUEL D., "*The Right to Privacy*" in *Harvard Law Review*, Vol. IV, N.º5, dezembro 1890. Disponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[47] O artigo 35º da versão original da CRP, sob a epígrafe de "Utilização da informática", que se manteve inalterada até aos dias de hoje, era composto por apenas 3 números com o seguinte teor:
«1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização.
2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.
3. É proibida a atribuição de um número nacional único aos cidadãos»

[48] LUÍS LINGNAU SILVEIRA, *Configuração Constitucional da Proteção de Dados* in *Em homenagem ao Prof. Doutor Diogo Freitas do Amaral*, Coimbra, Almedina, 2010, Pág. 505.

[49] Art. 35ª, nº 2 *in fine* da CRP.

existência deste organismo, correspondente, no nosso ordenamento jurídico, à Comissão Nacional de Proteção de Dados[50].

O artigo tal como se apresenta nos dias de hoje decorre da revisão constitucional de 1997, a qual estendeu a aplicação do preceito aos dados pessoais tratados em suporte manual[51]. Esta alteração resultou da harmonização do sistema jurídico português perante a Diretiva 95/46/CE do Parlamento e do Conselho, de 24 de outubro de 1995, aplicável tanto aos dados tratados informaticamente como aos dotados de suporte manual. Por conseguinte, a Lei Fundamental prevê que o direito à proteção de dados pessoais subsiste independentemente do suporte em que surjam, sem que para tal se exija o informático. A respetiva epígrafe não sofreu qualquer ajuste, provavelmente devido a falha ou esquecimento do legislador, nem tampouco revela o teor do preceito legal.

De um modo geral, o artigo 35º consagra não só a proteção dos cidadãos perante o tratamento de dados pessoais informatizados[52], como também a faculdade de aceder aos próprios dados pessoais. A matéria de proteção de dados pessoais surge constitucionalmente integrada nos chamados "direitos, liberdades e garantias". Ao reclamar da aplicação do regime estipulado nos artigos 17º e 18º da CRP, o artigo 35º apresenta-se suscetível de aplicação imediata e direta, sem carecer da intermediação do legislador ordinário. É oponível tanto a entidades públicas como a particulares e só pode ser restringido por normas gerais previstas na própria CRP que não atinjam o núcleo dos direitos consagrados, sendo que estas restrições não poderão desrespeitar o cerne desse direito tal como é configurado pela Lei Fundamental. Na verdade, o próprio termo de "dados pessoais" traz à colação outros direitos basilares, tais como o direito à dignidade humana, do desenvolvimento da personalidade, da integridade pessoal e da autodeterminação informativa.

Alterado sucessivamente em 1982, 1989 e por último em 1997, o artigo 35º consagra o direito ao conhecimento dos dados pessoais, o qual se desdobra num feixe de direitos, nomeadamente o acesso, o esclarecimento sobre a finalidade dos dados, o de retificação e

[50] Sobre a CNPD ver infra cap. III.2.

[51] O preceito inicialmente previu "registos mecanográficos", tendo então posteriormente sido adaptado às necessidades atuais.

[52] GOMES CANOTILHO e VITAL MOREIRA defendem que "a fórmula tratamento abrange não apenas a individualização, fixação e recolha de dados, mas também a sua conexão transmissão, utilização e publicação." Ver *Constituição da República Portuguesa Anotada* – Artigos 1.º a 107.º, Volume I, 4ª Edição Revista, Coimbra 2007, Anotação Artigo 35.º pág. 550

atualização, o de contestação, e, finalmente, o direito à eliminação dos dados cujo registo é interdito.

Vejamos.

O direito de informação ou de acesso corresponde ao direito basilar dos demais direitos e traduz-se no direito a ser informado de que os seus dados pessoais estão a ser tratados, por quem, e com que finalidade. Por conseguinte, permite ao titular dos dados exigir do responsável pelo tratamento dos seus dados pessoais que trate as informações que a ele respeitem e que lhas comunique para que possa conhecê-las[53]. Efetivamente, a primeira proteção de que um titular do dado deve dispor é o de conhecer e dele poder dispor, o que por conseguinte implica que o dado solicitado seja facultado sem injustificadas delongas nem envolva custos que por si só dificultem o exercício.

O direito de conhecer a finalidade a que se destina o tratamento dos dados e de controlar a informação disponível a seu respeito é referido como o direito à autodeterminação informativa[54]. Este direito de especial importância estabelece que cada um é livre de decidir o destino das informações que lhe digam respeito. Por sua vez, o direito de informação conjugado com a proibição de acesso de terceiros, salvo autorização legal em contrário, permite aferir que cada cidadão é "dono" dos seus próprios dados[55]. Ademais, ao impor que não se tornem públicos certos dados, veda o acesso de estranhos à informação sobre a vida privada e familiar e obriga a que ninguém divulgue informações deste teor que tenha sobre outrem.

O direito de retificação e atualização, previsto no n.º 1 do artigo 35º da CRP, incide sobre dados eventualmente inexatos ou desatualizados e corresponde ao direito, dirigido ao responsável pelo tratamento dos dados, de retificar e atualizar os seus dados alvo de tratamento[56].

Consagrado no artigo 12º da LPDP, assiste ainda aos titulares o direito de contestação[57]. Caracterizado por apresentar uma faceta mitigada da liberdade de disposição

[53] Art. 11º da LPDP.
[54] GOMES CANOTILHO e VITAL MOREIRA, *op. cit.*, pg. 551.
[55] LUÍS LINGNAU DA SILVEIRA, *Configuração constitucional da proteção de dados*, in Em Homenagem ao Professor Doutor Diogo Freitas do Amara, Coimbra, Almedina, 2010**,** pág. 508
[56] Art. 5º, n.º 1, al. d) da LPDP.
[57] LUÍS LIGNAU SILVEIRA, *op. cit.* pág. 510

dos respetivos titulares, permite-lhes oporem-se ao tratamento dos seus dados pessoais para efeitos de marketing direto[58] ou de qualquer outra forma de prospeção.

O direito à eliminação dos dados, cujo registo é interdito, encontra-se no n.º 3 do artigo 35º da CRP. Salvo nos casos previstos na lei, vigora uma proibição absoluta de tratamento informático de determinados tipos de dados pessoais. Igualmente previsto no artigo 7º da LPDP, visa evitar a existência de registos informáticos de dados de cariz pessoal, nomeadamente dados relativos a convicções filosóficas ou políticas, origem racial ou étnica, saúde, dados genéticos ou vida pessoal[59]. A asserção é feita de modo concludente no que aos chamados dados sensíveis diz respeito[60], uma vez que, dada a sua natureza, poderão representar um maior risco para os titulares dos mesmos. Por conseguinte, o seu tratamento exige uma proteção reforçada, já que o próprio processo pode originar situações discriminatórias. Embora a Lei Fundamental no seu artigo 35º, n.º3 não os inclua no leque de dados sensíveis, a Lei de Proteção de Dados pessoais, por outro lado, ao abrigo do artigo 7º, n.º 1, estabelece que os dados de saúde estão abrangidos pelo conceito de dados sensíveis, logo merecedores de proteção acrescida [61]. No entanto, o seu tratamento é permitido quando for necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde. De todo o modo, cumpre salientar que o que realmente definirá a especial sensibilidade dos dados pessoais será o contexto da sua utilização em detrimento da própria natureza.

A solução adotada pela ordem jurídica portuguesa através da inclusão de informações respeitantes à vida privada do titular dos dados no conjunto de dados sensíveis tem suscitado críticas, designadamente por parte dos representantes da Comissão Europeia, já que esses dados não constam no artigo 8º da Diretiva 95/46/CE. Partilhamos da opinião de LUÍS LINGNAU DA SILVEIRA, o qual defende que tal entendimento carece de justificação, pois o

[58] Ver Parecer da CNPD, "Princípios gerais aplicáveis ao marketing político no âmbito das Comunicações Eletrónicas" de 20 de setembro de 2005. Disponível em: http://www.cnpd.pt/bin/orientacoes/PRINCIPIOS-MARKETING-POLITICO-eprivacy.pdf.

[59] Embora o Código Penal português, no artigo 193º, não consagre qualquer classificação de dados, decorre da própria natureza e função do Direito Penal a inclusão de dados respeitantes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou à ordem étnica, provenientes do reconhecimento constitucional de dados pessoalíssimos.

[60] Dados sensíveis (ou pessoassílimos) reportam-se aos dados pessoais referentes a factos ou atos totalmente invioláveis e inatingíveis, por deveram ser subtraídos ao conhecimento de terceiros, bem como os dados pessoais referentes a aspetos que, ainda que possam ser do conhecimento de terceiros, apresentam uma grande potencialidade para eventuais práticas discriminatórias.

[61] A Diretiva 95/46/CE também os incluiu no art. 8º. Neste sentido veja-se o Acórdão do TC Acórdão 355/97, 7 de maio, que engloba os dados de saúde no conceito de "vida privada".

elenco previsto no artigo 8º deve ser interpretado como um mínimo desprovido de caráter taxativo. O Autor acrescenta ainda que "o direito comunitário deve considerar-se superior à legislação interna" apenas perante "as leis ordinárias, mas não para as normas constitucionais"[62]. Como tal, a Constituição Portuguesa deverá prevalecer sobre as orientações emergentes da Diretiva.

III.4. Comissão Nacional de Proteção de Dados

O legislador ordinário foi estimulado através de verdadeiro impulso legislativo a criar uma entidade responsável pelo controlo e fiscalização do "cumprimento das disposições legais e regulamentares em matéria de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei"[63] – a Comissão Nacional de Proteção de Dados[64].

Nos termos do artigo 35º n.º 2 da Constituição da República Portuguesa, fica a cargo da Lei a definição do conceito de dados pessoais, e bem assim das condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, garantindo a sua proteção, "designadamente através de entidade administrativa independente". Contudo, este preceito não é claro na atribuição de funções, pois é necessário apurar se a entidade deverá restringir a sua atuação em prol da proteção de dados ou se deve estender as suas atribuições à definição do próprio conceito de dados pessoais e às demais previsões estabelecidas no preceito. Na verdade, embora seja a entidade administrativa muitas vezes a determinar estas questões, o seu papel está centrado na proteção dos dados pessoais. Por sua vez, esta função encontra-se delimitada pela lei, enquanto fruto de vontade dos cidadãos, uma vez que a todo o processo de tratamento de dados pessoais subjaz o direito fundamental da reserva da vida privada.

Os poderes da CNPD foram ao longo dos tempos significativamente reforçados, operando nos dias de hoje como um elemento ao serviço da sociedade de informação[65]. O aumento do leque de atribuições deveu-se não só, num primeiro plano, à transposição da Diretiva 95/46/CE, como também à exponencial evolução da tecnologia informática, a qual

[62] LUÍS NOVAIS LINGNAU DA SILVEIRA, *O Direito à Protecçãp de Dados Pessoais (Tentativa de caracterização).* Disponível em: http://www.apdsi.pt/uploads/news/id545/2.11_luis%20silveira_070626.pdf
[63] Art. 22º da LPDP.
[64] Outrora designada por Comissão Nacional de Proteção de Dados Pessoais Informatizados, decorrente da aplicação da Lei n.º 10/91, a qual não era aplicável a ficheiros manuais.
[65] AMADEU GUERRA, *op. cit.*, pág. 154.

não se coaduna com normas rígidas, sob pena de se submeterem a uma acelerada desatualização. O aumento de competências procurou harmonizar o sistema jurídico português perante as orientações europeias e alcançar um equilíbrio entre os direitos, liberdades e garantias dos titulares dos dados e desenvolvimento económico se social, o qual luta pela eliminação de obstáculos ao tratamento e circulação de dados pessoais[66].

III.4.1. Legalização de tratamentos junto da CNPD

Segundo AMADEU GUERRA, a obrigação de notificação a que as entidades responsáveis pelo tratamento de dados pessoais estão obrigadas corresponde, afinal, a um dos pilares fundamentais ao exercício de funções pela CNPD, especialmente no controlo e fiscalização do cumprimento dos preceitos legais e regulamentares a que aquelas estão sujeitas em matéria de proteção de dados[67]. A notificação permite à entidade administrativa *sub judice* definir as condições de tratamento e limitar o processamento de determinado tipo ou categorias de dados, caso os qualifique como excessivos ou não pertinentes, autorizar a sua utilização para finalidades distintas das que justificaram a recolha, permitir interconexões, fixar o tempo de conservação e estabelecer normas de segurança adequadas à natureza dos dados[68]. Na verdade, devem ser comunicados à CNPD todos os elementos essenciais de modo a exercer as suas funções de fiscalização e controlo da legalidade do tratamento, e a verificar se os princípios *infra* sumariamente elencados são respeitados.

Quanto ao controlo e à análise da legalidade, a CNPD deve ser igualmente consultada sobre eventuais instrumentos jurídicos em preparação em instituições europeias ou internacionais respeitantes ao tratamento de dados pessoais, emitindo posteriormente o seu parecer sobre os tratamentos que estejam submetidos a ditames legais[69]. Relativamente aos poderes de decisão, salientamos em traços gerais os seguintes: o poder de autorizar o tratamento de dados sensíveis, ao abrigo do disposto no artigo 7º, n.º 2, e dos dados constantes no artigo 8º, n.º2; autorizar a interconexão de dados pessoais e a utilização dos dados para finalidades diversas das determinantes da recolha (artigo 23º, al. c) e d) da LPDP); autorizar o

[66] A LPDP atribui à CNPD a função de ponderar e procurar o referido equilíbrio, por exemplo, nas situações consagradas no art. 15º, n.º 4, nos termos do qual "A CNPD pode determinar que, nos casos em que a circulação em rede de dados pessoais referidos nos artigos 7.º e 8.º possa pôr em risco direitos, liberdades e garantias dos respetivos titulares, a transmissão seja cifrada".
[67] AMADEU GUERRA, *op. cit.*, pág. 165.
[68] Art. 23º e 115.º n.ºs 2 e 4. Lei n.º 67/98.
[69] Art. 22º, n.º2 e 23.º n.º1, al. a) e 28º, n.º2 da LPDP.

fluxo transfronteiriço de dados para os Estados que não assegure um nível de proteção adequado[70] e o poder de fixar o tempo de conservação dos dados pessoais de acordo com a da finalidade (artigo 23º, n.º 1 al. f) da LPDP).

III.4.1.1. Princípios subjacentes ao tratamento de dados

Conforme AMADEU GUERRA, é a partir do princípio da transparência que surgem os princípios subjacentes ao processo de tratamento de dados pessoais[71]. Previsto no artigo 10º da Diretiva 95/46/CE, na parte inicial do Considerando 39 e no n.º 1 do artigo 12º da Diretiva 2002/58/CE, é considerado o princípio fundamental sobre o tratamento de dados e da qualidade dos mesmos e traduz-se no direito dos titulares serem informados da existência de tratamento dos seus dados e das suas finalidades, bem como da identidade do seu responsável. Por conseguinte, obriga a que o responsável pelo tratamento comunique ao titular dos dados as finalidades do mesmo, quais os dados tratados, o prazo de conservação dos mesmos e outras informações relevantes para o exercício dos seus direitos[72]. Por outras palavras, o princípio da transparência impõe que o indivíduo seja esclarecido e informado de forma detalhada sobre o tratamento efetuado aos seus dados. Este princípio é especialmente assegurado pelo já referido direito de acesso do titular dos dados (artigo 2º da LPDP).

Da Lei Fundamental em conjugação com a LPDP extrai-se o princípio da lealdade, licitude e boa-fé, o qual determina que os dados devem ser recolhidos com o conhecimento do respetivo titular, ficando tal procedimento interdito a terceiros, pois aqui estaria desprovido de controlo do próprio titular. Como tal, o responsável está obrigado a efetuar tratamento em conformidade com a boa fé e de acordo com as normas nacionais, internacionais e europeias aplicáveis em vigor. Ademais, o princípio impõe que os dados só possam ser tratados para os fins que foram recolhidos, o que significa que apenas podem ser utilizados para a realização dos objetivos propostos e autorizados pelo respetivo titular[73].

[70] Artigos 19.º, n.º 2, 20.º, n.º2 e 23.º, n.º1 al. 1), todos da LPDP.
[71] Neste sentido, AMADEU GUERRA, *op. cit.*, pág. 163.
[72] CATARINA SARMENTO CASTRO, "Privacidade e proteção de dados pessoais em rede", *Direito da Sociedade da Informação (VII)*, Coimbra, Coimbra Editora, 2008, pág. 101.
[73] TATIANA MALTA VIEIRA, *O Direito à Privacidade na Sociedade da Informação – Efetividade desse direito fundamental diante dos avanços da tecnologia da informação*, Porto Alegre, Sergio Antonio Fabris Editor, 2007, pág. 283.

O princípio do consentimento que prevê que o tratamento dos dados pessoais dependa, regra geral, do consentimento de forma inequívoca do titular dos dados[74]. Por conseguinte, as informações detidas para certo fim poderão ser utilizadas para finalidades diversas tão-somente nos casos em que haja consentimento "prévio e expresso" do titular dos dados[75].

Por sua vez, o princípio da finalidade exige que os dados pessoais não possam ser utilizados para finalidades incompatíveis com as que originaram a sua recolha, sendo apenas possível a sua recolha para determinados fins, explícitos e legítimos. A finalidade tem de estar previamente determinada e informada ao próprio titular dos dados sujeitos a análise.

Já o princípio da proporcionalidade exige que os dados pessoais devem ser tratados de forma adequada e não excessiva, salvaguardado a justa medida entre a satisfação dos interesses que conduziram à sua recolha e a privacidade dos respetivos titulares[76].

O princípio da limitação do prazo de conservação, do qual decorre o direito ao esquecimento dos titulares, determina que apenas possam ser tratados e conservados os dados pelo período estritamente necessário à realização dos fins para que foram recolhidos, o que significa que não devem ser preservados para tratamento posterior ou por tempo indeterminado[77]. De modo a garantir que tal não ocorra, a Lei n.º 67/98, de 26 de outubro, ao abrigo do disposto no artigo 23.º, n.º1 al. f), conferiu à CNPD competência para fixar o tempo de conservação de dados pessoas em função da finalidade, tendo ainda a possibilidade de emitir diretivas sobre a matéria para certos setores de atividade. Em concordância com JOSÉ RENATO GONÇALVES, duvidamos, contudo, da adequação e da admissibilidade legal de um impedimento de acesso aos dados de saúde, por exemplo por um prazo de um ano, ou a quaisquer outros cujo conhecimento seja essencial para uma pessoa fazer valer um direito fundamental, inclusivamente pelo próprio titular dos dados, a quem os mesmos respeitam[78]. Contudo, a limitação temporal do armazenamento de dados pessoais só é aplicável aos dados conservados sob uma forma que permita a identificação das pessoas em questão. Desta forma,

[74] Art. 7º da Diretiva 95/46/CE e art. 7º da LPDP.
[75] Assim não será nas situações previstas no artigo 7º n.ºs 3 e 4 da LPDP.
[76] Previsto na al. c) do n.º 6 da Diretiva 95/46/CE, e bem assim na al. c) do n.º1 do art. 5º da LPDP.
[77] Consagrado na Diretiva de 95/46/CE (art. 6º n.1 al. e)), na Convenção 108 (art 5º al .e)), na Diretiva 2002/58/CE (Considerando 23), na LPDP (art. 5º n.1 al. e)), bem como na Lei 41/2002, no art. 6º, n.º 1 *in fine*.
[78] JOSÉ RENATO GONÇALVES, "Regime dos 'Dados Pessoais' Informatizados", *in SCIENTIA IURIDICA*, Braga, 2002, pág. 76.

é então possível conservar licitamente dados que já não sejam necessários mediante a sua anonimização ou "pseudonimização"[79].

Admitindo-se que informação significa poder, pode ainda ser delineado o princípio da minimização, o qual opera no sentido de reduzir ao mínimo e estritamente possível o tratamento de dados, de modo a evitar que terceiros detenham poder sobre aqueles cujos dados pessoais são alvo de tratamento[80].

O incumprimento destes e outros princípios conexos implícitos no processo de tratamento de dados pessoais pode dar origem à aplicação de sanções, não só pela CNPD como pela ANACOM, nas respetivas áreas de competência[81].

[79] Princípio defendido no Relatório Explicativo da Convenção 108 refere, no seu artigo 42.º, que o requisito relativo ao prazo máximo de armazenamento dos dados na sua forma nominativa não significa que, passado algum tempo, esses dados devem ser irrevogavelmente separados do nome da pessoa a quem dizem respeito, mas apenas que não deverá ser fácil estabelecer a ligação entre os dados e os elementos de identificação, objetivo este que poderá ser alcançado através da "pseudonimização" dos dados, ou seja, substituindo os elementos de identificação por um pseudónimo.

[80] Consagrado, p.e., na Recomendação de 12 de maio de 2010, relativa à utilização de uma metodologia harmonizada para classificar e comunicar queixas e pedidos de informação dos consumidores (2010/304/EU). Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32010H0304&from=EN

[81] A título de exemplo, a LPDP prevê aplicação de uma coima mínima de 498,80€ e máxima de 4.988€ às entidades que não respeitarem o direito à oposição dos titulares dos dados, por força do disposto no art. 38º *ex vi* art. 12º da LPDP.

IV. PROTEÇÃO DE DADOS PESSOAIS NO SETOR DAS COMUNICAÇÕES ELETRÓNICAS

IV.1. Breve referência comparativa - CNPD Vs. ANACOM

Em termos gerais, as entidades ora analisadas desempenham a função de assegurar o cumprimento da lei no que se refere à proteção dos dados nas comunicações eletrónicas.

A CNPD, por um lado, mais vocacionada para a proteção dos dados pessoais, é responsável por garantir que o acesso à informação armazenada no equipamento terminal respeitante a um assinante ou a qualquer utilizador só é autorizado quando este for devidamente informado sobre os objetivos da recolha e tratamento de dados, sendo para tal dada a possibilidade de recusa de tratamento. Ademais, assume um papel fundamental ao impor às empresas do setor a obrigação de informarem os assinantes do risco, de forma gratuita, sempre que se verifique o risco de violação da segurança de rede com repercussões sobre os dados pessoais de que estes são titulares[82].

Por outro lado, a ANACOM, enquanto entidade reguladora das comunicações, é o organismo responsável por assegurar que as empresas que oferecem serviços de comunicações eletrónicas e os fornecedores de rede pública de comunicações colaboram entre si e adotam as medidas adequadas à prevenção dos riscos inerentes ao setor, garantindo, assim, que as técnicas organizacionais são eficazes para manter a segurança não só dos seus serviços como também própria rede[83].

IV.2. Lei da Proteção de Dados Pessoais e Privacidade nas Telecomunicações

Num âmbito mais restrito das comunicações eletrónicas, emerge um conjunto de diplomas legais destinados à proteção da privacidade neste setor. A Lei n.º 69/98, de 28 de outubro, transpondo a Diretiva 97/66/CE, do Parlamento Europeu e do Conselho, foi pioneira

[82] Art. 3º, n.º 10 da Lei n.º 41/2004.
[83] Art. 3º, n.ºs 1 e 2 da Lei n.º 41/2004.

e veio regular o tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrónicas

A Lei n.º 69/98, de 28 de outubro, consagrou desde logo a confidencialidade das comunicações e a proibição de escutas, ao abrigo do disposto no artigo 5º, n.º 2. Ademais, este diploma para além de estabelecer a obrigação de eliminação de dados de tráfego ou de os tornar anónimos, logo que a respetiva chamada terminasse, também determinou que, quanto à faturação, o tratamento de dados apenas era lícito até ao final do período durante o qual a fatura poderia ser legalmente contestada ou cujo pagamento poderia ser reclamado[84].

Quatro anos após a publicação daquela lei, a Diretiva 2002/58/CE[85] revogou a Diretiva que deu origem à Lei n.º 69/98, de 28 de outubro, tendo ficado conhecida pela Diretiva relativa aos dados pessoais. Nascido do "boom" da Internet, este diploma legal, no Considerando 6, relembra a perigosidade da Internet e dos riscos associados a este sistema global de redes de computadores interligados: a Internet, embora permita criar uma infraestrutura mundial destinada ao fornecimento de um leque de serviços de comunicações eletrónicas, aumenta a probabilidade da violação da proteção de dados pessoais e da privacidade dos respetivos titulares.

A transposição para o ordenamento jurídico português foi realizada pela da Lei n.º 41/2004 de 18 de agosto, revogando assim a Lei nº 69/98. Em termos semelhantes aos previstos no artigo 5º n.º1 da Diretiva, a lei reservou um artigo dedicado à "Inviolabilidade das comunicações eletrónicas", sob o artigo 4º.

Dois anos volvidos, foi publicada a Diretiva 2006/24/CE[86], de 25 de maio, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que alterou a Diretiva 2002/58/CE. De acordo com o n.º 2 do artigo 1º, a Diretiva teve como principal objetivo "harmonizar as disposições dos Estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de

[84] Art. 6º da Lei n.º 69/98.
[85] Comummente designada por *Diretiva E-Privacy*, uma vez que incide sobre a privacidade nas comunicações eletrónicas.
[86] Conhecida como a *Data Retention Directive.*

investigação, de deteção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro.

Embora a implementação desta Diretiva não tenha sido fácil devido, nas palavras de RITA NEVES, ao "caráter invasivo da privacidade que lhe está subjacente"[87], foi transposta para o nosso ordenamento através da Lei n.º 32/2008, de 17 de julho, a qual, ao abrigo do seu artigo 4º, n.º 1, estabeleceu as categorias de dados a conservar, designadamente a fonte de uma comunicação, o seu destino, a respetiva data, hora e duração, o tipo da comunicação, o equipamento de telecomunicações dos utilizadores e a localização do próprio equipamento de comunicação móvel. Esta lei impõe aos operadores a obrigação de conservar os dados durante um ano a contar da data da conclusão da comunicação[88], sendo esta obrigação de conservação e transmissão efetuada quanto aos dados de tráfego e de localização[89], "bem como dos dados conexos para identificar o assinante ou o utilizador registado, gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações para fins de investigação, detenção e repressão de crimes graves por parte das autoridades competentes"[90]. Este diploma realça, contudo, através do n.º2 do artigo 1º, a proibição expressa da conservação de dados que revelem o próprio conteúdo das comunicações, "sem prejuízo do disposto na Lei n.º 41/2004, de 18 de agosto, e na legislação processual penal relativamente à interceção e gravação de comunicações".

Cumpre salientar que em 8 de abril de 2014, o TJUE declarou inválida a Diretiva 2006/24/CE, dada a interferência com direitos fundamentais de praticamente toda a população europeia, o que permitiria retirar conclusões precisas sobre a vida privada dos titulares dos

[87] RITA CASTANHEIRA NEVES, *As ingerências nas comunicações eletrónicas em processo penal: natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova*, Coimbra, Coimbra Editora, 2011, pág. 74.

[88] O nosso sistema jurídico português adotou um prazo inferior ao estabelecido no art. 6º da Diretiva 2006/24/CE, a qual estipula dois anos.

[89] Os dados de tráfego são os dados recolhidos para efetuar o envio da comunicação ou para efeitos de faturação. De acordo com o Considerando 15 da Diretiva 2002/58/CE podem ser considerados dados de tráfego os relativos "ao encaminhamento, à duração, ao tempo ou ao volume de uma comunicação, ao protocolo utilizado, à localização do equipamento terminal do expedido ou do destinatário, à rede de onde provém ou onde termina a comunicação, ao início, fim ou duração de uma ligação." Os dados de localização são dados referentes à localização do utilizador, que segundo o Considerando 14 da diretiva 2002/58/CE podem incidir sobre " a latitude, a longitude e a altitude do equipamento terminal do utilizador, sobre a direção de deslocação, o nível de precisão da informação de localização, a identificação da célula de rede em que o equipamento terminal está localizado em determinado momento e sobre a hora de registo da informação de localização.".

[90] Art. 1º, n.º1 da Lei 32/2008. Porém o n.º2 deste artigo realça a proibição de conservação de dados que revelem o conteúdo das comunicações.

dados retidos[91]. Todavia, a decisão do Tribunal de Justiça não prejudicou a vigência da Lei n.º 32/2008[92], pois, embora este diploma resulte da transposição daquela Diretiva, a validade de atos nacionais só pode ser apreciada pelos tribunais nacionais[93].

Com este novo pacote legislativo impôs-se aos operadores uma maior exigência ao nível das obrigações e uma menor flexibilidade ao nível comercial e contratual, dada a maior regulamentação da relação entre operadores e clientes.

IV.2.1. Regime atual

A primeira alteração da Lei n.º 41/2004, de 18 de agosto, foi efetuada pela atual Lei da Proteção de Dados Pessoais e Privacidade nas Telecomunicações em vigor no ordenamento jurídico português, resultante da transposição da Diretiva 2009/136/CE. A Lei n.º 46/2012, em 29 de agosto, à semelhança da alterada, incide sobre a matéria do tratamento de dados pessoais e à proteção da privacidade no setor das Comunicações eletrónicas.

Desprovida do tradicional período de *vacatio legis*, a Lei n.º 46/2012 entrou em vigor no dia seguinte ao da sua publicação, atribuindo novas competências à CNPD e à ANACOM, com especial incidência nas suas funções de supervisão e de controlo, no reforço da segurança do processamento do tratamento de dados pessoais dos utilizadores e assinantes e no combate à invasão da privacidade dos titulares dos dados por comunicações não solicitadas para fins de comercialização direta, no contexto da utilização de redes de comunicações eletrónicas.

A todo o regime estão subjacentes os princípios plasmados na LPDP e acima sumariamente identificados, tendo necessária aplicação no tratamento de dados pessoais no contexto das comunicações eletrónicas.

De forma a reforçar a segurança e os poderes da CNPD, a atual lei aditou à anterior o artigo 3º-A, no qual consagrou o regime da notificação a esta entidade responsável pela proteção de dados pessoais. Para tal, introduziu no setor das comunicações eletrónicas a

[91] O Acórdão invoca argumentos como a ausência de diferenciação, imitação ou exceção dos indivíduos, meios de comunicação eletrónica ou dos dados relativos ao tráfego em função do objetivo de luta contra os crimes graves, a inexistência de critérios objetivos face ao extenso período de conservação, desde 6 24 meses, e a omissão de qualquer imposição de conservação de dados na União (Acórdão no s processos apensos C-2932 e C - 594/12, disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=PT)

[92] Embora reconheçamos que este é um assunto que carece de uma reflexão mais prolongada, tal não compatível com os propósitos do presente estudo.

[93] A desarmonia do regime previsto nesta Diretiva com o Direito da União Europeia ou com as Constituições nacionais de países como a Bulgária, Roménia, Alemanha, Chipre e República Checa, deu origem a efetivas declarações de inconstitucionalidade das normas resultantes das transposições da Diretiva por estes países.

obrigatoriedade de notificação de *data breaches* à CNPD pelas empresas prestadoras de serviços de comunicações eletrónicas, bem como aos titulares dos dados pessoais violados, sempre que a violação possa "afetar negativamente os seus dados pessoais"[94], de modo a que aqueles possam tomar as devidas precauções[95]. Porém, caso seja comprovado perante a CNPD e reconhecido por esta que foram tomadas todas as medidas tecnológicas de proteção adequadas e aplicadas aos dados a que violação dizia respeito, de modo a convertê-los em dados incompreensíveis para todas as pessoas não autorizadas a aceder-lhes, a segunda notificação será desnecessária.

Contudo, e salvo melhor opinião, cremos que estas medidas de combate à violação de dados pessoais e de garantia de cooperação entre a CNPD e as entidades responsáveis pela prestação dos serviços será de difícil concretização, uma vez que a violação dos dados advém, na sua maioria, das próprias entidades prestadoras dos serviços a operar no setor.

No âmbito da proteção de dados pessoais, foi atribuída à CNPD a competência de supervisão, pelo que, sempre que ocorra uma violação deste teor, as empresas responsáveis pela prestação do serviço devem notificá-la, indicando não só as consequências da violação dos dados pessoais como detalhando as medidas por elas propostas ou tomadas para remediar a violação. Pode ainda, ao abrigo do referido no n.º 9 do artigo 3.º-A, esta autoridade emitir orientações ou instruções de acordo com as decisões emergentes da Comissão Europeia sobre as circunstâncias em que as empresas que oferecem serviços na área em estudo estão obrigadas a notificar a violação de dados e bem assim sobre a forma e o procedimento aplicáveis a essas notificações. Este artigo introduz ainda o poder de fiscalização do cumprimento das obrigações de notificação, impondo às sobreditas empresas a obrigação de assegurarem um registo das situações de violação de dados pessoais, no qual inscrevem os respetivos factos, efeitos e medidas tomadas.

Por outro lado, os prestadores de serviço encontram-se vinculados a tomarem as medidas necessárias e adequadas ao seu dispor, de modo a assegurar a confidencialidade das comunicações e impedir o acesso não autorizado às redes públicas de comunicações.

---

[94] Art. 3.º-A, n.º2. Por sua vez, o n.º 3 esclarece que é entendida como violação de dados pessoais aquela que afeta negativamente os dados ou a privacidade do assinante ou do utilizador "sempre que possa resultar, designadamente, em usurpação ou fraude de identidade, danos físicos, humilhação significativa ou danos para a reputação, quando associados à prestação e utilização de serviços de comunicações eletrónicas acessíveis ao público".

[95] Quanto ao conceito de *data breaches*, ver infra cap. *IV.3.*

Entre os vários poderes da ANACOM, destacamos a competência para emitir recomendações sobre as melhores práticas ao nível das medidas de segurança, que as empresas prestadoras de serviços de comunicação já estavam obrigadas a adotar ao abrigo da lei anterior, de auditar essas mesmas medidas, de forma direta ou mediante entidade independente e realizar auditorias de segurança extraordinária[96]. Esta atribuição visa garantir um maior grau de efetividade e eficiência das medidas, já que a lei anterior apenas fazia alusão ao dever das empresas prestadoras de serviços de comunicações eletrónicas adotarem medidas de modo a atestar a segurança dos respetivos serviços, e, se necessário, da rede. Contudo a Lei n.º 46/2012, de 29 de agosto faz recair sobre a ANACOM a obrigação de solicitar parecer à CNPD nos casos que envolvam matérias de proteção de dados pessoais[97].

De forma a assegurar uma melhor fiscalização e garantia do cumprimento da lei, uma vez impostas obrigações, a ANACOM pode então solicitar esclarecimentos às empresas relacionadas com a atividade por elas desempenhada, sempre que julgue convenientes, podendo, ainda, determinar as circunstâncias e a periodicidade do envio dessas informações (artigo 13º- E da Lei n.º 46/2012).

A Lei n.º 46/2014 introduziu um inovador regime sancionatório perante o incumprimento dos deveres legalmente estabelecidos, ampliando o campo de competências a nível sancionatório das entidades analisadas, através de três novos expedientes sancionatórios. Para além da até então atribuída faculdade de aplicação de coimas pelo incumprimento da Lei, as duas entidades ICP e CNP partilham ainda competências relativas à instauração, instrução e arquivamento de processos tendo sido acrescentado outros poderes como admoestações, sanções acessórias e sanções pecuniárias.

A admoestação corresponde a uma pena de substituição de uma pena concreta de multa e consiste numa solene censura oral feita ao visado. A inclusão deste tipo de sanções na Lei teve como principal objetivo reforçar da tutela punitiva dos ilícitos, e é aplicada aos casos que não se apresentam como suficientemente gravosos para a aplicação de coima sem qualquer tipo de consequência repreensiva. Quanto às sanções acessórias, cumpre salientar que caso a competência para a aplicação de medidas punitivas seja da ANACOM, esta entidade poderá, quando a culpa do agente o justificar, aplicar uma sanção acessória de perda a favor do Estado de objetos, equipamentos e dispositivos ilícitos e mesmo do "produto do

[96] Art. 3º nºs 4 a 8 da Lei n.º 46/2012.
[97] Art. 3º n.º10 da Lei n.º 46/2012.

benefício obtido pelo infrator através da prática da contraordenação", de acordo com o disposto no artigo 15.º-A. Ao aditar este artigo à lei anterior, a Lei n.º 46/2014 realça a necessidade de cumprimento pelo infrator da sanção acessória que lhe tenha sido aplicada, sob pena de incorrer em crime de desobediência qualificada[98].

Ao abrigo do artigo 15º-C, foi ainda expressamente atribuída à CNPD e à ANACOM a faculdade de imposição de sanções pecuniárias compulsórias, com um montante diário mínimo de €500 e o montante máximo de €100.000,00, sendo o valor concreto calculado de acordo com critérios de razoabilidade e proporcionalidade, e bem assim atendendo à situação económica do agente[99]. Nos termos do artigo 15º, a competência entre ambas é repartida essencialmente conforme o ilícito cometido, sendo que ANACOM detém um poder muito específico de aplicar a sanção acessória de "perda a favor do Estado de objetos, equipamentos e dispositivos ilícitos, incluindo o produto do benefício obtido pelo infrator através da prática da contraordenação"[100].

Importa referir que a CNPD foi ouvida aquando a preparação deste diploma legal, tendo emitido dois Pareceres: 33/2012 e 34/2012[101]. No segundo, pronunciou-se sobre a inclusão destes novos poderes sancionatórios, e defende que, atenta a sua natureza e vocação, "não considera necessário ou indispensável ao cabal exercício das suas atribuições e competências o recurso às sanções pecuniárias compulsórias, uma vez que detém poderes de autoridade, e investigação, de inquérito e, designadamente, de deliberar sobre aplicação de coimas"[102].

Das diversas medidas implementadas no sistema, destacamos as proibições e limitações ao armazenamento das comunicações e dos dados relativos aos assinantes, bem como a obrigação de eliminação dos dados de tráfego. Com efeito, a Lei 46/2014 veio determinar que os dados de tráfego apenas podem ser tratados na medida e pelo tempo necessários, desde que se haja previamente obtido o consentimento prévio e "expresso" do

[98] Vide art. 348.º, n.º 2 do Código Penal.
[99] Designadamente ao seu volume de negócios no ano civil anterior e ao impacto negativo do incumprimento no mercado e nos utilizadores. (art. 15º-C, n.º3 da Lei 46/2012). Relativamente a pessoas coletivas, de acordo com o artigo 14º, n.º 1, foram mantidos os valores mínimos e máximos das coimas aplicáveis a pessoas coletivas (€ 5.000 de coima mínima; 5.000.000€ de coima máxima).
[100] Art. 15º-A da Lei n.º 46/2012.
[101] Pareceres 33/2012 e 34/2012 da CNPD disponíveis em: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=37091
[102] Ao abrigo do disposto nos artigos 22º, n.º3, alíneas a), b), e artigo 23º, n.º1, alínea n), da LPDP. Acrescenta ainda que nos termos do regime sancionatório previsto nesta lei, o incumprimento de ordens encontra-se tipificado como crime (Cf. Art. 43º, n.º1, al. e) e art. 46º da LPDP)

titular[103]. Esta alteração introduziu pressupostos de admissibilidade mais restritos e exigentes face ao regime anterior[104], porquanto o consentimento tácito corresponde tão simplesmente a uma mera não oposição, impondo agora o consentimento expresso, de modo a provocar verdadeira consciencialização da necessidade de autorização.

A Lei n.º 46/2012 procedeu ainda à segunda alteração do Decreto-Lei n.º 7/2004, de 7 de janeiro, e à consequente revogação do artigo 22.º deste Decreto-Lei. Por sua vez, o regime das "Comunicações não solicitadas" passou a ser regulado pela Lei n.º 41/2004, nos termos previstos no artigo 13.º-A. Apesar do inquestionável reforço da proteção de dados pessoais dos utilizadores e de salvaguardar de forma evidente a sua esfera de privacidade, a Lei n.º 46/2012 criou novos entraves aos vendedores *online* na aproximação aos consumidores. A exigência de criação e manutenção de uma "Lista de Consentimentos", para além da até então obrigatória "Lista de oposições", provocou um agravamento substancial das obrigações a que as entidades emissoras de comunicações promocionais estão adstritas para fins de marketing direto. Após a publicação desta Lei, as empresas passaram a ser obrigadas a consultarem a "lista de recusas da Direção geral do Consumidor" e de salvaguardarem o direito de *opt in* [105] dos utilizadores.

De igual forma, a Lei em estudo introduziu alterações no regime legal aplicável aos *Cookies*. Ao invés do consagrado no sistema anterior, a Lei n.º 46/2012 passou a depender a possibilidade de utilização de *cookies*[106] da exigência do prévio consentimento do assinante ou utilizador, "com base em informações claras e completas nos termos da Lei de Proteção de Dados Pessoais, nomeadamente quanto aos objetivos do processamento", deixando de ser suficiente a mera "não oposição" manifestada pelo assinante ou utilizador[107]. O regime até aí

[103] Art. 6º, n.º 4 da Lei n.º 46/2012.

[104] Prescrevia o regime anterior ao abrigo do art. 6º, n.º4 que era bastante o consentimento prévio, sendo admissível se proferido tacitamente.

[105] *Opt in* ou sistema de oposição positiva traduz-se no regime em que é admitido o recurso a comunicações não solicitadas apenas nos casos em que o destinatário manifeste a intenção de receber, a qual afasta a presunção de aceite pelo silêncio (também comummente designada por "regra do consentimento prévio"). Por outro lado, o regime de *opt out* (sistema de oposição negativa) quele em que é permitido o recurso ao envio de mensagens publicitárias não solicitadas, exceto se o destinatário se opuser a recebê-las. *In* Parecer 4/2012 da Direção Geral do Consumidor de 29/05/2012, *Projeto de proposta de Lei de alteração à Lei n.º 41/2004, de 18 de agosto, para transposição da Diretiva n.º 2009/136/CE, de 25/11*. Disponível em http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626d6c7561574e7059585270646d467a4c31684a535339305a58683062334d76634842734e7a677457 56c4a587a55755a47396a&fich=ppl78-XII_5.doc&Inline=true.

[106] *Cookies* correspondem a pequenos ficheiros trocados entre o navegador e o servidor de páginas, disponibilizados por este, que visam essencialmente influenciar as preferências dos utilizadores.

[107] Art. 5º da Lei n.º 46/2012. Após o aparecimento dúvidas decorrentes da transposição da Diretiva 2009/136/CE quanto ao tipo de consentimento a prestar, o Grupo de Trabalho do Artigo 29º emitiu um parecer,

vigente consagrou o princípio da livre utilização das redes de comunicações eletrónicas para o armazenamento de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador, se estes fossem claramente informados sobre as finalidades do processamento[108]. Todavia, o processo em apreço não carecerá de consentimento prévio do titular dos dados pessoais caso o armazenamento técnico ou o acesso cumpra os dois requisitos cumulativos na lei, i.e., se tiver como finalidade única a transmissão de uma comunicação através de uma rede de comunicações eletrónicas e seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade de informação solicitado expressamente pelo assinante ou utilizador.

Esta é, indubitavelmente, uma medida de incontornável impacto para as empresas prestadoras de serviços no setor, sobretudo no mercado da publicidade *online*, pois configura um obstáculo à angariação de potenciais clientes, uma vez que a livre utilização de *cookies* permitia a qualquer entidade armazenar dados relativos às preferências dos assinantes ou utilizadores, possibilitando a criação de um "perfil de cada consumidor", essencial para adaptar a publicidade enviada ao utilizador/assinante aos seus interesses, tacitamente revelados pela opções que faz e pelos sites que procura sempre que navega na rede "internet". Esta posição foi de igual modo defendida pela empresa, na altura, Optimus, S.A., a qual alegou que as mudanças no regime acime referidas "têm um impacto negativo muito significativo na sua relação com os seus clientes", defendendo que a obtenção do consentimento por escrito do utilizador ou assinante é "absolutamente inexequível", uma vez que o operador raramente dispõe de dado de contacto e, por vezes, nem sequer conhece o nome do cliente[109].

Todavia, acreditamos que corresponde a uma medida de necessária implementação no nosso ordenamento, já que a publicidade disponível nos serviços das comunicações

---

de 3 de outubro de 2013, no qual delineou que aquele deve corresponder a um comportamento ativo ou a uma ação dos utilizadores e tem de ser obtido previamente ao armazenamento de cookies no aparelho do utilizador. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

[108] Vigorou o regime de *opt out*, sendo dada aos utilizadores ou assinantes a possibilidade e recusarem o processamento *sub judice*.

[109] *Comentários da Optimus – Comunicações, S.A. às alterações do regime de comunicações não solicitadas constantes da Proposta de Lei sobre o tratamento de dados pessoais e proteção de privacidade no setor das comunicações eletrónicas, que transpõe a Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro.* Disponível em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626d6c7561574e7059585270646d467a4c31684a535339305a58683062334d76634842734e7a677457 56c4a587a63756347526d&fich=ppl78-XII_7.pdf&Inline=true

eletrónicas, nomeadamente na Internet, para além de despoletar novos interesses nos utilizadores, também acarreta riscos acrescidos sobre a proteção dos dados pessoais e respetiva privacidade dos assinantes ou utilizadores dos serviços[110].

Por fim, estas entidades, ANACOM e CNPD, perante o regime estabelecido na lei anterior, passaram a beneficiar de novos poderes, nas respetivas áreas de competência, ao abrigo do disposto nos artigos 13.º-C e seguintes, sendo-lhes agora admitida, designadamente, a cooperação transfronteiriça e a aprovação de medidas para assegurar essa cooperação, a elaboração de regulamentos relativos às práticas a adotar para cumprimento da lei em estudo, a emissão de ordens e de recomendações, a publicação, nos respetivos *websites*, dos códigos de conduta de que tenham conhecimento, bem como outras informações que considerem relevantes, e a fiscalização do cumprimento dos deveres e obrigações consagrados na Lei n.º 46/2012, por via "dos vogais e técnicos devidamente mandatados pela CNPD, nos termos da Lei de Proteção de Dados Pessoais e dos agentes de fiscalização ou de mandatários devidamente credenciados pelo ICP-ANACOM, nos termos do artigo 112.º da Lei das Comunicações Eletrónicas. dos funcionários de cada uma das entidades, devidamente mandatados/credenciados para o efeito"[111].

Na verdade, entendemos que a lei consagra um regime multidisciplinar pela atribuição de competências às duas entidades, de forma estanque, sem subsistirem, até ao presente, casos de *overlapping* de competências destas duas entidades.

Importa, porém, referir que o envio de mensagens através dos serviços de comunicações eletrónicas que contenham dados pessoais, traduz-se numa responsabilidade bipartida pelos dados gerados na transmissão eletrónica. Por um lado, em relação aos dados pessoais incluídos na mensagem, a responsabilidade pela proteção dos mesmos cabe àquele que emite a mensagem. Por outro lado, pelos dados suplementares essenciais ao funcionamento do serviço, a responsabilidade pelos mesmos recai sobre aquele que propõe o serviço de emissão[112].

[110] Neste sentido, MIRA BURRI NENOVA, *EC Electronic Communications and Competition Law*, Cameron May, 2007 , pág. 88.
[111] Art. 13º-G da Lei n.º 46/2012.
[112] Vide Considerando 47 da Diretiva 95/46/CE.

IV.3. O caso dos *data breaches*

Dado o crescente desenvolvimento da tecnologia e a proporcional necessidade de proteção dos utilizadores, urge estabelecer procedimentos em caso de violação da segurança.

Prescreve o artigo 2.º, alínea i), da Diretiva 2002/58/CE como violação de dados pessoais a "violação da segurança que provoca, de modo acidental ou ilegal, a destruição, a perda, a alteração, a divulgação ou acesso não autorizados a dados pessoais transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público na Comunidade»[113]. Comummente designada por *data breaches* é, nas palavras da Information Commissioner's Office resumidamente definida pela como "*an incident which affected the availability, integrity or confidentiality of the personal data*"[114].

De forma a acautelar o direito à privacidade dos indivíduos, o artigo 4º, nº 3 da Diretiva 2002/58/CE impõe aos operadores a obrigação de comunicar à autoridade nacional competente todos os casos de violação de dados pessoais, no caso de Portugal, à Comissão Nacional de Proteção de Dados, e, caso a violação de dados pessoais seja suscetível de afetar negativamente os dados pessoais ou a privacidade do titular dos dados, o responsável pelo tratamento deverá igualmente notifica-lo. Por sua vez, estas notificações aos assinantes ou utilizadores, enquanto titulares dos direitos afetados, devem der efetuadas sem demora injustificada, quando seja provável que venham a repercussões sobre os dados pessoais e eventuais efeitos adversos sobre o indivíduo.

É neste sentido que surge o Regulamento (UE) n.º 611/2013 da Comissão relativo às medidas aplicáveis à notificação da violação de dados pessoais, em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho relativa à privacidade e às comunicações eletrónicas, cujo principal objetivo foi especificar algumas obrigações consagradas na Diretiva da Privacidade e Comunicações Eletrónicas[115], e bem assim uniformizar, a nível europeu, os procedimentos associados à notificação *data breaches*.

[113] A Lei n.º 46/2012 transpôs definição nos mesmos termos artigo. 2º, n.1, al. g).
[114] Information Commissioner's Office, *Notification of PECR security breaches, Privacy and Electronic Communications Regulations*. Disponível em: https://ico.org.uk/media/for-organisations/documents/1583/notification-of-pecr-security-breaches.pdf
[115] Diretiva 2009/136/CE, transposta para o direito nacional através da já referida Lei n.º 46/2012, de 29 de agosto.

Para tal, o diploma criou um regime de notificação dos casos de violação de dados pessoais à autoridade nacional competente, que compreende, se preenchidas determinadas condições, várias fases, cada uma delas submetida a um determinado prazo. O procedimento consagrado visa assegurar que a autoridade nacional competente é informada no imediato e de forma tão circunstanciada quanto possível sem, no entanto, dificultar indevidamente os esforços do operador para investigar a violação e tomar as medidas necessárias para a confinar e para obviar às suas consequências.

No âmbito das notificações, a par dos assinantes ou utilizadores, enquanto pessoas titulares de dados pessoais afetados, tanto a CNPD como a ANACOM deverão ser devidamente notificadas em caso de *data breaches*. Relativamente às notificações efetuadas às referidas autoridades nacionais competentes, a notificação deve cumprir certos requisitos e incluir as informações constantes do Anexo I[116], respeitantes não só à própria violação de dados pessoais como também ao operador responsável pelo processamento, descrevendo, designadamente, o resumo do incidente que deu origem à violação de dados pessoais, eventuais consequências da violação de dados pessoais e medidas propostas ou tomadas pelo prestador para fazer face à violação. Embora sem previsão no ordenamento jurídico português, de acordo com o Regulamento, o operador dispõe de um prazo de 24 horas após a deteção dessa violação para a notificar à autoridade nacional competente, se possível. Porém, caso as referidas informações não estejam disponíveis e seja necessário realizar uma investigação suplementar da violação de dados pessoais, o operador deve poder proceder a uma primeira notificação à autoridade nacional dentro daquele prazo. Por conseguinte, deverá ser efetuada a segunda notificação à autoridade nacional competente assim que possível, dispondo de três dias contados a partir da primeira notificação[117]. Embora entendamos que a análise do caso da violação exija um trabalho de investigação detalhado e aprofundado por parte das empresas prestadoras de serviço no setor, carecendo, muitas vezes, de um período superior a três dias, concordados com a pronúncia da ICO, a qual defende que os operadores devem agir "*to prioritise the investigation, to give it adequate resources, and expedite it as a*

[116] *Ex vi* art. 2º, n.º 2 segundo parágrafo do Regulamento (UE) n.º 611/2013.
[117] Na primeira notificação incluir os elementos constantes na secção 1 do Anexo I, pelo que a segunda notificação deve ser composta pelos elementos enumerados na secção 2 do anexo I e, se necessário, atualizar as informações já fornecidas.

matter of urgency", concluindo que, em princípio, o procedimento tradicionalmente não deverá ultrapassar duas semanas[118].

Por outro lado, os operadores estão obrigados a prestar informação aos assinantes, nos termos do artigo 47º-A da LCE, e a notificar a ANACOM das violações de segurança ou das perdas de integridade com impacto significativo no funcionamento das redes e serviços (art. 54.º-B). Estas medidas, introduzidas pela Lei n.º 51/2011, de 13 de setembro, resultado da transposição da Diretiva 2009/140/CE, permitem à ANACOM impor aos operadores a obrigação de prestação de informações adicionais aos assinantes, incluindo sobre medidas de gestão de tráfego que possam ter repercussões na qualidade de serviço.

Ademais, a lei faz ainda referência aos casos em que os dados ou a privacidade do assinante são afetados "negativamente". Uma vez que a Diretiva 2009/136/CE no artigo 4.º, n.º 3, não estabelece nenhuma escala ou critérios objetivos para avaliar o grau de gravidade da violação, nem define quaisquer limites que poderiam eventualmente ser tidos em consideração para apurar a necessidade de o prestador notificar os utilizadores, o Grupo de Trabalho do Artigo 29º identificou a necessidade de estabelecer uma metodologia de avaliação da gravidade universal e de fácil compreensão não só para as empresas que oferecem serviços de comunicações eletrónicas, como também para as autoridades competentes na Europa[119]. Na realidade, a perceção na avaliação da gravidade da situação quer da autoridade quer do operador deve ser semelhante, tal como ocorre noutros países a nível Europeu, de modo a evitar disparidades na aplicação da própria Diretiva. É nesse sentido que o Grupo de Trabalho, em cooperação com a *European Union Agency for Network and Information Security* (ENISA), propõe uma metodologia baseada numa escala de gravidade do efeitos negativos decorrentes violação de dados pessoais ou da privacidade, servindo-se de critérios auxiliares na determinação do grau da gravidade, dos resultados obtidos e o fundamento desta avaliação. Em termos gerais, o raciocínio apresentado faculta uma escala de gravidade que toma em consideração o impacto da violação sobre as pessoas,

[118] Notification of PECR security breaches, Privacy and Electronic Communications Regulations, ICO. Disponível em: https://ico.org.uk/media/for-organisations/documents/1583/notification-of-pecr-security-breaches.pdf

[119] Parecer 06/2012 sobre o projeto de decisão da Comissão relativa às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE relativa à privacidade e às comunicações eletrónicas1, aprovado a 12 de julho de 2012 do GRUPO DE TRABALHO DO ARTIGO 29º PARA A PROTEÇÃO DE DADOS, nº WP 197. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp197_en.pdf

os esforços necessários para a identificação dos indivíduos a partir dos dados e o nível de exposição dos dados que dizem respeito à violação.

Contudo, à semelhança das obrigações previstas na Diretiva 2002/58/CE, o Regulamento n.º 611/2013 retira a obrigação de notificação às pessoas em causa caso os dados tenham sido tornados ininteligíveis. Se a autoridade competente considerar que o operador demonstrou satisfatoriamente ter aplicado medidas tecnológicas de proteção[120] adequadas à de modo a tornar os dados ininteligíveis[121] para qualquer pessoa que não esteja autorizada a aceder-lhes, e se essas medidas tiverem sido aplicadas aos dados afetados, não se exige a notificação ao titular dos dados em causa[122].

[120] Estas medidas são essencialmente baseadas nas recomendações da ENISA, as quais sublinham que, para que os dados sejam considerados ininteligíveis, devem ser submetidos a um mecanismo de cifragem, uma função *hash* codificada ou uma exclusão irreversível. Ver GRUPO DE TRABALHO DO ARTIGO 29º PARA A PROTEÇÃO DE DADOS, Parecer 08/2012, (…) *cit.* Pág. 10.

[121] O Regulamento no art. 4º n.º 2 exemplifica alguns dos meios para tornar os dados ininteligíveis.

[122] Art. 4.º, n.º 3, da Diretiva 2002/58/CE; artigo 4.º, n.º 1, do Regulamento 611/2013; artigo 3.º-A, n.º 4 da Lei n.º 41/2004.

V. CONCLUSÃO

A importância da proteção dos dados pessoais surgiu desde cedo. Contudo, o crescente e incentivado desenvolvimento tecnológico despoletou a necessidade de readaptar as obrigações impostas aos operadores que oferecem serviços no setor das comunicações eletrónicas.

Percebemos como evoluiu o direito à privacidade e contatámos que o avanço tecnológico teve um impacto indubitável nesse percurso. Se, por um lado, o progresso das tecnologia facilitou as comunicações, por outro lado, permitiu maior intromissão e consequente invasão de privacidade dos cidadãos.

Tem sido essencial apostar no ajuste legislativo, de forma a acompanhar a sofisticação terminológica e acautelar as diversas contingências tecnológicas. Concomitantemente, é fundamental garantir transparência aos utilizadores e assegurar medidas que os protejam dos riscos inerentes à utilização das comunicações eletrónicas. A vasta legislação analisada no presente estudo espelha o resultado dos vários desafios colocados pelas novas ameaças à privacidade dos titulares dos dados pessoais face ao novo paradigma social.

Certo é que "*If we continue to develop our technology without wisdom or prudence, our servant may prove to be our executioner*[123]". Na verdade, não obstante a imposição de regulação específica ao setor, urge preservar e cultivar valores como a proteção da privacidade e da confidencialidade, sob pena de transitarem para um segundo plano.

Da leitura do regime regulamentar edificado pelo nosso ordenamento jurídico, coordenado com as funções desempenhadas pela CNPD, quanto à própria proteção de dados pessoais, e pela ANACOM, quanto ao setor das comunicações eletrónicas, parece-nos evidente que a Lei da Proteção de Dados Pessoais e Privacidade nas Telecomunicações reflete a importância adaptar as atribuições destas duas entidades à realidade atual, sem, contudo, sobrepor as responsabilidades assumidas por cada uma delas.

Por fim, cumpre referir que a proteção será sempre um trabalho imperfeito, o qual envolve não só os operadores mas todos os *players* da cadeia de valor.

[123] GENERAL OMAR NELSON BRADLEY, durante o discurso apresentado no dia da Aministia Internacional, em 11 de novembro de 1948.

BIBLIOGRAFIA

V.1. Doutrina

- AMARAL, Freitas, *Curso de Direito Administrativo*, 3ª edição, vol. I, Lisboa, Almedina, 2006
- CANOTILHO, Gomes; MOREIRA, Vital, *A Constituição da República Portuguesa Anotada*, Vol. I, 4ª Edição, Coimbra, Coimbra Editora, 2007.
- CARDOSO, José Lucas, *Autoridades Administrativas Independentes e Constituição*, Coimbra, Coimbra Editora, Outubro de 2002.
- CASTRO, Catarina Sarmento, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra, Almedina, 2005.
- CASTRO, Catarina Sarmento, "Privacidade e Protecção de dados pessoais em rede", *in Direito da Informação*, Vol. VII, Coimbra, Coimbra Editora, 2008.
- COELHO, José Dias (coord.), *Sociedade da informação – O percurso português*, Lisboa, Edições Sílabo, 2007.
- CONFRARIA, João, *Regulação e Concorrência, Desafios do século XXI*, Universidade Católica Editora, Lisboa 2011, 2ª Edição Revista e Actualizada.
- DONEDA, Danilo, *Da Privacidade à Proteção de Dados Pessoais*, Rio de Janeiro, Renovar, 2006.
- FERREIRA, Pedro, *A Proteção de Dados Pessoais na Sociedade de Comunicação - Dados de Tráfego, Dados de Localização e Testemunhos de Conexão*, Lisboa, O Espírito das Leis, 2006.
- GONÇALVES, José Renato, "Regime dos 'Dados Pessoais' Informatizados", *in Scientia Iuridica*, n.º 292 Braga, 2002.
- GONÇALVES, Pedro Costa, *Reflexões sobre o Estado Regulador e o Estado Contratante*, Direito Público e Regulação 8, Coimbra, Coimbra Editora, 2013.
- GUERRA, Amadeu, "Lei de Proteção de Dados Pessoais", *in Direito da Sociedade de Informação*, Vol. 2, Faculdade de Direito de Lisboa, Coimbra, Coimbra Editora, 2001.
- GUERRA, Amadeu, "El tratamento de datos personales para fines de prevención e investigación criminal. El tratamento de datos por parte de las autoridades policiales

de Portugal", *in Revista espanhola Protección de Datos,* N. 7 (Julio 2009 - Junio 2010).

- LOPES, J. de Seabra Lopes, "A Protecção da Privacidade e dos dados pessoais na sociedade da informação: tendências e desafios numa sociedade em transição", in *Estudos dedicados ao Prof. Doutor Mário Júlio Brito de Almeida Costa*, Universidade Católica Editora, Lisboa, 2002.
- MARQUES, Maria Manuel Leitão, MOREIRA, Vital, *A mão visível: mercado e regulação,* Coimbra, Almedina, 2003.
- MARQUES, Maria Manuel Leitão, ALMEIDA, João Paulo Simões, FORTE, André Matos, *Concorrência e regulação: a relação entre a Autoridade da Concorrência e as Autoridades de Regulação Sectorial,* Coimbra, Coimbra Editora
- MARQUES, Maria Manuel Leitão, SANTOS, António Carlos, GONÇALVES, Maria Eduarda, *Direito Económico,* Almedina, 2014
- MONTEIRO, António Pinto, *As Telecomunicações e o Direito na Sociedade da Informação – Actas do Colóquio organizado pelo IJC em 23 e 24 de Abril de 1998,* Coimbra, Instituto Jurídico da Comunicação, 1999.
- MOREIRA, Vital (coord.), *Estudos de regulação pública I,* Coimbra, Coimbra Editora, 2004.
- MOREIRA, Vital , MAÇÃS, Fernanda, *Autoridades Reguladoras Independentes - Estudo e Projecto de Lei-Quadro*, Coimbra, Coimbra Editora, 2003
- NENOVA, Mira Burri, *EC Electronic Communications and Competition Law*, Cameron May, 2007.
- NEVES, Rita Castanheira, *As ingerências nas comunicações electrónicas em processo penal: natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova,* Coimbra, Coimbra Editora, 2011.
- OTERO, Paulo, GONÇALVES, Pedro Costa, *Tratado de Direito Administrativo Especial,* Vol V, Coimbra, Almedina, 2011.
- ROQUE, Ana (coord.), *Regulação do mercado: novas .tendências*, Lisboa, Quid Juris?, 2004.
- RUARO, Regina Linden, RODRIGUEZ, Daniel Piñeiro, FINGER, Brunize " O Direito à Proteção de Dados Pessoais e a privacidade", *in Revista da Faculdade de Direito da Universidade Federal do Paraná*, Curitiba, n.53, 2011

- PAZ FERREIRA, Eduardo, MORAIS, Luís, ANASTÁCIO, Gonçalo, *Regulação em Portugal: novos tempos, novo modelo?*, Coimbra, Almedina, 2009.
- PAZ FERREIRA, Eduardo, "Em torno da regulação económica em tempos de mudança", *in Revista de Concorrência e Regulação*, ano I, número 1, Lisboa, Almedina, 2010.
- SILVEIRA, Luís Lingnau, "Configuração Constitucional da Protecção de Dados" in *Em homenagem ao Prof. Doutor Diogo Freitas do Amaral*, Coimbra, Almedina, 2010.
- TEIXEIRA, Glória, GUIMARÃES, Maria Raquel, *Direito e (tele)comunicações*, Coimbra, Coimbra Editora, 2008.
- VAZ, Ana, "Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais*", in Noção e Defesa*, Verão 2007, N.º 117 - 3.ª Série
- VIEIRA, Tatiana Malta, *O Direito à Privacidade na Sociedade da Informação – Efetividade desse direito fundamental diante dos avanços da tecnologia da informação*, Porto Alegre, Sergio Antonio Fabris Editor, 2007

V.2. Legislação

- Lei n.º 88/89, de 11 de setembro (define a Lei de Bases do Estabelecimento, Gestão e Exploração das Infraestruturas e Serviços de Telecomunicações)
- Lei n.º 91/97, de 1 de agosto (define as bases gerais a que obedece o Estabelecimento, gestão e exploração de redes de telecomunicações e a prestação de serviços de telecomunicações)
- Lei n.º 67/98, de 26 de outubro, (Lei da Proteção de Dados Pessoais)
- Lei n.º 69/98, de 28 de outubro (regula o tratamento dos dados pessoais e a proteção da privacidade no sector das telecomunicações, revogada pela Lei n.º 41/2004)
- Lei 5/2004, de 10 de fevereiro (Lei das Comunicações Eletrónicas)
- Lei n.º 41/2004, de 18 de agosto (relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas)
- Lei n.º 46/2012, de 29 de agosto (transpõe a Diretiva n.º 2009/136/CE e altera a Lei n.º 41/2004)
- Decreto-Lei 188/81, de 2 de julho (criou o ICP)
- Decreto-Lei n.º 283/89, de 23 de agosto (aprova os antigos estatutos do ICP)

- Decreto-Lei n.º 415/98, de 31 de dezembro (estabelece o regime da interligação entre redes públicas de telecomunicações e define os princípios gerais a que deve obedecer o Plano Nacional de Numeração)
- Decreto-Lei n.º 309/2001, de 7 de dezembro (aprova os Estatutos do (ICP-ANACOM)
- Decreto-Lei n.º 39/2015, de 16 de março (aprova atuais estatutos da ANACOM)
- Diretiva 95/46/CE, de 24 de outubro (relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados)
- Diretiva 2002/12/CE, de 5 de março de 2002 (relativamente aos requisitos em matéria de margem de solvência aplicáveis às empresas de seguro de vida)
- Diretiva 2002/20/CE, de 7 de março (relativa à autorização de redes e serviços de comunicações eletrónicas)
- Diretiva 2002/19/CE, de 7 de março (relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos)
- Diretiva 2002/22/CE, de 7 de março (relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas)
- Diretiva 2002/58/CE, de 12 de julho (relativa à privacidade e às comunicações eletrónicas)
- Diretiva 2006/24/CE, de 15 de março (relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE)
- Diretiva 2009/140/CE, de 25 de novembro de 2009 (altera a Diretiva 2002/21/CE relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, a Diretiva 2002/19/CE relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos e a Diretiva 2002/20/CE relativa à autorização de redes e serviços de comunicações eletrónicas)
- Diretiva 2009/136/CE, de 25 de novembro (que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n.o2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor)
- Constituição da República Portuguesa

- Regulamento (UE) n.º 611/2013 (relativo às medidas aplicáveis à notificação da violação de dados pessoais no âmbito da Diretiva relativa à privacidade e às comunicações eletrónicas)

V.3. Outros

- Evolução da Companhia Portuguesa Rádio Marcon: http://sitiomarconi.fundacao.telecom.pt/Default.aspx?tabid=270
- Acordo de Cooperação entre a ANACOM e a Autoridade da Concorrência: http://www.anacom.pt/render.jsp?contentId=132089#.VhwyFG5wRt2
- Parecer 08/2012 do GT: Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_pt.pdf
- Recomendação de 12 de maio de 2010, relativa à utilização de uma metodologia harmonizada para classificar e comunicar queixas e pedidos de informação dos consumidores (2010/304/EU). Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32010H0304&from=EN
- Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados, Documento de trabalho sobre questões relativas à proteção de dados no âmbito da tecnologia RFID (WP 105), adotado em 19 de janeiro de 2005, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf
- Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados, *Parecer 8/2006 sobre a revisão do quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, com destaque para a Diretiva relativa à privacidade e às comunicações eletrónicas* (WP 126), de 26 de Setembro de 2006, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp126_pt.pdf
- Grupo de Trabalho do Artigo 29.º Para A Proteção Dos Dados, *Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde electrónicos (RSE)* (WP 131), de 15 de fevereiro de 2007, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_pt.pdf

- Grupo de Trabalho do Artigo 29.º Para A Proteção Dos Dados, *Parecer 4/2007 sobre o conceito de dados pessoais* (WP 136), de 20 de junho de 2007., disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pt.pdf
- Grupo de Trabalho do Artigo 29.º Para A Proteção Dos Dados, *Parecer 1/2008 sobre questões de proteção de dados ligadas aos motores de pesquisa* (WP 148), de 4 de Abril de 2008, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_pt.pdf#h2-6
- Grupo de Trabalho do Artigo 29.º Para A Proteção Dos Dados, *Parecer 2/2008 sobre a revisão da Diretiva 2002/58/CE relativa à privacidade no sector das comunicações eletrónicas (Diretiva Privacidade Eletrónica)* (WP 150), de 15 de maio de 2008, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_pt.pdf
- Grupo de Trabalho do Artigo 29.º Para A Proteção Dos Dados, *Parecer 1/2009 sobre as propostas de alteração da Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (diretiva da privacidade eletrónica)* (WP 159), de 10 de fevereiro de 2009, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_pt.pdf
- Pareceres (33) e (34) da CNPD, disponíveis em: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=37091
- Parecer 4/2012 da Direção Geral do Consumidor de 29/05/2012, *Projeto de proposta de Lei de alteração à Lei n.º 41/2004, de 18 de agosto, para transposição da Diretiva n.º 2009/136/CE, de 25/11*. Disponível em http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626d6c7561574e7059585270646d467a4c31684a535339305a58683062334d76634842734e7a677457456c4a587a55755a47396a&fich=ppl78-XII_5.doc&Inline=true.
- *Comentários da Optimus – Comunicações, S.A. às alterações do regime de comunicações não solicitadas constantes da Proposta de Lei sobre o tratamento de dados pessoais e proteção de privacidade no setor das comunicações eletrónicas, que transpõe a Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro.* Disponível em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626d6c7561574e7059585270646d467a4c31684a535339305a58683062334d76634842734e7a677457456c4a587a63756347526d&fich=ppl78-XII_7.pdf&Inline=true

- Information Commissioner's Office, *Notification of PECR security breaches, Privacy and Electronic Communications Regulations.* Disponível em: https://ico.org.uk/media/for-organisations/documents/1583/notification-of-pecr-security-breaches.pdf

- Information Commissioner's Office, *Determining what is personal data – Data Protection Act.* Disponível em: https://ico.org.uk/media/1554/determining-what-is-personal-data.pdf

- Deliberação n.º 7680/ 2014 da CNPD aplicável aos tratamentos de dados pessoais decorrentes da utilização de tecnologias de geolocalização no contexto laboral. Disponível em: http://www.cnpd.pt/bin/orientacoes/DEL_7680-2014_GEO_LABORAL.pdf

- Deliberação n.º 629/2010 da CNPD sobre os Princípios aplicáveis ao tratamento de dados de gravação de chamadas. Disponível em: http://www.cnpd.pt/bin/orientacoes/DEL629_2010.pdf