Moreira, Ângela Maria de Sousa, 1982-

O regime jurídico de proteção de dados pessoais na esfera da Administração Pública : implementação e compliance na gestão dos dados pessoais

http://hdl.handle.net/11067/7570

Metadados

Data de Publicação 2024

Resumo A permanente evolução tecnológica e o incremento exponencial do tratamento automatizado de dados pessoais comportam riscos para os direitos e liberdades das pessoas singulares. Decorrente da gradual consciencialização desse facto, na Europa, a proteção de dados pessoais passou a ser considerada como um instrumento essencial para a proteção da pessoa humana e um direito fundamental. O presente estudo centra-se na análise do regime jurídico da proteção de dados e da sua aplicação na Administração...

Permanent technological evolution and the exponential increase in the automated processing of personal data imply risks to the rights and freedoms of natural persons. As a result of the gradual awareness of this fact, in Europe, the protection of personal data has come to be considered as an essential instrument for the protection of the human person and a fundamental right. This study focuses on the analysis of the legal regime for data protection and is application in Public Administration. T...

Palavras Chave Proteção de dados - Direito e legislação, Proteção de dados - Direito e legislação - Portugal, Direito à Privacidade, Direito à privacidade - - Portugal, Administração pública - Processamento de dados - Portugal

Tipo masterThesis

Revisão de Pares Não

Coleções [ULL-FD] Dissertações

UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

O regime jurídico de proteção de dados pessoais na esfera da Administração Pública: implementação e *compliance* na gestão dos dados pessoais

Realizado por:
Ângela Maria de Sousa Moreira

Orientado por:
Prof. Doutor Lourenço da Bandeira Manoel de Vilhena de Freitas

Constituição do Júri:

Presidente:	Prof. Doutor José Alberto Rodríguez Lorenzo González
Orientador:	Prof. Doutor Lourenço da Bandeira Manoel de Vilhena de Freitas
Arguente:	Prof. Doutor Luís Manuel Barbosa Rodrigues

Dissertação aprovada em: 15 de julho de 2024

Lisboa

2024

UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

O regime jurídico de proteção de dados pessoais na esfera da Administração Pública: implementação e *compliance* na gestão dos dados pessoais

Ângela Maria de Sousa Moreira

Lisboa

Janeiro 2024

UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

O regime jurídico de proteção de dados pessoais na esfera da Administração Pública: implementação e *compliance* na gestão dos dados pessoais

Ângela Maria de Sousa Moreira

Lisboa

Janeiro 2024

Ângela Maria de Sousa Moreira

O regime jurídico de proteção de dados pessoais na esfera da Administração Pública: implementação e *compliance* na gestão dos dados pessoais

Dissertação apresentada à Faculdade de Direito da Universidade Lusíada para a obtenção do grau de Mestre em Direito.

Área científica: Ciências Jurídico-Empresariais

Orientador: Prof. Doutor Lourenço da Bandeira Manoel de Vilhena de Freitas

Lisboa

Janeiro 2024

FICHA TÉCNICA

Autora Ângela Maria de Sousa Moreira

Orientador Prof. Doutor Lourenço da Bandeira Manoel de Vilhena de Freitas

Título O regime jurídico de proteção de dados pessoais na esfera da administração pública: implementação e *compliance* na gestão dos dados pessoais

Local Lisboa

Ano 2024

CASA DO CONHECIMENTO DA UNIVERSIDADE LUSÍADA - CATALOGAÇÃO NA PUBLICAÇÃO

MOREIRA, Ângela Maria de Sousa, 1982-

O regime jurídico de proteção de dados pessoais na esfera da administração pública: implementação e *compliance* na gestão dos dados pessoais / Ângela Maria de Sousa Moreira ; orientado por Lourenço da Bandeira Manoel de Vilhena de Freitas. - Lisboa : [s.n.], 2023. - Dissertação de Mestrado em Direito, Faculdade de Direito da Universidade Lusíada.

I - FREITAS, Lourenço Vilhena de, 1973-

LCSH
1. Proteção de dados - Direito e legislação
2. Proteção de dados - Direito e legislação - Portugal
3. Direito à privacidade
4. Direito à privacidade - Portugal
5. Administração pública - Processamento de dados - Portugal
6. Universidade Lusíada. Faculdade de Direito - Teses
7. Teses - Portugal - Lisboa

1. Data protection - Law and legislation
2. Data protection - Law and legislation - Portugal
3. Privacy, right of
4. Privacy, right of - Portugal
5. Public administration - Data Processing - Portugal
6. Universidade Lusíada. Faculdade de Direito - Dissertations
7. Dissertations, academic - Portugal - Lisbon

LCC
1. KKQ844.5.M67 2024

APRESENTAÇÃO

O regime jurídico de proteção de dados pessoais na esfera da Administração Pública: implementação e *compliance* na gestão dos dados pessoais

Ângela Maria de Sousa Moreira

A permanente evolução tecnológica e o incremento exponencial do tratamento automatizado de dados pessoais comportam riscos para os direitos e liberdades das pessoas singulares. Decorrente da gradual consciencialização desse facto, na Europa, a proteção de dados pessoais passou a ser considerada como um instrumento essencial para a proteção da pessoa humana e um direito fundamental.

O presente estudo centra-se na análise do regime jurídico da proteção de dados e da sua aplicação na Administração Pública. Para tal, procede-se ao estudo da evolução histórico-legislativa da noção de privacidade até ao momento em que atinge o *status* de direito fundamental e ao exame dos principais princípios e disposições relevantes do regime jurídico vigente nesta matéria. Adicionalmente, analisam-se os deveres dos responsáveis pelo tratamento dos dados pessoais no setor público e as principais medidas que estes devem implementar para garantir a segurança dos dados pessoais tratados.

Palavras-chave: Privacidade; dados pessoais; RGPD; Administração Pública, responsabilidade; conformidade.

PRESENTATION

The legal regime for the protection of personal data in the sphere of Public Administration:

implementation and compliance in personal data management

Ângela Maria de Sousa Moreira

Permanent technological evolution and the exponential increase in the automated processing of personal data imply risks to the rights and freedoms of natural persons. As a result of the gradual awareness of this fact, in Europe, the protection of personal data has come to be considered as an essential instrument for the protection of the human person and a fundamental right.

This study focuses on the analysis of the legal regime for data protection and is application in Public Administration. To this end, we study the historical-legislative evolution of the notion of privacy until the moment it reaches the status of fundamental right and examine the main principles and relevant provisions of the legal regime in force in this matter. Additionally, the duties of those responsible for processing data in the public sector are analyzed and the main measures that they must implement to guarantee the security of the personal data processed.

Keywords: Privacy; personal data; GDPR; Public Administration, responsibility; compliance.

LISTA DE TABELAS

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

AIPD – Avaliação de Impacto sobre a Proteção de Dados;

AP – Administração Pública;

Art.º – Artigo;

CC – Código Civil;

CEDH – Convenção Europeia dos Direitos do Homem;

CEPD - Comité Europeu para a Proteção de Dados;

CNPD – Comissão Nacional de Proteção de Dados;

CPA – Código do Procedimento Administrativo;

CRP – Constituição da República Portuguesa;

DUDH – Declaração Universal dos Direitos Humanos;

ELSJ - Espaço de Liberdade, de Segurança e de Justiça;

EPD/DPO – Encarregado de Proteção de Dados / *Data Protection Officer*;

ETS - *European Treaty Series*

EUA – Estados Unidos da América;

GNS – Gabinete Nacional de Segurança;

GT 29 – Grupo de Trabalho do Artigo 29.º para a Proteção de Dados;

I.e. - *Id est;*

ISO/IEC – *International Organization of Standardization* **/** *International Electrotechnical Commission*;

LE – Lei de Execução Nacional do RGPD (Lei n.º 58/2019, de 8 de agosto);

NATO - *North Atlantic Treaty Organization*;

OCDE - Organização para a Cooperação e Desenvolvimento Económico

P. – Página

PP. – Páginas

RCM – Resolução do Conselho de Ministros;

RRCEE - Regime da Responsabilidade Civil Extracontratual do Estado e Pessoas Coletivas de Direito Público;

RGPD – Regulamento Geral sobre a Proteção de Dados (Regulamento (EU) 2016/679, de 27 de abril de 2016);

RT – Responsável pelo tratamento dos dados;

SGSI - Sistema de Gestão de Segurança da Informação;

STJ – Supremo Tribunal de Justiça

TEDH - Tribunal Europeu dos Direitos do Homem

TFUE – Tratado sobre o Funcionamento da União Europeia;

TJUE - Tribunal de Justiça da União Europeia;

TRL – Tribunal da Relação de Lisboa;

UE – União Europeia;

V.g. – *Verbi grata.*

SUMÁRIO

1. INTRODUÇÃO

Em 27 de abril de 2016 foi adotado, pela União Europeia, o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, que introduziu alterações significativas ao regime jurídico em matéria de proteção de dados pessoais, asseverando o direito fundamental à proteção de dados consagrado na Carta dos Direitos Fundamentais da União Europeia e nos Tratados europeus.

Com o desiderato de atualizar e harmonizar as regras de proteção de dados entre os Estados-Membros, a reforma assenta na pretensão de criar um mercado único, que assegure a livre circulação de pessoas, serviços e capitais, incluindo as atividades desenvolvidas na esfera digital, contribuindo para o seu desenvolvimento em condições de concorrência leal e um elevado nível de proteção dos consumidores e dos seus dados. O concernente quadro legal obriga todas as empresas e organizações da União Europeia que tratem dados pessoais, bem como as que, encontrando-se fora da EU, tratem dados de titulares residentes na Europa, desde que comercializem os seus produtos e/ou serviços ou monitorizem comportamentos que ocorram dentro da UE.

O reforço da proteção jurídica dos direitos dos titulares dos dados assenta, por seu turno, no estabelecimento de novas regras e procedimentos particularmente direcionados para os tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares. Concomitantemente, decorre dos princípios que regem o tratamento de dados pessoais, que o responsável pelo tratamento deve atuar de um modo lícito, leal e transparente para com o titular dos dados, adotando procedimentos que assegurem o exercício dos seus direitos. Nessa medida, o responsável pelo tratamento dos dados assume um papel fundamental na garantia da conformidade do tratamento dos dados.

A Administração Pública está sujeita às regras do RGPD sempre que efetue o tratamento de dados pessoais relacionados com um indivíduo. Sem prejuízo da transversalidade do regime, é no domínio do setor público que o presente estudo se centra, em particular, no que tange às responsabilidades dos serviços e organismos públicos no que respeita à adoção de medidas de *compliance* e às principais técnicas a adotar por estas entidades para garantir a segurança da informação pessoal objeto de tratamento.

Com efeito, o RGPD elenca apenas alguns exemplos de medidas técnicas e organizativas, não prevendo o emprego de qualquer metodologia específica ou normas de segurança vinculativas, que orientem as entidades no caminho da

conformidade legal. Os aspetos práticos da aplicação do RGPD nas organizações é um desafio para a maioria das entidades públicas porquanto acarreta a intersecção de conhecimentos de várias áreas científicas, aliada à capacidade de adotar uma metodologia de controlo interno que permita examinar todas as atividades de tratamento de dados, identificar vulnerabilidades e adotar procedimentos para dirimir os riscos e recuperar de eventuais incidentes de segurança.

Nesta conformidade, o presente trabalho possui como objetivo primordial a compreensão das efetivas responsabilidades dos principais intervenientes no processo de implementação do RGPD e aferição dos ajustes organizacionais tidos por necessários relativamente à generalidade das entidades públicas.

Este estudo adota a forma dissertativa expositiva e aplica um raciocínio dedutivo e indutivo, dividindo-se em três partes.

Na primeira parte, pretende-se efetuar a análise da evolução do direito à privacidade, que surge primitivamente associado a um invento tecnológico, tendo sido espalhado pela doutrina como um direito negativo, de não ingerência nos aspetos relacionados com a esfera da vida privada do indivíduo. Todavia, o contexto histórico de conflito mundial e o desenvolvimento tecnológico estimularam o processo de convergência do ordenamento em torno da pessoa, robustecendo a capacidade de processar dados informatizados e desencadeando inúmeros desafios para a privacidade, o que impôs uma redefinição da conceção deste direito. Assoma-se, neste quadro, o direito de cada indivíduo impedir a circulação de informações que dizem respeito a aspetos íntimos da sua vida privada. A designada «privacidade informacional» passa a constar dos textos constitucionais, enquanto direito fundamental, ancorada nos direitos à intimidade, vida privada, sigilo, imagem, honra, inviolabilidade da casa e inviolabilidade dos dados. Nesta sede, almeja-se ainda demonstrar que o percurso evolutivo da conceção do direito foi acompanhado por um avanço legislativo assente na garantia dos direitos e liberdades fundamentais e na criação de um mercado único de circulação de dados e capitais a nível europeu, refletido na necessidade de estabelecer uma harmonização legislativa, que se logrou alcançar com a publicação do RGPD.

Na segunda parte do estudo realizamos a análise dos aspetos essenciais do RGPD, nomeadamente o seu âmbito de aplicação, as noções de «dado pessoal» e «dados sensíveis», os princípios aplicáveis ao tratamento dos dados, bem como os direitos dos titulares. Faz-se, também, uma breve referência ao processo legislativo de aprovação da lei de execução nacional, com enfoque na decisão da CNPD de

desaplicação de algumas das suas normas, com fundamento na violação do RGPD. Neste capítulo, pretende-se evidenciar as normas que constituem o cerne conceptual nesta matéria e cujo teor reveste suma importância para a compreensão das demais disposições do Regulamento. Almeja-se, ainda, comprovar que a regulamentação vigente deve ser observada à luz da proteção dos direitos dos titulares dos dados e que os princípios consignados impõem um tratamento de dados baseado na adoção de medidas concretas que permitam efetivar o exercício desses direitos.

Na terceira parte alude-se primeiramente aos principais intervenientes do modelo de conformidade, partindo da noção e responsabilidades do «responsável pelo tratamento», bem como a análise do regime da responsabilidade civil extracontratual do estado e demais entidades públicas (RRCEE). Este estudo tem como finalidade demonstrar as responsabilidades que o RGPD atribui diretamente ao responsável pelo tratamento dos dados, bem como as que emergem para o Estado e seus representantes, no que tange aos danos causados ao titular dos dados, decorrentes do incumprimento das regras estabelecidas em matéria de proteção de dados. Ainda no mesmo capítulo afloram-se os conceitos de «subcontratante» e de «responsáveis conjuntos» e verifica-se a designação e funções do «encarregado da proteção de dados» (EPD/DPO) nas entidades públicas, enquanto figura interveniente e com responsabilidades pelo cumprimento dos desideratos em matéria de proteção de dados.

Por último, e ainda dentro da terceira parte, atendendo a que a segurança dos dados constitui uma das formas de assegurar o cumprimento dos princípios que regem o tratamento dos dados pessoais e de garantir o exercício dos direitos dos titulares, faz-se o enquadramento legal dos requisitos de segurança e uma incursão prática pelas medidas técnicas e organizativas a adotar pelos responsáveis pelo tratamento e pelos subcontratantes neste âmbito. A este respeito ambiciona-se evidenciar que de entre as obrigações que impendem sobre os responsáveis pelo tratamento de dados e subcontratantes, incluindo no setor público, acha-se a designada abordagem baseada no risco, calculada em função da probabilidade e impacto para os direitos e liberdades do titular dos dados. Por outro lado, atendendo a que o RGPD incentiva a adoção de políticas internas adequadas e a aplicação de medidas técnicas e organizativas, importa enumerar o conjunto de medidas recomendadas pela autoridade de controlo e outras entidades para acautelar a segurança dos dados pessoais, sem prejuízo do facto de as mesmas deverem ser determinadas em função dos factos e circunstâncias de cada situação concreta.

2. ANÁLISE SOBRE A EVOLUÇÃO HISTÓRICA E LEGISLATIVA DO DIREITO À PRIVACIDADE

2.1. DA GÉNESE E CONSTRUÇÃO DO "*RIGHT TO PRIVACY*" NOS EUA

A ideia de privacidade deriva primitivamente da síncrise entre o que deve permanecer reservado e o que deve ser levado ao conhecimento público[1] tendo, no decorrer do tempo, evidenciado diferentes contornos consoante o momento histórico-cultural apreciado e evoluído no sentido da distinção entre os aspetos da vida pessoal em oposição às questões inerentes à vida social ou comunitária. [2]

Trata-se de uma noção de difícil delimitação, em particular quando se procura definir o que deve ser mantido reservado ou escondido do conhecimento de terceiros, considerando cuidar-se de *"compreensões que se transformam em cada sociedade"* [3], abrangendo questões jurídicas, filosóficas e culturais, com enfoque nas divergências conceptuais norte americana e europeias disseminadas pela respetiva doutrina e jurisprudência. Enquanto a *privacy* norte americana foi construída em torno da liberdade, a europeia ancorou-se na dignidade humana. Nos EUA o direito edificou-se através da jurisprudência e na Europa tornou-se "*(…) um direito constitucionalmente reconhecido e protegido de tal modo que todos os interesses privados partilham um valor: o respeito pela dignidade do indivíduo, sua integridade e independência*". [4]

Nesta conformidade, para se compreender a génese do "*right to privacy*" enquanto figura jurídica autónoma**,** é necessário recuar ao final do século XVIII e observar os entendimentos doutrinários e jurisprudenciais manados no contexto da revolução liberal norte-americana, donde emerge a ideia de progresso baseado na liberdade do indivíduo face à autoridade do Estado e à ingerência do mesmo na esfera da vida privada das pessoas. Dá-se a fragmentação da sociedade feudal e a origem da sociedade urbana num emaranhado de relações sociais, acompanhado pela alteração

[1] Na Antiguidade Clássica, pese embora Aristóteles tenha distinguido os conceitos de esfera privada ("oikos") e esfera pública ("polis"), foram os romanos a conceber a expressão "*privatus*", cuja definição incluía as questões inerentes à família e aos aspetos económicos, por oposição às relações em comunidade e à vida do cidadão na cidade. Desta distinção sobressai, assim, a existência de informação que não constitui interesse para o domínio público. Neste sentido, *vd.* CORREIA, Victor - Sobre o direito à Privacidade [Em linha]. O Direito. Editora Almedina. Lisboa. Ano 146.º, N.º 1 (2014), p. 9. Disponível em: https://www.cidp.pt/revistas/direito/O%20Direito%20(2014)%20I%20TEXTO.PDF [acedido em 14.11.2022]

[2] PINTO, Paulo Mota - *Direitos de Personalidade e Direitos Fundamentais: estudos*. 1.ª Edição. Coimbra: Gestlegal, 2018. p. 509.

[3] CRUZ, Marco Aurélio Cunha e; MENDES, Marina Letycia - Aproximações do paradigma libertário do "right to privacy" norte-americano. Revista Brasileira de Direito Civil em Perspetiva [Em linha]. Curitiba. Volume 2, N.º 2 (jul./dez. 2016), p. 94. Disponível em: Aproximações do Paradigma Libertário do "Right to Privacy" Norte-Americano | Cruz | Revista Brasileira de Direito Civil em Perspectiva (indexlaw.org) [acedido em 14.11.2022]. e-ISSN: 2526-0243.

[4] TEIXEIRA, Maria Leonor - Proteção de dados e big data: Os desafios líquidos do pós-panoptismo. Revista do Ministério Público. Lisboa. N.º 159 (jul./set. 2019), p. 198.

nas relações de produção. *"*[O] *acesso à propriedade de uma morada deixa de ser um privilégio da nobreza. A burguesia proprietária pode agora desfrutar de um ambiente próprio, reservado, ou seja, livre dos olhares alheios. Em síntese, o seu lar".* [5] É neste quadro que a «*nova*» classe social burguesa decide reclamar o direito de ser deixado em paz.

Assim, em 1791, decorrente da proteção dos ideais liberalistas, procedeu-se à ratificação da declaração de direitos (*bill of rights*), concebida como instrumento de defesa dos indivíduos face ao poder estadual, cujas emendas ao texto constitucional aprovam medidas para proteção de direitos específicos contra a invasão dos governos federais.[6] Nesta sede, destaca-se particularmente o teor do texto a IV emenda[7], que proíbe a execução de buscas e apreensões sem prévio mandato judicial.

A ideia de privacidade surge, deste modo, tal como afirma COSTA GOMES, primitivamente descrita como estando presente no sistema jurídico norte-americano, adotado pela *common law* (*i.e.,* no Direito privado), emergindo de decisões judiciais. [8] Tal conceito surge primeiro evidenciado como uma manifestação do interesse individual de "ser deixado só", designadamente no caso *Wheaton v. Peters*, no ano de 1834. Contudo, não logrou o mesmo obter, à data, o reconhecimento formal da comunidade jurídica como um direito, facto que só se veio a verificar com a publicação do artigo de Samuel D. Warren e Louis D. Brandeis, que adiante abordaremos.[9]

Sem prejuízo do que antecede, importa notar a obra entretanto publicada, sob a designação de "*A Treatise on the Law of Torts: Or the Wrongs Which Arise Independently of Contract*" (1879)[10], da autoria do juiz norte-americano Thomas Cooley, onde é utilizada a expressão «*right to be let alone*», admitindo-se a existência de um "*direito a ser deixado em paz*". Todavia, o trabalho onde o termo surge inserido

[5] *Cfr.* Acórdão do STJ de 03/03/2010, Proc. n.º 886/07.8PSLSB.L1.S1 (relator Santos Cabral), disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/25061d49157a048c8025770a002ed7d7?OpenDocument [acedido em 14-11-2022].

[6] CRUZ, Marco Aurélio Cunha e; MENDES, Marina Letycia, *Ob. Cit.*, p. 99.

[7] Em cujo texto original se dispõe que "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*". *Cfr.* Nacional Constitution Center [Em linha]. Disponível em: https://constitutioncenter.org/the-constitution/amendments/amendment-iv [acedido em 23.11.2022].

[8] GOMES, Manuel Januário da Costa - O problema da salvaguarda da privacidade antes e depois do computador. Boletim do Ministério da Justiça. Ministério da Justiça. Lisboa. N.319 (out.1982), p. 22.

[9] ZANINI, Leonardo – O surgimento e o desenvolvimento do *right of privacy* nos Estados Unidos. Revista Jurídica Luso-Brasileira [Em linha]. Centro de Investigação do Direito Privado. Lisboa. Ano 1, N.º 4 (2015), pág. 791. Disponível em https://www.cidp.pt/revistas/rjlb/2015/4/2015_04_0791_0817.pdf [acedido em 25.11.2022] ISSN: 2183-539X.

[10] COOLEY, Thomas - A treatise on the law of torts, or the wrongs which arise independent of contract [Em linha]. Callaghan and company. Chicago (1879), disponível em: https://repository.law.umich.edu/books/11/ [acedido em 23.11.2022].

versa sobre responsabilidade civil, definindo que *"o direito à personalidade pode ser considerado como sendo um direito de completa imunidade: o direito de ser deixado em paz (…)*.[11] O Autor desenvolve a sua fundamentação, salientando que existe um dever o de não infligir danos ou adotar uma conduta suscetível de os provocar.[12] Assim, pese embora Thomas Cooley tenha sido responsável pelo cunho da expressão, não a relacionou com a noção de privacidade porquanto na sua obra faz corresponder o «direito de ser deixado só» com o conceito de imunidade pessoal, numa aceção física, traduzida no direito de ter o próprio corpo deixado em paz contra agressões perpetradas por terceiros.[13]

O debate em torno da proteção da esfera da vida privada das pessoas face à ingerência de terceiros, ganha mais tarde a atenção dos académicos da área do direito quando, em 1890, foi publicado, na reconhecida *Harvard Law Review*, um artigo denominado por «*The Right to Privacy*»[14], que se constitui como o primeiro manifesto em prol do reconhecimento da proteção jurídica da ideia de privacidade. O artigo foi redigido pelos advogados Sanuel D. Warren e Louis D. Brandeis, que decidem expressar-se doutrinariamente, manifestando descontentamento quanto à intrusão da imprensa na esfera da privacidade individual, nomeadamente por parte dos jornalistas munidos da mais recente inovação tecnológica à data: a máquina fotográfica em movimento.[15] [16] Para o efeito, os Autores do artigo reuniram decisões jurisprudenciais antigas em matéria de difamação, violação do direito de propriedade, violação da confiança ou contrato implícito, defendendo que as decisões analisadas estão ancoradas num princípio mais amplo, digno de reconhecimento autónomo, a que designaram «direito à privacidade (*right to privacy*)», incluído nos princípios defendidos

[11] "*The right to one's person may be said to be a right ou complete immunity: to be let alone*." *Cfr*. COOLEY, Thomas, *Ob. Cit.,* p. 29.
[12] "*The corresponding duty is, not to inflict an injury, and not, within such proximity as might render it successful, to attempt the infliction of an injury*." *Ibidem,* p. 29.
[13] Neste sentido, *vd.* ZANINI, Leonardo, *Ob. cit.*, p. 791.
[14] WARREN, Samuel D.; BRANDEIS, Louis D. – The Right to privacy. Harvard Law Review [Em linha]. Vol. 4, n.º 5 (dez.1980) pp. 193-220, disponível em: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents (acedido em 22.11.2022).
[15] Neste sentido, *vd.* PINTO, Paulo Mota, *Ob. Cit.*, pág. 512 e PINHEIRO, Alexandre Sousa. *Privacy e Proteção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional.* Lisboa: Faculdade de Direito da Universidade de Lisboa. 2011. pp.348-349. Dissertação de Doutoramento em Ciências Jurídico-Políticas.
[16] Na verdade, em 1880 um jornalista e advogado de nome Edward Lawrence Gorkin já havia empregado a teoria do *right to privacy* no seu artigo "*Rights of the Citizen – IV – To his own reputation*" não tendo, contudo, logrado desenvolver possíveis formas de defesa da sua tese face aos poderes público ou privado. *Cfr.* GODKIN, Edward L. - The rights of the citizen, IV – to his own reputation. *Scribner´s Magazine*, Vol. 8, n. 1 (1890), *apud* SEIPP, David J. - The Right to Privacy in Nineteenth Century America. Harvard Law Review [Em linha]. Vol. 94, (1981), p. 1909. Disponível em https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=2613&context=faculty_scholarship [acedido em 22.11.2022].

pela *Common Law*.[17] [18] Este direito traduz-se na possibilidade, que cada indivíduo detém, de escolher partilhar, ou não partilhar, com terceiros, informações sobre sua vida privada, hábitos, atos e relações.[19] Os Autores defenderam a necessidade do reconhecimento do *right to privacy,* fundada na suscetibilidade que a divulgação de informação pessoal não consentida tem de afetar a personalidade do indivíduo*,* assinalando que o direito à privacidade constitui o direito que *"(…) cada indivíduo possui de proteger sua integridade psicológica, exercendo controle sobre informações que refletiam e aferravam a sua personalidade (…),* tendo incorporado nesta classificação *"(…) um insight psicológico, o que era pouco explorado naquela época (…)*"[20], distinguindo-o do direito à liberdade e do direito à propriedade jurisprudencialmente considerados. A definição *right to privacy* preconizada pelos Autores garantia às pessoas uma ampla liberdade, protegia os sentimentos, pensamentos, emoções, informações pessoais e imagem, pelo que quaisquer intromissões indesejadas na vida das pessoas, a verificar-se, consubstanciariam uma ofensa à própria pessoa, i.e., à sua independência, individualidade, dignidade e honra.[21] Os Autores distinguiram o direito à privacidade do direito à propriedade, "(…) *de modo a garantir a autonomização e a definição de formas próprias de tutela para o primeiro*"[22], constituindo um novo ilícito civil («*torts*»), cujas ações e providências (cautelares) são suscetíveis de ser intentadas junto tribunais comuns.[23]

Não obstante o impacto do artigo doutrinário de Warren e Brandeis no sistema jurídico norte-americano, a aplicação do *privacy* não foi consensual nem tampouco uniforme, tendo-se sucedido casos julgados de forma distinta e tendencialmente reservada a determinados estratos sociais, marcada pelos ideais opostos dos conservadores e dos liberais.[24]

---

[17] Cfr. PEIXOTO, Erick L. C.; JÚNIOR, Marcos E. – Breves Notas Sobre a Ressignificação da Privacidade. Revista Brasileira de Direito Civil – RBDCivil [Em linha]. Vol. 16. (abr./jun.2018) Belo Horizonte, p. 39. Disponível em: https://www.academia.edu/36820607/BREVES_NOTAS_SOBRE_A_RESSIGNIFICA%C3%87%C3%83O_DA_PRIVACIDADE_BRIEF_NOTES_ON_THE_RESSIGNIFICATION_OF_PRIVACY [acedido em 25.11.2022].

[18] No mesmo sentido, *vd.* GLANCY, Dorothy - The invention of the right to privacy. Arizona Law Review [Em linha]. Vol. 21, n. º 1 (1979), p. 21. Disponível em: https://law.scu.edu/wp-content/uploads/Privacy.pdf [acedido em 25.11.2022].

[19] GLANCY, Dorothy J., *Ob. cit.*, págs. 22-23.

[20] PEIXOTO, Erick L. C.; JÚNIOR, Marcos E., *ob.cit.* p. 40-41.

[21] Neste sentido, ZANINI, Leonardo*, ob.cit.* Pág. 795.

[22] PINHEIRO, Alexandre Sousa, *Op. Cit*. p. 353.

[23] *Ibidem* p. 353.

[24] DONEDA, Danilo. Da privacidade à proteção dos dados pessoais [Em linha]. Rio de Janeiro: Renovar, 2006, p. 90. Disponível em: https://www.academia.edu/23345535/Da_privacidade_%C3%A0_prote%C3%A7%C3%A3o_de_dados_pessoais [acedido em 26.11.2022].

Volvidos 80 anos sobre a publicação do artigo, aquando do julgamento do caso *Roe v. Wade,* o Juiz J. Blackmun admitiu que a Constituição não reconhece expressamente o direito à privacidade salientando, porém, que a jurisprudência do Supremo Tribunal dos Estados Unidos permite a sua extração da Constituição, identificando *"raízes daquele direito"* nas emendas constitucionais.[25] [26]

Este panorama começa a alterar-se de forma mais contundente no decorrer da década de 1960, motivado, sobretudo, pelo crescimento da circulação de informações, consequência do desenvolvimento exponencial da tecnologia, dela advindo uma *"capacidade técnica cada vez maior de recolher, processar e utilizar a informação".*[27]

E foi assim que, em 1974, no plano infraconstitucional, foi aprovada a primeira lei alusiva ao direito à privacidade, sob a designação de Privacy Act of 1974[28], que regimenta sobre o modo como a criação e uso de bases de dados informatizados impacta no direito à privacidade, instituindo quatro direitos processuais e substantivos, preceituando mormente que: i) as agências governamentais mostrem os registros de indivíduos mantidos sob o seu controlo; ii) sigam determinados princípios, chamados "práticas de informação justa", quando do recolhimento e do tratamento com dados pessoais; iii) sejam aplicadas restrições sobre como as agências podem compartilhar dados de um indivíduo com outras pessoas e agências e iv) admite que o governo seja processado por violar as disposições.[29] Este diploma garantiu aos norte-americanos uma maior segurança no desenvolvimento de atividades de compilação de dados pessoais, bem como a possibilidade de verificar possíveis abusos na recolha de dados.

[25] NETO, Eugênio Facchini - A noção de privacy na jurisprudência da suprema corte norte-americana: existe um conceito unificador? Revista de Direito Brasileira [Em linha]. Vol. 25, N.º 10 (2020) Florianólopis, SC. p.419-420. Disponível em: A NOÇÃO DE PRIVACY NA JURISPRUDÊNCIA DA SUPREMA CORTE NORTE-AMERICANA: EXISTE UM CONCEITO UNIFICADOR? | Neto | Revista de Direito Brasileira (indexlaw.org) [acedido em 03/12/2020].

[26] Nomeadamente na Primeira Emenda (caso Stanley v. Geórgia, de 1969), na Quarta e na Quinta Emenda (casos Terry v. Ohio, de 1968, Katz v. United States, de 1967, Boyd v. United States, de 1886, Olmstead v. United States, de 1928), nas penumbras do Bill of Rights (caso Griswold v. Connecticut, de 1965), na Nona Emenda (voto concorrente de J. Goldberg, no caso Griswold), ou no conceito de liberdade garantido pela primeira seção da Décima Quarta Emenda (caso Meyer v. Nebraska).

[27] DONEDA, Danilo. Da privacidade (…), *Ob. Cit*., p. 91.

[28] The Privacy Act of 1974. Public Law 93-579, as codified at 5 U.S.C. 552ª. Disponível em: https://dpcld.defense.gov/Portals/49/Documents/Privacy/pa1974.pdf [acedido em 02.01.2023].

[29] MACEDO, Fernanda; BUBLITZ, Michelle; RUARO, Regina - A privacy norte-americana e a relação com o direito brasileiro. Revista Jurídica Cesumar [Em linha]. Vol. 13, n.º 1 (jan./jun. 2013), p. 161-178. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/2666/1898 [acedido em 15.12.2023]. ISSN 1677-64402.

2.2. EVOLUÇÃO CONCEPTUAL E LEGISLATIVA DO DIREITO À PRIVACIDADE NA EUROPA

2.2.1. ENQUADRAMENTO CONCEPTUAL E TUTELA JURÍDICA

A privacidade na Europa desenvolveu-se alicerçada na proteção da dignidade do indivíduo, a partir do reconhecimento dos direitos de personalidade[30], pelo que importa primeiramente fazer um breve enquadramento do direito à privacidade face à tutela geral da personalidade[31]. Para tal, cumpre deslindar sucintamente alguns conceitos relevantes.

Em termos sumários, a personalidade é classificada pela doutrina como uma qualidade[32] inerente à pessoa, enquanto sujeito de direitos e obrigações[33] e titular autónoma de relações jurídicas, devendo a sua natureza ser considerada pelo sistema jurídico vigente no efetivo momento sua tutela.[34]

No nosso ordenamento jurídico, a personalidade das pessoas singulares adquire-se aquando do nascimento com vida e termina com a morte[35], donde se extrai que todo o ser humano possui personalidade jurídica.[36] E se os direitos e deveres são atribuídos às pessoas a partir do momento em que adquirem personalidade jurídica, esta constitui-se como condição necessária à realização dos fins ou interesses de cada indivíduo na vida em sociedade.[37] [38]

Visando a proteção da pessoa, os direitos de personalidade centram-se na respetiva vida, abarcando diversos direitos, tais como, entre outros, o direito ao nome, à honra, à imagem, à reserva da intimidade da vida privada, à saúde, à integridade física e moral, à liberdade psicológica e física.

---

[30] PINTO, Paulo Mota. *Op cit*. p. 478.

[31] A matéria inerente aos direitos de personalidade abrange uma problemática conceptual extensa, que foge ao nosso propósito, pelo que, tendo em vista a melhor compreensão dos seus aspetos essenciais, sugere-se a leitura dos seguintes autores: PINTO, Carlos Mota - *Teoria Geral do Direito Civil*, 3.ª Ed. Atualizada. Coimbra: Coimbra Editora, 1996. ISBN 972-32-0383-9; CAMPOS, Diogo Leite de. - *Direitos da Personalidade*. Lisboa: Associação Académica da Universidade Autónoma de Lisboa. 1991; SOUSA, Rabindranath Capelo de - *O Direito Geral de Personalidade*, 1.ª ed. (reimpressão), Coimbra: Coimbra editora. 2011; DRAY, Guilherme Machado - *Direitos de Personalidade*. Anotações ao Código Civil e ao Código do Trabalho Coimbra: Almedina. 2006.

[32] *Cfr.* VASCONCELOS, Pedro Pais de - *Teoria Geral do Direito Civil*, 5.a ed., Coimbra: Almedina, 2008, p. 35.

[33] PINTO, Carlos Mota - *Teoria Geral do Direito Civ*il, Ob. cit., p. 86.

[34] *Ibidem*, p. 87.

[35] *Cfr*. artigos 66.º, n.º 1 e 68.º, n.º 1 do *Código Civil*, respetivamente.

[36] PINTO, Carlos Mota- *Teoria Geral do Direito Civ*il, *ob. cit*., p. 86.

[37] *Ibidem*, p. 100.

[38] No continente europeu, Portugal foi pioneiro no reconhecimento e positivação dos direitos de personalidade e, bem assim, na concernente proteção contra quaisquer violações ilícitas ou ameaças de ofensa, físicas ou morais (*cfr.* artigo 70.º do Código Civil).

MENEZES CORDEIRO [39] dissocia os bens de personalidade em três círculos. O primeiro – biológico – abrange a vida e a integridade física dos sujeitos, que compreende o direito à vida, à saúde e à integridade física. O segundo – moral–, integra a intocabilidade espiritual, nomeadamente o direito ao bom nome e à reputação. O terceiro, – social – respeita às relações entre as pessoas, v.g., direito ao nome, à imagem e à vida privada. Sem prejuízo, insta salientar que os direitos de personalidade não possuem um caráter taxativo porquanto, independentemente da existência de previsão legal específica, deverão ser reconhecidos quantos direitos se afigurem necessários na defesa da personalidade da pessoa.[40]

Para além dos normativos internos, também diversos diplomas internacionais de relevo, conforme adiante se abordará, garantem a proteção da pessoa humana e da sua dignidade. E mesmo dentro do nosso ordenamento jurídico é possível constatar que os direitos de personalidade não possuem um âmbito exclusivamente civilista, estando alguns insertos no corpo do texto constitucional, sob a epígrafe "outros direitos pessoais"[41], classificados como direitos fundamentais de personalidade.

Assim, na distinção entre direitos de personalidade e direitos fundamentais, cumpre salientar que os primeiros são aqueles que apenas possuem influência sobre as relações entre particulares, ou entre estes e o estado, desde que este último intervenha despido do seu poder de império, correspondendo-lhes "*(…) uma tutela assente em meios igualmente promanantes do Direito Civil.*[42] Por outro lado, os direitos fundamentais de personalidade serão os que, tendo assento no texto constitucional, "*pressupõem uma relação entre os particulares e o estado (revestido este, aqui, do seu ius imperii), posto que lancem, outrossim, sua luz sobre as relações entre particulares (…)*". Ademais, os mecanismos de tutela, nesta situação:

> "(…) *já serão de índole jusconstitucional. em face do que não nos será difícil compreender que nem todos os direitos de personalidade serão veros direitos*

[39] *Cfr.* CORDEIRO; António Menezes - *Tratado de Direito Civil IV***.** 4.ª Ed., rev. e atual. Coimbra: Almedina, 2017, p.118.

[40] Nesse sentido, *vd*. SOUSA, Rabindranath Capelo de, *op. cit.*, p. 151.

[41] Previstos no artigo 26.º da CRP, onde se dispõe que "*1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reservada intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação. 2. A lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias. 3. A lei garantirá a dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica. 4. A privação da cidadania e as restrições à capacidade civil só podem efetuar-se nos casos e termos previstos na lei, não podendo ter como fundamento motivos políticos*.".

[42] DIAS FERREIRA, Diogo - Trabalhador, reserva da intimidade da vida privada e «redes sociais. Nótulas reflexivas sobre um delicado problema juslaboral, Revista da Ordem dos Advogados [Em linha]. Lisboa. Ano 80 (jul./dez. 2020), p. 586**,** disponível em: https://portal.oa.pt/media/132093/diogo-figueiredo-perfeito-dias-ferreira.pdf [acedido em 10.01.2023].

> *fundamentais, e vice-versa. Mas também é verdade que, hodiernamente, se verifica larga tendência de absorção daqueles por estes; é dizer, de «constitucionalização» de alguns direitos de personalidade, alçapremando-os, de tal guisa, ao status de direitos fundamentais".*[43]

Neste enquadramento importa, agora, compreender a evolução do direito à privacidade em face da tutela da personalidade. Com efeito, conforme já mencionado, a noção do que é "privado" surge como critério negativo ou antagónico em relação ao que é público, mormente por não incluir informação relevante para terceiros. Durante séculos, esta dicotomia esteve baseada na tensão entre o social e o individual, situação que se foi alterando com o decurso do tempo, tendo passado a abarcar a vida pessoal e familiar em contraposição à vida social ou comunitária.[44] Assim, a noção de privacidade foi evoluindo de modo a incluir os aspetos relacionados com a individualidade da pessoa e a respetiva esfera social mais íntima, *i.e.,* a família, excluindo, por conseguinte, todas as questões relacionadas com a vida social ou comunitária. Sem prejuízo, do termo privacidade não é possível extrair um significado preciso, na medida em que este possui características intrínsecas que lhe conferem elasticidade e imprecisão, sendo afetada pelo contexto histórico-político e pela perspetiva em que é analisada. Da aludida elasticidade resulta a dificuldade de delimitar o bem jurídico e, por conseguinte, a respetiva tutela jurídica.[45]

Acresce, por outro lado, que de entre as várias espécies de direitos fundamentais de personalidade legalmente regimentadas constam os direitos que preservam a intimidade da vida privada, tal como o direito à intimidade e à privacidade, que muitas vezes, se confundem, na medida em que a intimidade é o núcleo da vida privada.

Para dar resposta a esta problemática foi elaborada, em 1953, por Heinrich Hubmann[46] a teoria das esferas ou teoria dos círculos concêntricos (*Sphärentheorie,* no direito alemão), que influenciou os textos constitucionais europeus. Esta teoria distingue o que é liberdade individual, quer no plano social, quer no inter-relacional, de modo a melhor definir o conceito e gerar proteção jurídica. A sua aplicação permite, nomeadamente, distinguir privacidade de intimidade, cujos conceitos são muitas vezes empregues como sinónimos.[47]

---

[43] *Ibidem.*
[44] PINTO, Paulo Mota - *Direitos de Personalidade e Direitos Fundamentais, Ob. Cit*., pág. 509.
[45] *Ibidem*, pág. 503-504.
[46] Cujo critério teórico consta da sua Obra "*Das persomlichkeitrecht*" e foi desenvolvida pela jurisprudência e doutrina alemãs.
[47] *Cfr.* HIRATA, Alessandro - Direito à privacidade. Enciclopédia jurídica da PUC-SP [Em linha]. Coord. De Celso F. Campilongo, Alvaro A. Gonzaga e André L. Freire. Tomo: Direito Administrativo e Constitucional. 1.ª Ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade [acedido em 09.02.2023].

O seu Autor defende que a intensidade da tutela jurídica da privacidade deve variar de forma inversamente proporcional à sociabilidade do comportamento analisado. Ou seja, quanto mais interno for o comportamento no seio das esferas, mais intensa deverá ser a proteção jurídica, representando os diferentes graus de manifestação do sentimento de privacidade.[48] Para tal, dividiu a noção de privacidade em três esferas concêntricas, i.e., a esfera privada, a esfera íntima e a esfera secreta (*Privatsphäre*, *Intimsphäre* e *Geheimsphäre*). A primeira – a esfera privada –, agrega as outras duas esferas e encerra os aspetos da vida da pessoa excluídos do conhecimento de terceiros. A segunda, – a esfera íntima –, serve de intermediária entre as outras duas e abarca os valores inerentes à intimidade, com acesso restrito a determinados indivíduos com os quais a pessoa se relaciona de forma mais intensa. Por último, a menor e mais interna esfera, a do segredo, referindo-se ao sigilo. Desse modo, quanto mais interna for a esfera, mais intensa deve ser a proteção jurídica.[49]

Muitos autores recorrem a este instrumento para enquadrar situações concretas e definir o grau de confidencialidade a que estão sujeitas, tendo em vista balizar a ingerência de terceiros na vida privada, por parte do Estado ou de outras pessoas.

Contrastando da maioria dos autores, que sustentam a existência de três esferas, MENEZES CORDEIRO[50] defende que esta teoria é composta pelas esferas pública, individual-social, privada, secreta e íntima. [51]

Na esfera pública incluem-se as personalidades públicas, v.g., políticos, atletas, artistas, pelo que, o escrutínio dos aspetos da vida privada na esfera pública, possuem uma tutela menos intensa, dado o manifesto interesse do público na exploração da vida íntima. Não obstante, não deve entender-se uma ausência de proteção legal neste âmbito. Já a esfera individual-social, integra os aspetos ou elementos que cada ser humano partilha com aqueles com quem detém relações de proximidade, tais como os amigos, conhecidos ou mesmo colegas de trabalho.[52] Por seu turno, no domínio da esfera privada, estão incluídas as pessoas que integram um círculo mais

[48] SAMPAIO, José Adércio Leite. Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998., p. 254. ISBN: 8573082178

[49] Não obstante a sua aplicação pelos tribunais alemães, a teoria das esferas enfrenta algumas críticas. Aponta-se, designadamente, a impossibilidade de se determinar cientificamente as fronteiras que dividem as três esferas, podendo também salientar-se a falta de relevância prática na divisão do conceito em esferas, "(…) ***não resultando em proteção jurídica diversa.***".[49] *Cfr*. FERRAZ JUNIOR, Tércio Sampaio - Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado [Em linha]. Cadernos de direito constitucional e ciência política. Ano 1. São Paulo: Revista dos Tribunais, 1992. p. 215-217. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231 [acedido em 22/12/2022].

[50] CORDEIRO, A. Meneses, *Tratado de Direito Civil IV*, *Ob. cit*., pp. 261-262.

[51] No mesmo sentido, VASCONCELOS, Pedro Pais de - *Direito de Personalidade*. Coimbra: Almedina. 2014, p. 80.

[52] CORDEIRO, A. Meneses, *Tratado de Direito Civil IV*, *Ob. cit*., p. 262.

íntimo e que compartilham aspetos da vida privada desconhecidos por quem está fora daquele contexto específico, designadamente os familiares e outras pessoas mais próximas. A esfera secreta integra os detalhes ou situações da vida privada que o titular não deseja ver divulgados, v.g., informações e acontecimentos confidenciais, que não podem ser acessíveis sem um consentimento, pois a sua disseminação poderá representar lesão para os direitos de personalidade, devendo possuir uma tutela absoluta. Por último, a esfera íntima e mais restrita de todas, representa tudo o que é segredo para o indivíduo, a quem quase ninguém tem acesso.[53]

No mesmo sentido caminha PAIS DE VASCONCELOS[54], para quem a esfera da vida íntima engloba os aspetos mais secretos da vida pessoal, aqueles que a pessoa nunca ou quase nunca partilha com outras pessoas, exceto as pessoas muito próximas, como a sexualidade, a afetividade, a saúde e a nudez, enquanto a esfera da vida privada seria mais ampla, envolvendo aspetos que as pessoas comungam com pessoas de sua relação, mas não a conhecidos ou ao público. Já para ALEXANDRE PINHEIRO, é na esfera do segredo que se desenvolvem os *"(…) pensamentos, opiniões, descrição de sensações, atuações e outros factos que o indivíduo pretende que se mantenham reservados e tem interesse em que sobre eles exista segredo."*[55].

Sem prejuízo do que antecede, há, contudo, que perceber que a integração em cada uma das esferas pode variar de pessoa para pessoa, consoante a respetiva perceção do que constitui informação íntima e confidencial.

Neste quadro, o direito à privacidade afigura-se como uma nova forma de liberdade pessoal, passando de uma liberdade negativa, baseada no poder de recusar ou proibir a utilização das informações sobre a própria pessoa, convertendo-se numa liberdade positiva de poder controlar os próprios dados.[56] É nesta perspetiva que ALEXANDRE PINHEIRO[57] critica a teoria das esferas, ressaltando ser no âmbito da autodeterminação informacional, originada nos direitos da personalidade, que devem ser estabelecidas as áreas que devem ser protegidas e as que devem ser objeto de tratamento. *Id est*, no domínio da matéria em apreço, o que compreende a «esfera privada» deve estar na livre disponibilidade de decisão de cada indivíduo, tendo este a faculdade de converter uma informação integrada na esfera íntima em informação objeto de divulgação pública, dependendo da personalidade individual e da situação concreta.

[53] *Ibidem*.
[54] VASCONCELOS, Pedro Pais - *Teoria Geral do Direito Civil*. *Ob.cit*. p. 64.
[55] PINHEIRO, Alexandre Sousa, *Ob. Cit*. p. 541.
[56] SAMPAIO, José Adércio Leite. *Ob. cit*., p. 492-493.
[57] PINHEIRO, Alexandre Sousa. Privacy e protecção de dados pessoais, ob. cit., p. 452.

Nesta conformidade, evidencia-se contexto europeu do pós II.ª Guerra Mundial (meados do século XX), associado ao desenvolvimento tecnológico, com especial relevo para a invenção do computador e a democratização da fotografia e da imprensa, que contribuíram para a transformação da personalidade, atribuindo-lhe valor jurídico [58].

Estas circunstâncias factuais trouxeram fragilidades à conceção originária do «direito a ser deixado só», abrindo espaço para uma noção cujo centro de gravidade é a possibilidade de cada um controlar o uso das informações que lhe dizem respeito, i.e., o chamado direito à autodeterminação informativa, traduzido no poder de controlar as suas próprias informações. Do exposto adveio a necessidade de conceber regras específicas que regulem a recolha e utilização de dados pessoais, emergindo assim um novo conceito de vida privada, conhecido em algumas jurisdições como «privacidade informacional» [*informational privacy*] e noutras como «direito à autodeterminação informacional» [*right to informational self-determination*].[59]

Registou-se, assim, a propensão de inclusão do direito à privacidade entre os instrumentos de tutela da personalidade, desvinculando-o do direito de propriedade inicialmente concebido. Verificou-se, ademais, uma necessidade premente em se conceder uma tutela integral à personalidade, concebendo-se a pessoa humana como titular de um conjunto de direitos que salvaguardem os direitos de personalidade. O homem passa a ser observado como figura central do Direito e do Estado, o fim máximo das ações do Estado e dos outros seres humanos. Por essa razão, a sua dignidade é elevada, o que permitiu olhar para pessoa humana como detentora de consciência, sentimentos e ideais a que correspondem direitos de personalidade (*v.g.* honra, reputação e dignidade), tendo assumido um papel de destaque, corporizado em inúmeras restrições e proibições.[60]

Este conceito levou ao desenvolvimento de normas legais especiais que asseguram a proteção da informação pessoal. Nas palavras de ALEXANDRE PINHEIRO, *"(…) no espaço europeu, a terminologia e a linguagem que saíram da doutrina para os textos legais e se expandiram "extramuros" através dos textos de Direito Internacional e das diretivas comunitárias têm uma decisiva influência germânica*." [61].

[58] Nesse sentido, *vd.* PINHEIRO, Alexandre Sousa. *Ob. Cit*. p. 526.
[59] Manual da Legislação Europeia sobre Proteção de Dados - Agência dos Direitos Fundamentais da União Europeia [Em linha]. Ed. 2018, Luxemburgo: Serviço das Publicações da União Europeia, 2022., p. 21. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_pt.pdf. [acedido em 26.12.2022]. ISBN 978-92-871-9825-9.
[60] PINTO, Paulo Mota - *Direitos de Personalidade e Direitos Fundamentais, Ob. Cit*., pág. 478.
[61] PINHEIRO, Alexandre Sousa - *Privacy e Proteção de Dados Pessoais, Ob. Cit*. p. 515.

De facto, os direitos de personalidade encontram tutela na dignidade da pessoa humana, ancorada no valor da pessoa e concernente necessidade de respeito desta. Esta representação possui génese germânica e assenta na perspetiva da proteção contra os perigos que decorrem das instituições de poder na sociedade, contextualizadas na necessidade de fortalecer os direitos fundamentais após a vivência de duas guerras mundiais.[62]

A este respeito, importa evidenciar os baluartes conceptuais manados pelo modelo legislativo germânico, mormente o concebido pela respetiva lei fundamental e que inspirou o direito europeu. Com efeito, de acordo com o artigo 1.º da *Grundgesetz*[63]*, "A dignidade da pessoa humana é intangível. Respeitá-la e protegê-la é obrigação de todo o poder público.".*[64] Acresce que o artigo 2.º da mesma Lei assevera que todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral.

Das referidas disposições extrai-se, portanto, que dignidade da pessoa humana enquanto direito fundamental de personalidade constitui o sustentáculo dos princípios plasmados no texto constitucional, presidindo e guiando os demais princípios e normas legais vigentes.[65]

Para ALEXANDRE PINHEIRO, o princípio da dignidade:

> "*(…) juridicamente construído através de uma decisão política, releva, sobretudo, a intenção de dotar o Estado de posições gerais de respeito e ação, enquanto pessoa coletiva pública nas tarefas que desenvolve, nomeadamente no exercício de funções soberanas. A "positivação" não significa um "esbulho antropológico": o ser humano não fica subtraído à possibilidade de construir o seu destino dentro de qualquer quadro moral de ação e formação.*". [66]

Deste modo, conforme precedentemente analisado, os direitos fundamentais constitucionalmente positivados em sede de direito público distinguem-se dos direitos de personalidade, que regimentam as posições jurídicas elementares, reconhecidas e reguladas pela lei civil e que e emergem da posição paritária do ser humano. Estes últimos inserem-se no rol dos direitos fundamentais, cuja proteção é indispensável à defesa da dignidade, da liberdade e do livre desenvolvimento da pessoa humana

---

[62] ANDRADE, José Carlos Vieira de - *Os direitos fundamentais na Constituição portuguesa de 1976.* 4.ª Ed. Coimbra: Almedina. 2009. p. 68.

[63] Disponível em: https://www.uni-wuerzburg.de/fileadmin/36020000/grundgesetz.pdf (acedido em 03-01-2023).

[64] Tradução livre de: "*Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt*".

[65] Neste sentido, vd. NOVAIS, Jorge Reis - A dignidade da pessoa humana: dignidade e inconstitucionalidade. Vol. II, Coimbra: Almedina, 2017, p. 35.

[66] *Ob. Cit*. p. 992.

porquanto respeitam à sua essencialidade. Por seu turno, o desfrute desses direitos deve ser articulado com a autonomia e a privacidade individuais. Nesta medida, o direito à privacidade constitui-se como um direito de personalidade integrado nos direitos que preservam a intimidade da vida privada, protegidos pelo ordenamento jurídico com a finalidade de preservação da dignidade da pessoa humana, abordada em diversos normativos internacionais. E pese embora, em regra, sejam admitidas restrições aos direitos de personalidade, tal não pode suceder quando estas afetem a dignidade da pessoa humana porquanto, tal facto, contraria o princípio da ordem pública.[67] [68]

A privacidade, na matriz europeia, apresenta-se assim como um direito essencialmente defensivo, que coexiste com vários outros da mesma índole, como os direitos à inviolabilidade do domicílio, ao sigilo de correspondência, à imagem.[69]

Nas palavras de OLIVEIRA ASCENÇÃO, tal facto encontra explicação nos riscos associados à vivência contemporânea citadina em que o homem permanece sozinho, desamparado face ao Estado e a terceiros, situação agravada pelas vulnerabilidades inerentes ao desenvolvimento tecnológico, que o torna exposto, o que demanda a adoção das *"(…) cautelas indispensáveis para evitar que da revelação ou do mero conhecimento de dados individuais resulte o afrontamento das pessoas a que respeitam*.". [70]

Não obstante a evolução tecnológica constituir uma realidade presente e permanente, não é possível imiscuirmo-nos da necessidade e relevância quanto à existência de limites inexcedíveis que salvaguardem os valores inerentes à dignidade da pessoa humana, onde se incluem os direitos fundamentais e de personalidade e, bem assim,

---

[67] Neste sentido *vd.* Acórdão do STJ de 30.05.2019, 2ª secção, Processo n.º 336/18.4T8OER.L1.S1, Relator: Catarina Serra, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/32d36f4f4a970a598025840a00511a7f?OpenDocument [acedido em 05.01.2023], onde se refere que *"(…) o direito à reserva sobre a intimidade da vida privada e os outros direitos de personalidade são concretizações da dignidade da pessoa humana. A dignidade humana é um valor intangível e indisponível de todas as pessoas – é, justamente, um daqueles "valores injuntivos do ordenamento". Assim, se são admissíveis, por princípio, restrições aos direitos de personalidade, já não o são aquelas que atinjam / toquem o limite da dignidade da pessoa humana, por violarem o princípio da ordem pública*.".

[68] Para Mota Pinto, deve entender-se por ordem pública *"o conjunto dos princípios fundamentais, subjacentes ao sistema jurídico, que o Estado e a sociedade estão substancialmente interessados em que prevaleçam e que têm uma acuidade tão forte que devem prevalecer sobre as convenções privadas (…) que não são suscetíveis de uma catalogação exaustiva, até porque a ordem pública é variável com os tempos". Cfr. Teoria Geral do Direito Civil*, *ob. cit.,* p. 434.

[69] ASCENSÃO, José de Oliveira - A reserva da intimidade da vida priva e familiar. *Revista da Faculdade de Direito da Universidade de Lisboa*, Coimbra Editora: Vol. 43, N.º 1 (2002), p. 14.

[70] ASCENÇÃO, José de Oliveira - A dignidade da pessoa e o fundamento dos direitos humanos. Estudos em Homenagem ao Prof. Doutor Martim de Albuquerque. Revista da Ordem dos Advogados (ROA) [Em linha], Ano 68, Vol. I. (2008). Disponível em: https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados-roa/ano-2008/ano-68-vol-i/doutrina/jose-oliveira-ascensao-a-dignidade-da-pessoa-e-o-fundamento-dos-direitos-humanos/ [acedido em 22.12.2022].

o direito à reserva da intimidade da vida privada. Para tal terá de existir um compromisso entre aquilo que é o desenvolvimento tecnológico e a salvaguarda dos mais elementares direitos inerentes ao ser humano.[71]

2.2.2. EVOLUÇÃO LEGISLATIVA

Sem prejuízo da constatação que o direito à privacidade mereceu a tutela do direito supranacional geral[72], importa destacar os principais diplomas europeus nesta matéria, cuja evolução parte de:

> *"(…) um enfoque mais técnico e restrito até a abertura mais recente a técnicas mais amplas e condizentes com a profundidade da tecnologia adotada para o tratamento de dados, em busca de uma tutela mais eficaz e também vinculando a matéria aos direitos fundamentais*". [73]

Na Europa, o direito ao respeito pela vida privada foi consagrado pela Convenção Europeia dos Direitos do Homem (CEDH)[74], juridicamente vinculativa para as suas partes contratantes, i.e., os Estados-membros. O documento foi subscrito em Roma em 1950, tendo entrado em vigor no dia três de setembro de 1953. Trata-se de um tratado internacional destinado a proteger os direitos humanos e as liberdades fundamentais na Europa[75], incluindo o direito à vida privada e familiar, vertido no seu artigo 8.º.[76] De acordo com este artigo, o direito à proteção contra a recolha e utilização de dados pessoais faz parte do direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência.[77] Os Estados-Membros do Conselho da Europa estão vinculados às disposições do CEDH. Sem prejuízo, de modo a assegurar o respetivo cumprimento, foi criado, em 1959, o Tribunal Europeu dos

[71] GOMES, Manuel Januário da Costa, *ob. Cit.*, pp. 20-21.
[72] Em particular por via da Declaração Universal dos Direitos Humanos (DUDH) das Nações Unidas, cujo artigo 12.º preceitua a respeito da vida privada e familiar. A DUDH influenciou a formulação de outros instrumentos sobre direitos humanos na Europa. *Cfr*. Organização das Nações Unidas (ONU), Declaração Universal dos Direitos do Homem (DUDH), 10 de dezembro de 1948. Disponível em: PT-UDHR-v2023_web.pdf (unric.org) [acedido em 25.12.2022].
[73] DONEDA, Danilo - A Proteção dos dados pessoais como um direito fundamental. Revista Espaço Jurídico [em linha], Joaçaba, Vol. 12, n.º 2 (jul./dez. 2011), p. 96. Disponível em: https://www.researchgate.net/publication/277241112_A_protecao_dos_dados_pessoais_como_um_direito_fundamental/link/5934045faca272fc553c4abe/download [acedido em 05-01-2023].
[74] Conselho da Europa, Convenção Europeia dos Direitos do Homem, disponível https://www.echr.coe.int/Documents/Convention_POR.pdf [acedido em 25.12.2022].
[75] União Europeia, disponível em: https://eur-lex.europa.eu/PT/legal-content/glossary/european-convention-on-human-rights-echr.html [acedido em 25.12.2022].
[76] *Cfr.* art.º 8.º da CEDH, "1. *Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros*".
[77] *Cfr.* Manual da Legislação Europeia sobre Proteção de Dados, *Ob. Cit*., p. 13.

Direitos do Homem – TEDH, que assegura o cumprimento das inerentes obrigações, por via da apreciação de queixas apresentadas de alegadas violações da Convenção.[78] [79]

Contudo, a evolução tecnológica ditava a necessidade de adotar regras mais pormenorizadas para salvaguardar as pessoas através da proteção dos seus dados, pelo que, em meados da década de 70, o Comité de Ministros do Conselho da Europa adotou várias resoluções sobre a proteção de dados pessoais que faziam referência ao artigo 8.º da CEDH. Assim, abraçando a orientação das normas constitucionais dos países já citados, tendo em vista acautelar a recolha indevida de informações pessoais, o Conselho da Europa, em 1968, aconselhou, por via da Recomendação 509, sobre Direitos Humanos e Desenvolvimentos Tecnológicos Modernos e Científicos[80], que o Comité de Ministros instruísse o Comité de Peritos em Direitos do Homem para que se procedesse à análise da legislações nacionais dos Estados-membros à luz do preceituado pelo artigo 8.º da CEDH. Esta Recomendação visava aferir se as mesmas protegem adequadamente o direito à privacidade cometidas através da utilização de métodos científicos e técnicos modernos procedendo, em caso, negativo, à emissão de recomendações nesta matéria. Nesta senda, mais tarde, o Conselho da Europa elaborou as Resoluções n.ºs (73) 22[81] e (74) 29[82], de 1973 e 1974, respetivamente, com o objetivo de definir os princípios para a proteção de dados pessoais que se encontrassem em bancos de dados automatizados nos setores público e privado e, bem assim, promover a uniformização das legislações nacionais dos Estados-membros. Para tal, era necessário estabelecer regras internacionais

[78] O TEDH, na sua jurisprudência, tem enveredado pela interpretação atualista (ou dinâmica) dos direitos consagrados na CEDH, permitindo extrair outros direitos do respetivo elemento textual, ainda que embora não expressamente previstos. Tal sucedeu com o direito à proteção de dados, pelo que a CEDH deve ser interpretada em conjunto com a jurisprudência do Tribunal, disponível em: HUDOC - European Court of Human Rights (coe.int) [acedido em 27.12.2022].
Portugal ratificou a CEDH a 9 de novembro de 1978, data em que a Convenção entrou em vigor na ordem jurídica portuguesa. A Convenção é, portanto, vinculativa para o Estado Português e uma fonte de obrigações que devem ser cumpridas no plano interno, sob pena de responsabilização internacional.

[79] A este respeito, importa salientar que CEDH *"(…) vigora diretamente na ordem jurídica portuguesa ex vi do art.º 8.º, n.º 2, da CRP, e em patamar inferior ao das normas constitucionais, mas superior ao das leis ordinárias devendo o direito interno ser aplicado de harmonia com a jurisprudência do TEDH, sobre este instrumento jurídico*". *Cfr*. Acórdão do TRL de 23.02.2017, Processo n.º 23019/16.5T8LSB.L1-8 (relator Isoleta Almeida Costa), disponível em: Acórdão do Tribunal da Relação de Lisboa (dgsi.pt) [acedido em 15.01.2023].

[80] CdE Recommendation 509 (1968), Human rights and modern scientific and technological developments. Disponível em https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en [acedido em 19.01.2023].

[81] (Resolução (73) 22 relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor privado), de 26 de setembro de 1973. Disponível em https://rm.coe.int/1680502830 [acedido em 21.01.2023].
(Resolução (74) 29 relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor público), 20 de dezembro de 1974. Disponível em: https://rm.coe.int/16804d1c51 [acedido em 21.01.2023].

vinculativas que obstassem à existência de discrepâncias nas legislações internas entre os vários Estados-membros.

Ao mesmo tempo, vários países europeus legislavam sobre o controlo de uso de informações pessoais quer por entidades privadas quer pelo próprio governo. Sobre o assunto, importa desde logo salientar a primeira lei relativa à proteção de dados, aprovada em 1970, pelo Parlamento do Estado de Hesse, o *Hessisches Datenschutzgesetz.* O diploma era aplicável à recolha e tratamento de dados por entidades públicas e não continha qualquer disposição que limitasse ou enquadrasse o processo de licitude do tratamento. Para além do exposto, limitava-se a reconhecer direitos secundários dos titulares, tais como corrigir e restaurar dados, definindo ainda a figura do supervisor de dados, enquanto entidade responsável por supervisionar o cumprimento da lei.[83]

Apesar da vanguarda da ciência jurídica alemã nesta matéria, os progressos estaduais impediram o legislador federal de avançar com a elaboração de um diploma aplicável a todo o território nacional. Tal veio a verificar-se noutro país, a Suécia, que em 1973, aprovou o *Datalag,* um diploma experimental que visou testar soluções jurídicas, registais e regulatórias. Todavia, também neste caso foram vivenciadas contrariedades que impediram a sua efetiva aplicação, dificuldades essas decorrentes da digitalização no processamento de informações dos cidadãos e da realização de um censo nacional. Não obstante, "(…) *a prática de legislar sobre proteção de dados de modo integrado, i.e., com um diploma nuclear complementado por legislação setorial iniciado pela Suécia e pela Alemanha, mantém-se várias décadas volvidas, como um elemento central da conceção europeia*.". [84] [85]

E é neste quadro que, em 28 de janeiro de 1981, foi aberta a adesão à Convenção para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais (Convenção ETS[86] n.º 108). Considerada a matriz

[83] CORDEIRO, A. Barreto Menezes - *Direito de proteção de dados à Luz do RGPD e da Lei n.º 58/2019.* Coimbra: Almedina. 2020. p. 64-65.

[84] *Ibidem*, pp. 65-66.

[85] Sem prejuízo do que antecede, importa ainda evidenciar o facto de, entretanto, três países europeus terem procedido à inclusão do direito à proteção de dados enquanto direito fundamental nos respetivos textos constitucionais, i.e., Portugal, Espanha e Áustria. Com efeito, no caso específico de Portugal, cumpre registar que, pese embora apenas tenha aderido à CEDH em novembro de 1978, a Constituição da República Portuguesa de 1976 já previa, no seu artigo 33.º, o direito à intimidade da vida privada e familiar e proibia a utilização abusiva de informações relativas às pessoas e famílias. Paralelamente, o artigo 35.º do mesmo diploma reconhecia o direito dos cidadãos a tomar conhecimento do que constar de registos mecanográficos a seu respeito, retificar e atualizar esses mesmos dados, impedindo o tratamento de dados referentes a convicções políticas, religiosas ou de vida privada.

[86] Também conhecida como a Convenção de Estrasburgo. Encontra-se disponível em: https://rm.coe.int/1680078b37 [acedido em 05.02.2023].

de todas as leis sobre proteção de dados pessoais, a ETS foi o primeiro instrumento internacional juridicamente vinculativo, especificamente dedicado à sua proteção.[87]

A Convenção 108 do Conselho da Europa permitia a adesão de Estados não membros do Conselho da Europa[88], sendo organizada por um conjunto de princípios, tidos hoje por "*universais*" e consagrados nas diversas leis sobre proteção de dados pessoais a nível mundial. O objetivo da Convenção 108 é o tratamento de liberdades e direitos fundamentais, que incluem a privacidade e a proteção de dados pessoais, deferindo-lhes autonomia e caracterização de direito fundamental conforme, aliás, resulta expresso na respetiva nota preambular[89] e que deve ser harmonizado com a liberdade de circulação da informação pessoal nos Estados signatários. Daqui emerge a necessidade de *"(…) harmonizar direitos fundamentais com as vantagens económicas próprias de mercados abertos, onde a livre circulação de dados pessoais constitui um importante fator de gestão*".[90]

O diploma aplica-se, assim, a todos os tratamentos de dados pessoais realizados tanto pelo setor privado como pelo setor público[91], incluindo os tratamentos de dados efetuados pelas autoridades policiais e judiciárias visando, paralelamente, garantir o respeito pelos direitos e liberdades fundamentais de cada indivíduo, em particular, o seu direito à privacidade em relação a "*tratamentos automatizados dos dados pessoais que lhe digam respeito*". [92]

Dos aspetos relevantes da Convenção cumpre destacar as definições previstas no artigo 2.º, mormente as de «Dados de Caráter Pessoal»[93], «ficheiro automatizado», «tratamento automatizado» e «responsável pelo ficheiro»; a qualidade dos dados, que demanda que o tratamento dos dados obedeça aos princípios da lealdade e da licitude, limitação das finalidades, minimização, exatidão e limitação a conservação.

---

[87] Manual da Legislação Europeia sobre Proteção de Dados, *op.cit*. p. 16.

[88] Portugal aderiu à Convenção 108 a 14 de maio de 1981, pese embora apenas tenha vindo a ratificá-la em 1993, pela Resolução da Assembleia da República n.º 23/93, de 09/07 (retificada pela Retificação n.º 10/93, de 20/08, publicada no *Diário da República*, I Série-A, n.º 195/93); ratificada pelo Decreto do Presidente da República n.º 21/93, de 09/07 e sendo aplicável no nosso País de 01-01-1994 (*cfr*. https://www.ministeriopublico.pt/instrumento/convencao-para-proteccao-das-pessoas-relativamente-ao-tratamento-automatizado-de-dados-2) [acedido em 07.02.2023].

[89] Onde se dispõe que o Conselho da Europa tem por finalidade *"(…) realizar uma união mais estreita entre os seus Membros e que um dos meios de alcançar esta finalidade é a proteção e o desenvolvimento dos direitos do homem e das liberdades fundamentais*".

[90] PINHEIRO, Alexandre Sousa - *Privacy e Proteção de Dados Pessoais.* p. 638.

[91] *Cfr*. artigo º 3.º, n.º 1.

[92] *Cfr.* artigo 1.º.

[93] "*A definição de dados pessoais assenta nos elementos da "identificação" e da "identificabilidade", não referindo, no articulado, as dificuldades ou custos que podem ser despendidos no processo. No entanto, de acordo com o n.º 28 do Memorando Explicativo da Convenção do Conselho da Europa, por pessoa identificável deveria entender-se «uma pessoa facilmente identificável». Não se cobre, assim, a identificação de pessoas por métodos excessivamente complexos". Cfr*. PINHEIRO, Alexandre Sousa - *Privacy e Proteção de Dados Pessoais ob. cit.* p. 639.

Releva, de igual modo, evidenciar a consagração do direito do indivíduo de ser informado sobre a existência de ficheiros automatizados a seu respeito, de aceder à informação, de retificar e de suprimir dados pessoais que lhe digam respeito e que constem de ficheiros automatizados. E a proibição de tratamento de dados «sensíveis», na ausência de garantias jurídicas adequadas. [94]

Da Convenção de Estrasburgo e das já mencionadas Resoluções do Conselho da Europa dimanaram, assim, um "núcleo comum" de princípios aplicáveis em matéria de proteção de dados pessoais, os quais vêm a constituir:

> "(…) *a espinha dorsal das diversas leis, tratados, convenções ou acordos entre privados em matéria de proteção de dados pessoais, formando o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais*.". [95]

Mais tarde, numa altura em que vários Estados-Membros já tinham aprovado legislação interna em matéria de dados, é adotada a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995[96], relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Diretiva de Proteção de Dados). Esta Diretiva surge no contexto emergente da livre circulação de mercadorias, capitais, serviços e pessoas no mercado interno, que demanda o livre fluxo de dados e que apenas seria exequível se Estados-membros estivessem aptos a confiar na existência de um nível de proteção elevado e uniforme nesta matéria. O propósito do diploma era, no essencial, nivelar o nível de proteção dos direitos, liberdades e garantias ao seu expoente máximo e aproximar as legislações nacionais nesta matéria.[97] O diploma tem por objeto a "(…) *proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais*" (*cfr*. artigo 1.º, n.º 1), definindo que o seu âmbito de aplicação abrange o *"(…) tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como o tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados"* (*cfr*. artigo 3.º, n.º 1). Do disposto exclui-se o tratamento de dados no âmbito das atividades não sujeitas à aplicação do direito comunitário[98] [99], bem como das atividades que tenham por objeto a segurança pública,

[94] *Cfr.,* artigo art.º 5.º, alíneas a), b), c), d) e e), artigo 8.º, al. a) e artigo 6.º, respetivamente.
[95] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental, *Ob. Cit*., pp. 100-101.
[96] JO L 281 de 23.11.1995, p. 31. Disponível em: 3b2_to_ps.ps 1..28 (europa.eu) [acedido em 29.01.2023].
[97] Manual da Legislação Europeia sobre Proteção de Dados, *ob. cit.* p. 18.
[98] Tais como as previstas nos títulos V e VI do Tratado da União Europeia.
[99] Nesta sede importa referir que o âmbito territorial da Diretiva abrangia não só os 15 países membros da UE à data, mas também os não membros que integram o Espaço Económico Europeu (EEE). Com efeito,

a defesa e a segurança do Estado, das atividades do Estado no domínio do direito penal e das efetuadas por pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas (*cfr*. art.º 3.º, n.º 2). No artigo 6.º da Diretiva são introduzidos os princípios consignados pela Convenção de Estrasburgo e adotados novos mecanismos de proteção, designadamente a criação de autoridades de controlo independentes a quem compete verificar o cumprimento das regras sobre proteção de dados[100]. O artigo 7.º, por seu turno, consagra os fundamentos de legitimidade para o tratamento dos dados pessoais e o artigo 8.º regimenta sobre as categorias específicas de dados. Os artigos 10.º e 11.º elencam a informação que deve ser prestada ao titular dos dados aquando da recolha destes, que varia consoante sejam recolhidos diretamente do titular ou indiretamente. O direito de acesso vem previsto no artigo 12.º da Diretiva e garante ao titular dos dados o direito de aceder aos dados que lhe digam respeito. De acordo com o artigo 13.º (derrogações e restrições), os Estados-membros podem tomar medidas legislativas destinadas a restringir o alcance das obrigações e direitos referidos no n.º 1 do artigo 6.º, no artigo 10.º, no n.º 1 do artigo 11.º e nos artigos 12.º e 21.º, sempre que tal restrição constitua uma medida necessária à proteção: a) da segurança do Estado; b) da defesa; c) da segurança pública; d) da prevenção, investigação, deteção e repressão de infrações penais e de violações da deontologia das profissões regulamentadas; e) de um interesse económico ou financeiro importante de um Estado-membro ou da União Europeia, incluindo nos domínios monetário, orçamental ou fiscal; f) de missões de controlo, de inspeção ou de regulamentação associadas, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas c), d), e) e g), de pessoa em causa ou dos direitos e liberdades de outrem.

Sem prejuízo, em virtude dos diversos processos instaurados junto do TJUE[101], com fundamento na violação dos direitos humanos por parte da legislação da UE, atendendo à omissão da respetiva proteção nos tratados da Comunidades Europeias e a fim de conceder proteção às pessoas singulares, este Tribunal passou a incorporar os direitos fundamentais nos chamados princípios gerais de direito europeu. De acordo com o TJUE, *"(…) estes princípios gerais refletem as disposições sobre*

não obstante no âmbito do direito da UE, as restrições e proibições ao livre fluxo de dados entre os Estados-Membros por razões relativas à proteção de dados serem proibidas pelo artigo 1.º, n.º 2, da Diretiva de Proteção de Dados, a área do livre fluxo de dados foi alargada pelo Acordo sobre o Espaço Económico Europeu (EEE), que integra a Islândia, o Listenstaine e a Noruega no mercado interno (*Vd*. Acordo com a Decisão do Conselho e da Comissão de 13-12-1993, publicado no JO 1994 L 1, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ%3AL%3A1994%3A001%3ATOC [acedido em 13.02.2023].

[100] Solução que mais tarde foi também incorporada no Protocolo Adicional à Convenção 108 de 2001.

[101] À data, designado de Tribunal de Justiça das Comunidades Europeias (TJCE).

proteção dos direitos humanos constantes das constituições nacionais e dos tratados sobre direitos humanos, em especial a CEDH. O TJUE afirmou que asseguraria a conformidade do direito da UE com estes princípios.".[102]

Nesta conformidade, a UE, admitindo a suscetibilidade de lesão dos direitos humanos através das suas políticas, num esforço para aproximar os cidadãos da União, proclamou, em 2000, a Carta dos Direitos Fundamentais da União Europeia, que, não obstante tratar-se de um documento político, se tornou juridicamente vinculativa como direito primário da UE[103], com a entrada em vigor do Tratado de Lisboa em 1 de dezembro de 2009.[104] [105]

Proclamada solenemente em Nice, em dezembro de 2000, a Carta é, desde a entrada em vigor do Tratado de Lisboa, em dezembro de 2009, juridicamente vinculativa (*cfr.* artigo 6.º do Tratado da União Europeia).

Os artigos 7.º e 8.º da Carta consagram, respetivamente, o direito ao respeito pela vida privada e familiar e o direito à proteção dos dados pessoais. O artigo 8.º é constituído por três números:

> *"(i) reconhece a natureza fundamental e universal do direito à proteção de dados, n.º 1 – esta universalidade é também reconhecida no artigo 16.º/1 do TFUE; (ii) elenca um conjunto variado de princípios concretizadores no RGPD: da lealdade, da licitude (em sentido estrito), da limitação das finalidades, n.º 2; (iii) consagra o consentimento como principal fundamento de licitude do tratamento de dados pessoais, n.º 2; (iv) identifica alguns direitos dos titulares: o direito de aceso e o direito à retificação, n.º 2; e (v) determina a constituição de uma autoridade independente para fiscalizar o seu cumprimento, n.º 3*.".[106]

É, contudo, por via da jurisprudência do TJUE que tem sido possível constatar o entendimento da existência de uma relação de proximidade entre o direito à proteção de dados pessoais e o direito à intimidade da vida privada, o primeiro revelado, como uma manifestação ou um prolongamento, ainda que parcial, do direito fundamental do respeito da vida privada.[107] [108] Nos termos do respetivo artigo 51.º, o âmbito de

[102] Manual da Legislação Europeia sobre Proteção de Dados, *ob. cit.* p. 20.
[103] *Vd*. artigo 6.º, n.º 1, do TUE. O direito primário da UE também atribui à UE competência genérica para legislar sobre matérias relacionadas com a proteção de dados (artigo 16.º do TFUE).
[104] *Ibidem*, p. 21.
[105] Disponível em: Carta dos Direitos Fundamentais da União Europeia (europa.eu) [acedido em 07.02.2023].
[106] CORDEIRO, A. Barreto Menezes - Direito à Proteção de Dados (…), *ob. Cit*. p. 69.
[107] Sobre o assunto evidencia-se o Acórdão *Digital Rights Ireland*, em que o TJUE sublinhou "*O importante papel desempenhado pela proteção dos dados pessoais na perspetiva do direito fundamental ao respeito da vida privada*", sem prejuízo do reconhecimento da autonomia deste último concretizado em legislação própria. É por via deste entendimento que o TEDH tem defendido a posição dos titulares dos dados pessoais, ao abrigo do artigo 8.º da CEDH.
[108] Nesse sentido, *vd.* CORDEIRO, A. Barreto Menezes - Direito à Proteção de Dados (…), *ob. cit*. p. 70.

aplicação da Carta é restrito ao âmbito de aplicação do direito da União Europeia, isto é, vincula as instituições, os órgãos e organismos da União Europeia em toda a sua atuação, mas vincula apenas os Estados-membros quando apliquem direito da União. Contudo, o direito da UE é frequentemente aplicável a nível nacional e influencia partes significativas da legislação e das políticas dos Estados-membros. Isto torna os juízes, os políticos, os funcionários governamentais e os profissionais da justiça agentes fundamentais em matéria de aplicação da Carta. A Carta é aplicável sempre que trabalhem no âmbito do direito da UE.[109]

Por último, quanto à legislação europeia específica em matéria de proteção de dados, importa ainda evidenciar o Regulamento (CE) n.º 45/2001 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados[110], a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas)[111], a Diretiva 2006/24/CE 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[112], e que altera a Diretiva 2002/58/CE (Diretiva da Conservação de Dados, invalidada em 8 de abril de 2014).

Na sequência dos programas de Tampere (outubro de 1999) e de Haia (novembro de 2004), o Conselho Europeu aprovou, em dezembro de 2009, o programa plurianual no Espaço de Liberdade, de Segurança e de Justiça (ELSJ) para o período 2010-2014 – conhecido por Programa de Estocolmo.[113] Nas suas conclusões de junho de 2014, o Conselho Europeu definiu as orientações estratégicas para o planeamento legislativo e operacional para os próximos anos no quadro do ELSJ, em conformidade com o artigo 68.º do TFUE. Um dos principais objetivos consiste em proteger melhor os dados

[109] *Cfr.* Agência dos Direitos fundamentais da EU, disponível em: O que são os direitos fundamentais? | European Union Agency for Fundamental Rights (europa.eu) [acedido em 07.02.2023].

[110] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32001R0045 [acedido em 09.02.2023].

[111] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002L0058 [acedido em 09.02.2023].

[112] Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006 , 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, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32006L0024 [acedido em 09.02.2023].

[113] *Cfr.* Parlamento Europeu, Programa de Estocolmo, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:pt:PDF [acedido em 09.02.2023].

pessoais na UE.[114] Este documento esteve na base da elaboração do Regulamento Geral da Proteção de Dados.

[114] *Cfr.* Parlamento Europeu, Espaço de Liberdade, de Segurança e de Justiça (ELSJ), disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf [acedido em 09.02.2023].

3. O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD): ASPETOS FUNDAMENTAIS

3.1. OBJETO E ÂMBITO DE APLICAÇÃO DO REGULAMENTO

3.1.1. OBJETO:

Em 27 de abril de 2016, o Parlamento Europeu e o Conselho aprovaram o Regulamento Geral de Proteção de Dados - RGPD[115], um ato legislativo da União Europeia, obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-membros a partir de 25 de maio de 2018[116], revogando a Diretiva 95/46/CE, precedentemente em vigor[117].

Dispõe o artigo 1.º do RGPD que são estabelecidas normas "(…) *relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*"[118], visando a proteção dos "*direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais*"[119] e salvaguardando que a livre circulação de dados pessoais na EU, que "*não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais*". [120] [121]

O diploma introduz, assim, um conjunto de novas regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à sua livre circulação, visando o desenvolvimento adequado do mercado interno, nomeadamente no que respeita à economia digital, impondo uma disciplina totalmente uniforme entre

[115] Publicado no Jornal Oficial da União Europeia (JOUE) L 119/1, de 04.05.2016, sob a referência Regulamento (UE) 2016/679 d**o** Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), com posteriores retificações publicadas no JOUE L 127/2, de 23.05.2018, página 2 e JOUE L 74, de 04.03.2021, p. 35.

[116] *cfr.* art.º 99.º do RGPD.

[117] *cfr.* art.º 94.º, n.º 1 do RGPD.

[118] Cfr. Art.º 1.º, n.º 1.

[119] cfr. Art.º 1.º, n.º 2.

[120] cfr. Art.º 1.º, n.º 3.

[121] O Considerando (13) do RGPD acrescenta que *"(…) [o] bom funcionamento do mercado interno impõe que a livre circulação de dados pessoais na União não pode ser restringida ou proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais. (…).*

os vários Estados-membros[122], sem prejuízo da cautela dos direitos e liberdades fundamentais das pessoas singulares. [123]

Para ALEXANDRE PINHEIRO**,** o artigo 1.º do RGPD baseia-se:

> *"(…) na necessidade de garantir a integração económica e social resultante do funcionamento do mercado interno e impedir que o recurso a argumentos relacionados com a proteção de dados pessoais possa funcionar como um obstáculo ao seu funcionamento.*[124]

Nesta conformidade, constituem pressupostos organizatórios do RGPD a existência de: (i) um normativo que assegura a adequada proteção dos dados pessoais em todos os Estados da UE; (ii) um Regulamento que confere e reforça uma proteção idêntica dos dados pessoais nos Estados da UE; e a (iii) ausência de fundamento para a recusa da circulação dos dados pessoais com fundamento no prejuízo dos direitos tutelados pelos artigos 12.º e seguintes do RGPD.[125]

Sem prejuízo do que antecede, importa referir que o RGPD não exclui o direito dos Estados-membros no que tange à definição *"*[d]*as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais*." [126]

3.1.2. ÂMBITO DE APLICAÇÃO:

Os artigos 2.º, 3.º e 4.º do RGPD regimentam acerca do âmbito de aplicação do diploma, definindo os requisitos para aferir do enquadramento respetivo por parte das entidades que tratam dados pessoais.

3.1.2.1. ÂMBITO DE APLICAÇÃO MATERIAL:

Dispõe artigo 2.º, n.º 1 do RGPD que o diploma é aplicável "(…) *ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao*

[122] De acordo com o previsto nos considerandos (5), (6) e (7) do RGPD, a integração económica e social resultante do funcionamento do mercado interno incrementou a necessidade da recolha e partilha de dados pessoais no seio da UE e os desafios da evolução tecnológica e a globalização aumentaram o risco de exposição das pessoas, demandando um quadro de proteção de dados sólido e mais coerente.
[123] *Vd.* Considerandos (1), (2) e (4) do RGPD, que aludem à natureza do direito à proteção dos dados pessoais, à sua função na sociedade e à sua articulação com outros direitos fundamentais.
[124] PINHEIRO, Alexandre [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina. 2018, p. 97.
[125] *Ibidem*.
[126] *Cfr.* Considerando (10), *in fine,* do RGPD.

tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados"[127].

MENEZES CORDEIRO refere que o legislador europeu não previu deliberadamente a definição de «meios automatizados» porquanto "(…) *pretendeu evitar-se que o RGPD fosse, com fundamento no eventual conteúdo positivado, contornado, ou que se tornasse, a breve trecho, obsoleto (princípio da neutralidade tecnológica)"*[128]. E acrescenta que o conceito de tratamento por meios automatizados respeita às operações sobre dados pessoais que envolvam equipamentos de processamento de dados, numa aceção ampla, nos termos da qual o conceito de tratamento por meios não automatizados é sinónimo de tratamento manual, aferido *a contrário sensu* do conceito de tratamento automatizado. Do exposto decorre que o RGPD abrange as operações de tratamento de dados pessoais independentemente de resultarem de intervenção humana. Contudo, não se aplica a todos os tratamentos não automatizados, mas apenas aos que estejam contidos em ficheiros ou a eles se destinem. [129] [130]

O artigo 2.º, n.º 2 do RGPD prescreve, por seu turno, que o RGPD não se aplica ao tratamento de dados pessoais efetuado: (i) no exercício de atividades não sujeitas à aplicação do direito da União (*cfr.* art.º 2.º, n.º 2 al. a)[131]; (ii) pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do Tratado da União Europeia, capítulo 2, Título V (*cfr.* art.º 2.º, n.º 2 al. b)[132]; (iii) por pessoas singulares, no exercício de atividades exclusivamente pessoais ou domésticas (*cfr.* art.º 2.º, n.º 2 al. c) [133]; (iv) pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo

[127] Sobre a matéria, o considerando (15) do mesmo diploma esclarece que a fim de se evitar o sério risco de ser contornada a proteção das pessoas singulares, esta deverá ser neutra em termos tecnológicos e deverá ser independente das técnicas utilizadas. A proteção das pessoas singulares deverá aplicar-se ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento manual, se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros.

[128] CORDEIRO, A. Barreto Menezes - *Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019.* Coimbra: Almedina. 2020, p. 85.

[129] *Ibidem*, págs. 85-86.

[130] Insta remeter para o art.º 4.º, n.º 6) onde se encontra a definição de «Ficheiro», como "*qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico*;".

[131] O Considerando (16) do RGPD esclarece que o RGPD não abrange as questões de defesa dos direitos e das liberdades fundamentais ou da livre circulação de dados pessoais relacionados com atividades que se encontrem fora do âmbito de aplicação do direito da União, como as que se prendem com a segurança nacional nem se aplica ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relacionadas com a política externa e de segurança comum da União.

[132] Cujas disposições versam exclusivamente sobre a «Política externa e de segurança comum».

[133] De acordo com o considerando (18)**,** excluem-se as atividades que não possuam qualquer ligação com uma atividade profissional ou comercial. O TJUE dispôs que a expressão deve ser interpretada no sentido de que tem apenas por objeto as atividades que se inserem no quadro da vida privada ou familiar dos particulares, *cfr.* Processo C-73/07, de 16.12.2008, Satamedia, n.º 44, p. I-9987, disponível em: eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62007CJ0073 [acedido em 19.03.2023].

a salvaguarda e a prevenção de ameaças à segurança pública (*cfr.* art.º 2.º, n.º 2 al. d)[134].

Das diferenças materiais em relação à legislação anterior evidencia-se, em particular, a definição de «dados pessoais», prevista na al. a) do artigo 3.º da Lei n.º 67/98[135] que contrasta com a atual, prevista no artigo 4.º, n.º 1) do RGPD[136], que se tornou mais abrangente, passando a incluir outros elementos, tais como, os dados de localização ou identificadores por via eletrónica, bem como os elementos da identidade genética.

3.1.2.2. ÂMBITO TERRITORIAL:

O artigo 3.º do RGPD alude ao âmbito territorial de aplicação, dispondo que o mesmo é aplicável ao tratamento de dados pessoais: i) *"(…) efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União*" (cfr. art.º 3.º, n.º 1) [137]; ii) de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, desde que as atividades de tratamento estejam conexionadas com a oferta de bens ou serviços [138] a esses titulares de dados na

[134] No considerando (19) do RGPD dispõe-se que "[a] *proteção das pessoas singulares em matéria de tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico. O presente regulamento não deverá, por isso, ser aplicável às atividades de tratamento para esses efeitos (…)".* Neste contexto**,** é aprovada a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

[135] Que transpôs para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho e em cujo artigo 3.º, al. a) se definia o conceito como *"qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".*

[136] Que define «dado pessoal» como a "*informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica*".

[137] O considerando (22) do RGPD elucida que qualquer tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado na União deverá ser feito em conformidade com o presente regulamento, independentemente de o tratamento em si ser realizado na União. O estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto.

[138] Sobre o assunto, o considerando (23) estatui que para se determinar se existe ou não oferta de bens ou serviços aos titulares dos dados que se encontrem na União, "(…) *há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da*

União ou com do controlo do seu comportamento, desde que esse comportamento tenha lugar na União [139] (cfr. art.º 3.º, n.º 2, al. a) e b)); iii) efetuado por um responsável pelo tratamento estabelecido num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público. [140]

O âmbito de aplicação territorial do RGPD acha-se, assim, definido com base em dois critérios principais: o critério do «estabelecimento», nos termos do artigo 3.º, n.º 1, e o critério do «direcionamento», nos termos do artigo 3.º, n.º 2. Além disso, o artigo 3.º, n.º 3, confirma a aplicação do RGPD ao tratamento sempre que o direito de um Estado- Membro se aplique por força do direito internacional público.[141]

3.2. LEI DE EXECUÇÃO NACIONAL

O RGPD, não obstante, instituir uma aplicação coerente e homogénea das regras de proteção de dados, não exclui, como se viu, a faculdade de regulação de situações específicas do tratamento de dados pessoais ao nível do direito interno dos Estados-Membros, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais.

Em Portugal, a definição de determinados aspetos executórios do RGPD faz-se por via da Lei n.º 58/2019, de 8 de agosto[142], que assegura a execução do RGPD, na ordem jurídica nacional e que entrou em vigor em 9 de agosto de 2019, i.e., com um hiato temporal de mais de um ano em relação à aplicação plena do RGPD, verificada em 25 de maio de 2018.

União. Existem fatores *"(…) como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União."*.

[139] De acordo com o considerando (24) do RGPD, para se aferir se existe «controlo do comportamento», deve determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

[140] O considerando (25) prescreve que sempre que o direito de um Estado-Membro seja aplicável por força do direito internacional público, o regulamento deverá ser igualmente aplicável aos responsáveis pelo tratamento não estabelecidos na União, por exemplo numa missão diplomática ou num posto consular de um Estado-Membro.

[141] *Cfr.* Diretriz 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3.º) Versão 2.0 12 de novembro de 2019 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf [acedido em 25.08.2023].

[142] Publicada em *Diário da República,* Série I, n.º 151/2019, de 8 de agosto de 2019.

No que concerne à tardia entrada em vigor da aludida lei**,** importa salientar a celeuma que lhe antecedeu, em particular no que respeita ao Parecer da Comissão Nacional de Proteção de Dados (CNPD) à respetiva proposta de Lei 120/XIII/3.ª (GOV) [143].

Com efeito, no seguimento do Despacho n.º 7456/2017 da Ministra da Presidência e da Modernização Administrativa, de 17 de agosto de 2017[144], foi constituído um Grupo de Trabalho com o desiderato de preparar a legislação portuguesa para a aplicação do RGPD, tendo os trabalhos culminado na apresentação da proposta de lei 120/XIII/3.ª (GOV). Após publicação da proposta, foram solicitados e recebidos pareceres e contributos de diversas entidades, de entre as quais a CNPD, que apresentou o Parecer n.º 20/2018 e o seu contributo para a revisão do respetivo articulado. [145]

Por via do mencionado Parecer, a CNPD dirigiu inúmeras críticas ao legislador nacional, não só pela reprodução de normas do RGPD mas, também, pela incompatibilidade de parte destas com o direito da União decidindo, por conseguinte, com fundamento no princípio do primado do direito da União Europeia[146] e, nos demais argumentos elencados na deliberação, que irá futuramente desaplicar essas mesmas normas nos casos que venha a apreciar relativamente ao tratamento de dados e às condutas dos respetivos responsáveis ou subcontratantes.

Nesta conformidade, após a entrada em vigor da Lei 58/2019, de 8 de agosto a CNPD, por através da Deliberação 2019/494, de 3 de setembro[147], tornou pública a decisão de desaplicar um conjunto de normas que a integram e cuja aplicação, no seu entendimento, viola o RGPD.

No documento destaca a CNPD que, de modo a assegurar a transparência das decisões futuras e contribuir para a certeza e segurança jurídicas**,** aplicará diretamente as normas do RGPD porquanto o conjunto de normas da LE que entende desaplicar acham-se *"(…) manifestamente restringidas, contrariadas ou comprometidas no seu efeito útil*".[148]

Os artigos visados pela decisão são os seguintes: (i) artigo 2.º, n.º 1 e n.º 2 (Âmbito de aplicação); (ii) artigo 20.º, n.º 1 (Dever de segredo); (iii) artigo 23.º (Tratamento de

[143] Publicada no *Diário da Assembleia da República* (DAR), Série II A- número 89, de 26 de março de 2018, pp. 30-48, disponível em: Debates Parlamentares - Diário 089, p. 30 (2018-03-26) (parlamento.pt) [acedido em 25.08.2023].
[144] Publicado em *Diário da República*, Série II, n.º 163/2017, de 24 de agosto de 2017.
[145] Ambos disponíveis em doc.pdf (parlamento.pt).
[146] Decorrente do artigo 8.º, n.º 4 da CRP, que estatui que "*As disposições dos tratados que regem a União Europeia e as normas emanadas das suas instituições, no exercício das respetivas competências, são aplicáveis na ordem interna, nos termos definidos pelo direito da União, com respeito pelos princípios fundamentais do Estado de direito democrático*.".
[147] Disponível no histórico de decisões da CNPD, in www.cnpd.pt [acedido em 16.03.2023].
[148] *Cfr.* Deliberação da CNPD n.º 2019/494, de 3 de setembro de 2019, p. 11-v, disponível no histórico de decisões da CNPD, in www.cnpd.pt [acedido em 16.03.2023].

dados pessoais por entidades públicas para finalidades diferentes); (iv) artigo 28.º, n.º 3, alínea a) (Relações laborais); (v) artigo 37.º, n.º 1, alíneas a), h) e k) e n.º 2 (Contraordenações); (vi) artigo 38.º, n.º 1, alínea b) e n.º 2 (Contraordenações graves); (vii) artigo 39.º, n.º 1 e 3 (Determinação da medida da coima); (viii) artigo 61.º, n.º 2 (Renovação do consentimento); e (ix) artigo 62.º, n.º 2 (Regimes de proteção de dados pessoais).

De acordo com o preconizado pela Autoridade em apreço, para além dos tribunais nacionais:

> "*(…) também as entidades administrativas estão obrigadas a desaplicar as normas nacionais que contrariam o direito da União Europeia, como o determinou expressamente o TJUE, no acórdão Fratelli Costanzo, que veio vincular todos os órgãos da Administração Pública ao dever de aplicar integralmente o direito da União afastando, se necessário, as disposições nacionais que constituam um obstáculo à plena eficácia das normas daquele direito*". [149]

Por último, da leitura das normas da Lei de execução nacional insta evidenciar algumas disposições específicas para o setor público, nomeadamente o disposto no artigo 26.º, que remete para o disposto na Lei n.º 26/2016, de 22 de agosto em matéria de acesso a documentos administrativos que contenham dados pessoais[150]; o artigo 44.º, n.º 2, onde se refere que "*(…) as entidades públicas, mediante pedido devidamente fundamentado, podem solicitar à Comissão Nacional de Proteção de Dados a dispensa da aplicação de coimas durante o prazo de três anos a contar da entrada em vigor da presente lei*" e o artigo 58.º que prevê que as orientações técnicas para a aplicação do RGPD pela administração direta e indireta do Estado sejam aprovadas por resolução do Conselho de Ministros, a qual pode recomendar a sua aplicação também ao setor empresarial do Estado.[151]

[149] *Ibidem,* pp.1-2.

[150] Não obstante as alterações supervenientes, a própria Lei n.º 58/2019, de 8 de agosto, altera o disposto no n.º 9 da Lei 26/2016 que passa a dispor que "*Sem prejuízo das ponderações previstas nos números anteriores, nos pedidos de acesso a documentos nominativos que não contenham dados pessoais que revelem a origem étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, dados genéticos, biométricos ou relativos à saúde, ou dados relativos à intimidade da vida privada, à vida sexual ou à orientação sexual de uma pessoa, presume-se, na falta de outro indicado pelo requerente, que o pedido se fundamenta no direito de acesso a documentos administrativos*".

[151] Como veio a suceder com a publicação da RCM n.º 41/2018, de 28 de março, p.p. 1424 – 1430, disponível em: Diário da República n.º 62/2018, Série I de 2018-03-28 [acedido em 18.03.2023], que define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais.

3.3. DADOS PESSOAIS:

3.3.1. DEFINIÇÃO LEGAL DE DADO PESSOAL

O artigo 4.º, n.º 1 do RGPD, define «dado pessoal» como a *"(…) informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)"* estabelecendo ainda, com recurso a exemplos, o que se entende por pessoa singular identificável.[152]
De acordo com o desiderato em apreço, toda e qualquer informação pessoal é tida por relevante e merecedora de proteção jurídica, independentemente da sua natureza. Para MENEZES CORDEIRO**,** este conceito, mesmo quando interpretado de modo flexível, extravasa o sentido que lhe foi tradicionalmente conferido no seio dos direitos de personalidade, nos termos do qual a vida privada abrange tudo o que não seja público e profissional ou social.[153] Para o Autor, o conceito de dado pessoal na aceção do RGPD abrange qualquer informação relativa à pessoa identificada ou identificável, incluindo todos os aspetos familiares ou sociais, privados ou públicos, físicos ou mentais[154], formato ou suporte em que se encontrem e, até, da sua veracidade ou falsidade. [155]
Nesse sentido, o Grupo de Trabalho do Artigo 29.º estabeleceu a existência de quatro "pilares" principais que podem ser distinguidos na definição de "dados pessoais", a saber: (i) "qualquer informação", (ii) "relativa a", (iii) "identificada ou identificável", (iv) "pessoa singular". Estes elementos estão intimamente ligados e apoiam-se uns nos outros, e juntos determinam se uma informação deverá ser ou não considerada como "dados pessoais". [156]

3.3.2. CONCEITO DE DADOS SENSÍVEIS

O n.º 1 do artigo 9.º do RGPD proíbe tratamento de dados pessoais o *"(…) que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados*

[152] *Cfr*. Artigo 4.º, n.º 1 do RGPD, *in fine*, onde se refere que "*(…) é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular*".
[153] CORDEIRO, A. Barreto Menezes - *Direito da Proteção de Dados (…), ob. cit.*, p. 108.
[154] Independentemente de serem dados objetivos ou factuais.
[155] *Ibidem*, pp. 108-109.
[156] Grupo de Trabalho para a Proteção de Dados instituído ao abrigo do Artigo 29.º, Parecer 4/2007 sobre o conceito de dados pessoais, WP 136, 20 de junho de 2007, p. 26.

biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa".

O preceito transcrito dá-nos, deste modo, a noção de dados sensíveis por referência a categorias específicas de informações pessoais que, pela sua natureza, são consideradas especialmente sensíveis e, portanto, merecedoras de proteção jurídica acrescida.

Essas categorias de dados são consideradas sensíveis porque seu tratamento pode implicar riscos significativos para os direitos e liberdades das pessoas, como discriminação, estigmatização ou violação da privacidade.[157]

Como refere o n.º 1 do artigo 9.º do RGPD, as categorias especiais de dados não devem ser objeto de tratamento, salvo quando se verifique a existência de uma base legal específica que permita o tratamento da informação sensível, designadamente nas situações elencadas no n.º 2 do mesmo dispositivo. Nesta conformidade, é lícito o tratamento de dados sensíveis, quando se constate a existência de: (i) consentimento explícito, i.e., se o titular dos dados der um consentimento claro e inequívoco para o tratamento dos seus dados sensíveis, esse tratamento pode ser realizado; (ii) obrigação legal, na medida em que em determinadas situações, o tratamento de dados sensíveis pode ser necessário para o cumprimento de obrigações jurídicas impostas ao responsável pelo tratamento dos dados; (iii) proteção de interesses vitais, quando o tratamento for necessário para proteger interesses vitais do titular dos dados ou de outra pessoa e o titular dos dados estiver física ou legalmente incapaz de dar o consentimento; (iv) finalidades relacionadas com a saúde, i.e., o tratamento de dados sensíveis relacionados à saúde pode ser permitido para fins de medicina preventiva, diagnóstico médico, prestação de cuidados de saúde ou tratamento médico, gestão de serviços de saúde, ou para fins de investigação científica ou estatística no domínio da saúde; (v) ações judiciais, nas situações em que o tratamento de dados sensíveis é necessário para o exercício ou defesa no âmbito de ações judiciais.[158]

[157] Sobre este assunto importa atender ao disposto no considerado (51) do RGPD que, para além de dar alguns exemplos do que pode ou não ser incluído na definição de dados sensíveis refere, ainda, que em determinadas situações, o tratamento de dados pessoais sensíveis pode ser justificado com base em interesse público, desde que sejam respeitados os direitos fundamentais e a essência do direito à proteção de dados. No entanto, o tratamento deve ser proporcional ao objetivo visado e deve ser acompanhado de medidas adequadas e específicas para garantir a proteção das informações sensíveis. O considerando destaca ainda a necessidade de estabelecer normas específicas para o tratamento de dados sensíveis, tendo em conta a natureza dos dados, as finalidades do tratamento e o respeito aos direitos fundamentais das pessoas. Essas normas devem garantir a proteção da natureza sensível dos dados pessoais, com base no segredo profissional ou em regras profissionais legalmente reconhecidas.

[158] Estas derrogações específicas à proibição geral de tratamento de categorias especiais de dados pessoais, tal como refere o considerando (52) do RGPD, deverão ser permitidas quando estiverem previstas no direito da União ou dos Estados-Membros e sujeitas a salvaguardas adequadas, de forma a proteger os dados pessoais e outros direitos fundamentais, caso tal seja do interesse público,

Do exposto resulta que o RGPD impõe requisitos mais exigentes para o tratamento dos dados sensíveis incluindo, entre outras, a necessidade de obter consentimento explícito do titular dos dados ou a constatação de existência de base legal específica para o concernente tratamento. Além disso, medidas adicionais de segurança e proteção devem ser implementadas para garantir a confidencialidade e a integridade dessas informações sensíveis.

3.4. OS PRINCÍPIOS QUE REGEM A PROTEÇÃO DE DADOS PESSOAIS

O RGPD, tal como sucede na maioria da legislação europeia, aborda a temática da proteção dos dados pessoais pelo estabelecimento de grandes princípios, que guiam e enquadram as demais normas regulamentares.

No artigo 5.º do RGPD estão consagrados os princípios que devem ser observados no tratamento de dados pessoais, mormente os princípios da licitude, da lealdade, da transparência; da limitação das finalidades; da minimização dos dados; da exatidão dos dados; da limitação da conservação; da integridade e da confidencialidade; e da responsabilidade.

Este artigo e a relação que estabelece com os artigos 6.º e 9.º do mesmo diploma, nas palavras de ALEXANDRE PINHEIRO, *"(…) operam verdadeiramente como a «Constituição do RGPD», tendo origem no artigo 5.º da Convenção 108 e no artigo 6.º da Diretiva 95/46/CE*." [159]

Toda a legislação sobre proteção de dados adotada pela União Europa ou pelo Conselho da Europa, após a entrada em vigor do RGPD, deve observar estes princípios[160], apenas sendo admissíveis restrições aos princípios relativos ao tratamento de dados na medida em que correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º do RGPD e seja respeitada a essência dos direitos

nomeadamente o tratamento de dados pessoais em matéria de direito laboral, de direito de proteção social, incluindo as pensões, e para fins de segurança, monitorização e alerta em matéria de saúde, prevenção ou controlo de doenças transmissíveis e outras ameaças graves para a saúde. Essas derrogações poderão ser previstas por motivos sanitários, incluindo de saúde pública e de gestão de serviços de saúde, designadamente para assegurar a qualidade e a eficiência em termos de custos dos procedimentos utilizados para regularizar os pedidos de prestações sociais e de serviços no quadro do regime de seguro de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos. Uma derrogação deverá também permitir o tratamento desses dados pessoais quando tal for necessário à declaração, ao exercício ou à defesa de um direito, independentemente de se tratar de um processo judicial ou de um processo administrativo ou extrajudicial.

[159] PINHEIRO, Alexandre [et al.] – *Comentário ao Regulamento (…), ob. cit.*, p. 205.

[160] É de salientar a Convenção Modernizada para a Proteção de Indivíduos em Relação ao Tratamento de Dados Pessoais, aprovada na 128ª Sessão do Comité de Ministros (Elsinore, Dinamarca, dias 17 e 18 de maio de 2018, pelo protocolo de alteração n.º 223 e designada por Convenção 108+, disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf [acedido em 18.04.2023].

e liberdades fundamentais. Podem ser estabelecidas derrogações e restrições a estes princípios, desde que reunidas três condições cumulativas, a saber: i) que as mesmas estejam previstas na lei; ii) prossigam um objetivo legítimo e iii) sejam necessárias numa sociedade democrática.[161]

3.4.1. PRINCÍPIO DO TRATAMENTO LÍCITO, LEAL E TRANSPARENTE («LICITUDE, LEALDADE E TRANSPARÊNCIA»)

O artigo 5.º, n.º 1, al. a) do RGPD, estabelece que os dados pessoais devem ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados. Este princípio agrega e conexiona as noções de tratamento lícito, leal e transparente, que devem ser aplicadas de forma integrada.

O princípio da licitude**,** *stricto sensu*, demanda que qualquer tratamento de dados pessoais tenha fundamento numa norma permissiva pressupondo, *lato sensu*, a observância da Lei, i.e., o cumprimento do RGPD e demais legislação nacional e comunitária.[162] Nesta conformidade, o tratamento de dados é lícito na medida em que os dados pessoais sejam objeto de tratamento tendo por base um fundamento de licitude, de entre os elencados no artigo 6.º do RGPD. Do exposto resulta que só é lícito o tratamento de dados que preencha, pelo menos, uma das seguintes condições: i) consentimento, i.e., "*O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas*" [cfr. Art.º 6.º, n.º 1, al. a)] [163]; ii) execução de um contrato, i.e., o tratamento seja "*(…) necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados*;" [cfr. Art.º 6.º, n.º 1, al. b)]; iii) cumprimento de uma obrigação jurídica, na medida em que o tratamento seja "*(…) necessário para o cumprimento de uma obrigação jurídica a que o responsável*

[161] Manual da Legislação Europeia sobre Proteção de Dados - Agência dos Direitos Fundamentais da União Europeia, Ed. 2018, Luxemburgo: Serviço das Publicações da União Europeia, 2022. ISBN 978-92-871-9825-9, p. 133. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_pt.pdf. [acedido em 18.04.2023].

[162] CORDEIRO, A. Barreto Menezes [et al.] - Comentário ao regulamento geral de proteção de dados e à Lei nº 58/2019. - Coimbra: Almedina, 2021. p. 102;

[163] Sobre o assunto importa referir que o n.º 11) do art.º 4.º do RGPD define «Consentimento» do titular dos dados como *"uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;*" e o n.º 2 do art.º 7.º do mesmo diploma alude às condições aplicáveis ao consentimento definindo que "*Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples.*" Por seu turno, o n.º 3 do mesmo dispositivo prescreve que *"O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento.".*

pelo tratamento esteja sujeito;" [cfr. Art.º 6.º, n.º 1, al. c)] [164]; iv) defesa de interesses vitais, quando o tratamento seja "*(…) necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular*;" [cfr. Art.º 6.º, n.º 1, al. d)]; v) exercício de funções de interesse público ou exercício da autoridade pública, na media em que o tratamento seja "*necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento*;" [cfr. Art.º 6.º, n.º 1, al. e)]; [165] vi) interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, nas situações em que o tratamento seja:

> "*(…) necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança* [cfr. Art.º 6.º, n.º 1, al. f)].

Mais dispõe o n.º 1 do artigo 6.º do RGPD, *in fine*, que o prescrito pela alínea f) não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições. Esta alínea sublinha a importância do princípio da legalidade na prossecução das atribuições das entidades públicas. Daqui resulta que o tratamento de dados pelas autoridades públicas assenta na existência de um ato legislativo donde resulte, por via das atribuições das autoridades públicas, a necessidade do tratamento de dados pessoais. [166]

Associado ao princípio da licitude acha-se o princípio da transparência[167], taxativamente previsto no artigo 5.º, n.º 1, al. a) do RGPD e que abrange todo o

[164] De acordo com o disposto no art.º 6.º, n.º 3 do RGPD, o fundamento jurídico para o tratamento referido no n.º 1, alíneas c) e e) do n.º 1 do mesmo dispositivo, é definido: a) Pelo direito da União; ou b) Pelo direito do Estado-Membro ao qual o responsável pelo tratamento está sujeito. A finalidade do tratamento é determinada com esse fundamento jurídico ou, no que respeita ao tratamento referido no n.º 1, alínea e), [i.e., exercício de Funções de Interesse Público ou Exercício da Autoridade Pública], deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. Esse fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento em conformidade com o capítulo IX. O direito da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido.

[165] *Vd.* nota anterior.

[166] *Cfr.* Art.º 3.º, n.º 2 e artigo 266.º, n.º 2, ambos da CRP e artigo 3.º do CPA.

[167] De acordo com as Orientações relativas à transparência na aceção do Regulamento 2016/679, do Grupo de trabalho do artigo 29.º, adotadas em 29 de novembro de 2017 e revistas e adotadas pela última vez em 11 de abril de 2018, p. 5. Disponível em: ARTICLE29 - Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) (europa.eu) [acedido em 20.04.2023]., a transparência é um dos elementos há muito consagrados no direito da EU e visa criar confiança nos processos que afetam os cidadãos fazendo com que estes compreendam e, se necessário, se oponham a esses processos. A transparência constitui uma expressão do princípio da lealdade em relação ao tratamento dos dados pessoais enunciado no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia.

processo de tratamento de dados pessoais "*(…) desde os primeiros contactos (formação), passando pela sua recolha e demais tratamentos (execução), até mesmo após o termo da relação (…)* [abrangendo] *o conteúdo das informações transmitidas aos titulares ou a terceiros, como os procedimentos a adotar nessa transmissão*". [168]

Este princípio é passível de ser observado em inúmeros artigos do RGPD, em particular, nos artigos 12.º, 13.º e 14.º ou ainda nos artigos 34.º e 37.º, donde se extrai que as informações ou comunicações relacionadas com o tratamento dos dados pessoais devem ser transmitidas de um modo conciso, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples[169]. Importa referir que o considerando (39) do RGPD destaca que o princípio da transparência respeita, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento, à(s) finalidade(s) do tratamento e à salvaguarda o seu direito a obter a confirmação e a comunicação dos concernentes dados pessoais alvo de tratamento. Do propósito do princípio da transparência decorre, ainda, que as pessoas singulares a quem os dados dizem respeito devem ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento.[170]

Em estreita ligação com o princípio anteriormente referido encontra-se o princípio da lealdade, também previsto no artigo 5.º, n.º 1, al. a) do RGPD, que significa que, no decurso do tratamento de dados, o responsável pelo tratamento deve dar a conhecer ao titular dos dados, de modo claro, conciso e numa linguagem facilmente compreensível os riscos, as regras e os direitos do titular. No cumprimento deste princípio relevam não só os artigos 13.º e 14.º do RGPD, que aludem às informações a prestar junto do titular dos dados, mas também, entre outros, os 15.º, 21.º, 24.º e 30.º que versam, respetivamente, sobre os direitos de acesso e de oposição, à responsabilidade do RT e à necessidade de elaborar e conservar um registo de atividades de tratamento.

Em suma, o princípio da lealdade *"(…) está relacionado com o desenvolvimento do tratamento dos dados pessoais com respeito por uma relação de equilíbrio entre responsáveis e subcontratantes e titulares dos dados pessoais*"[171], evidenciando a

[168] CORDEIRO, A. Barreto Menezes [et al.] - *Comentário ao regulamento (…), ob cit, p. 103.*
[169] *Cfr*. Artigo 12.º, n.º 1 do RGPD.
[170] Para uma maior compreensão do significado, elementos e requisitos da transparência, sugere-se a leitura das mencionadas orientações sobre a transparência na aceção do RGPD.
[171] PINHEIRO, Alexandre [et al.] – *Comentário ao Regulamento (…), ob. cit.*, p. 207.

importância da transparência, da ética e da responsabilidade assumida pelas entidades que procedem à recolha e tratamento dos dados pessoais, assegurando que os titulares dos dados tenham consciência e controlo sobre as suas informações pessoais.

3.4.2. PRINCÍPIO DA «FINALIDADE» OU DA «LIMITAÇÃO DAS FINALIDADES»

O artigo 5.º, n.º 1 al. b) do RGPD determina que os dados pessoais devem ser:

> "*Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»);"*.

Do exposto decorre que as finalidades do tratamento devem reunir os seguintes requisitos: i) ser determinadas, ii) ser explícitas e iii) ser legítimas e, os dados não podem ser tratados posteriormente de uma forma incompatível com essas finalidades, sem prejuízo da viabilidade de tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica, ou para fins estatísticos.

Para MENEZES CORDEIRO, a determinação das finalidades deve anteceder o processo de tratamento, não podendo o seu reconhecimento ficar por realizar ou ser adiado ou condicionado a um evento futuro nem tão-pouco o preenchimento do quesito da «finalidade determinada» pode der efetuado com recurso a expressões vagas. Ao exposto acresce que, para que sejam explícitas**,** devem ser, também, conhecidas dos interessados, sob pena de se verificar a violação do princípio da transparência, devendo a expressão «legítimas», ser interpretada de modo amplo, i.e., no sentido de que não basta apenas o cumprimento das condições de licitude previstas no artigo 6.º do RGPD, e sim, de todas as disposições legais aplicáveis. [172]

Este princípio assume especial relevância porquanto**,** após conhecida a finalidade do tratamento**,** é possível apurar se a informação pessoal recolhida é necessária e não excessiva, cumprindo com os requisitos do princípio da minimização dos dados, adiante melhor explanado.

Por último, importa ainda evidenciar que de acordo com o considerando (50) do RGPD, o tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos "*(…) apenas deverá ser*

[172] *Vd*. CORDEIRO, A. Barreto Menezes [et al.] - *Comentário ao regulamento (…), ob cit, p. 103.*

autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos". Para apurar da aludida compatibilidade deve atender-se, entre outros, à existência de uma ligação entre a primeira finalidade e aquela a que se destina a nova operação de tratamento que se pretende efetuar, o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação com o RT; à natureza dos dados pessoais; às consequências que o posterior tratamento dos dados pode ter para o seu titular; e à existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas.

Sem prejuízo do que antecede, importa ter em consideração que o tratamento subsequente para fins de interesse público, de investigação científica, histórica ou para efeitos estatísticos não é considerado, nos termos do artigo 5.º do RGPD, contrário ao princípio da limitação das finalidades.

3.4.3. PRINCÍPIO DA «MINIMIZAÇÃO DOS DADOS»

Previsto no artigo 5.º, n.º 1, al. c) do RGPD, de acordo com o princípio da minimização dos dados, os dados pessoais tratados devem ser *"*[a]*dequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»)".* O normativo indica que apenas devem ser tratados os dados pessoais que sejam relevantes e estritamente necessários para cumprimento da finalidade para a qual são tratados.

Este princípio está associado ao princípio da limitação das finalidades, já previsto na Diretiva 95/46/CE[173], tendo, no entanto, assumido uma redação mais clara, uma vez que a expressão "não excessivos" foi substituída por "limitados ao que é necessário".

O princípio da minimização compõe-se em três pilares; i) adequação; ii) pertinência; e iii) necessidade. O primeiro demanda a delimitação dos tratamentos aos dados pessoais que se enquadrem nas finalidades prosseguidas, excluindo-se, desde logo, os dados não relacionados ou inapropriados. O segundo, circunscreve as atividades dos responsáveis a tratamentos que possam contribuir para a prossecução dessas finalidades e, de acordo com o último, o tratamento dos dados apenas será legítimo

[173] *Cfr.* al. c) do n.º 1 do artigo 6.º da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, *cit.* p. 40.

caso não exista um método alternativo menos invasivo, nomeadamente os previstos nos artigos 32.º, n.º 1 (anonimização) ou 25.º, n.º 1 (pseudonomização).[174]

3.4.4. PRINCÍPIO DA EXATIDÃO

O artigo 5.º, n.º 1, al. d) do RGPD prescreve que os dados pessoais devem ser "*Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»)*".

O princípio da exatidão compreende três dimensões: i) a proibição de recolher ou armazenar dados incorretos; ii) o dever de atualização dos dados detidos, sempre que se mostre necessário; e iii) o dever de apagar ou de retificar os dados incorretos, à luz das finalidades prosseguidas.[175]

Do exposto decorre que um responsável pelo tratamento que conserve dados pessoais não deve utilizar essas informações sem adotar medidas para se certificar, com um grau de certeza razoável, que os dados são exatos e estão atualizados, sendo que a obrigação de assegurar a exatidão dos mesmos é interpretada no contexto da finalidade do tratamento dos dados.[176]

O TJUE, no Acórdão *Rijkeboer*[177], remetendo para o preâmbulo da Diretiva 95/46/CE - [a qual refere que o titular de direitos deve dispor de um direito de acesso aos dados que lhe dizem respeito para poder verificar se os dados estão corretos] -, declarou que:

> "*o direito ao respeito da vida privada implica que a pessoa em causa possa assegurar-se de que esses dados pessoais são tratados com exatidão e de forma lícita, ou seja, em especial, que os dados de base que lhe dizem respeito são exatos e são enviados a destinatários autorizados"*.

3.4.5. PRINCÍPIO DA LIMITAÇÃO DE CONSERVAÇÃO

O artigo 5.º, n.º 1, al. e) do RGPD[178] preceitua que os dados pessoais devem ser:

> "*Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os*

[174] Cfr. CORDEIRO; António Menezes - *Direito da proteção de dados (…), ob. cit.,* p. 159.
[175] *Ibidem*.
[176] Manual da Legislação Europeia sobre Proteção de Dados *ob cit*., p. 145.
[177] TJUE, acórdão de 7 de maio de 2009 no processo C-553/07, College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=74028&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=597837 [acedido em 18.06.2023].
[178] Tal como no como o artigo 5.º, alínea e), da Convenção n.º 108.

> *dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»)".*

Este princípio remete-nos para a necessidade de limitar temporalmente o tratamento dos dados, tendo em conta finalidades do tratamento, após o que devem os mesmos ser eliminados. Nesse sentido, o responsável pelo tratamento deve fixar os prazos para o apagamento ou para a sua revisão periódica, assegurando a sua conservação apenas durante o período estritamente necessário à prossecução da finalidade para a qual foram recolhidos e tratados, salvo quando tratados para os fins previstos no artigo 89.º, n.º 1 do RGPD. Nestas situações, compete ao responsável pelo tratamento adotar as medidas técnicas e organizativas necessárias para salvaguardar os direitos e liberdades do titular dos dados. [179]

Sem prejuízo do que antecede, importa referir que a limitação temporal do armazenamento de dados pessoais apenas se aplica aos dados conservados de modo que permitam a identificação dos respetivos titulares sendo, todavia, legítimo o armazenamento dos dados que já não são necessários, com recurso à anonimização. Os dados para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos podem ser conservados durante períodos mais longos, desde que os referidos dados sejam utilizados exclusivamente para os fins acima referidos[180]. Devem ser estabelecidas medidas técnicas e organizativas adequadas para a conservação em curso e para a utilização de dados pessoais para salvaguardar os direitos e liberdades do titular dos dados. [181]

3.4.6. PRINCÍPIO DA «INTEGRIDADE E CONFIDENCIALIDADE» OU DA «SEGURANÇA» DOS DADOS

O artigo 5.º, n.º 1, al. f) do RGPD dispõe que os dados pessoais devem ser "*Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou*

[179] CORDEIRO; António Menezes - Direito de proteção de dados (…), ob. cit., p. 160.
[180] Cfr. Artigo 5.º, n.º 1, alínea e) do RGPD e artigos 5.º, n.º 4, al. b), e 11.º, n.º 2 da Convenção n.º 108 modernizada.
[181] Manual da Legislação Europeia sobre Proteção de Dados *ob cit.*, p. 148.

danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»)".[182]

Este princípio demanda a aplicação de medidas técnicas e organizativas adequadas aquando do tratamento de dados pessoais para os proteger contra o acesso, utilização, modificação, divulgação, perda, destruição ou danificação acidentais, não autorizados ou ilícitos.

Por conseguinte, o artigo 32.º, n.º 1 do RGPD refere que, ao aplicar as medidas técnicas ou organizativas adequadas, o responsável pelo tratamento e o subcontratante têm em consideração as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, que, dependendo do caso, podem incluir, designadamente, a pseudonimização[183] e a cifragem de dados pessoais e/ou o teste e a avaliação regular das medidas para garantir a segurança do tratamento dos dados.

O n.º 56 do relatório explicativo da Convenção n.º 108 modernizada elenca outras possibilidades de garantias adequadas, tais como, a implementação de uma obrigação de sigilo profissional, ou a adoção de medidas de segurança especiais de ordem técnica como a cifragem dos dados.[184]

Da leitura dos artigos 7.º, n.º 2 da Convenção 108+ e artigos 33.º e 34.º do RGPD retira-se que**,** ao aplicar medidas de segurança específicas, o responsável pelo tratamento ou o subcontratante deve ter em conta diversos elementos, mormente, (i) a natureza e o volume dos dados pessoais tratados; (ii) as potenciais consequências prejudiciais para os titulares dos dados; (iii) a necessidade de restringir o acesso aos dados; (iv) os métodos e técnicas mais avançados de tratamento dos dados na implementação de medidas de segurança adequadas; (v) o custo, que deve ser

[182] No mesmo sentido dispõe o considerando (39) do RGPD e artigo 7.º da Convenção n.º 108 modernizada.

[183] O conceito de «pseudonimização» vem definido no artigo 4.º, n.º 5 do RGPD como "o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável".

[184] "*In order to prevent adverse effects for the data subject, processing of sensitive data for legitimate purposes needs to be accompanied by appropriate safeguards (which are adapted to the risks at stake and the interests, rights and freedoms to be protected), such as for instance, alone or cumulatively; the data subject's explicit consent; a law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be permitted; a professional secrecy obligation; measures following a risk analysis; a particular and qualified organisational or technical security measure (data encryption, for example)*". Cfr. Convention 108 + - Convention for the protection of individuals with regard to the processing of personal data. Explanatory report, p. 21. Disponível em: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf [acedido em 21.06.2023].

proporcionado à gravidade e probabilidade dos potenciais riscos; e (vi) a necessidade de revisão periódica das medidas de segurança.[185]

3.4.7. PRINCÍPIO DA RESPONSABILIDADE

O artigo 5.º, n.º 2 do RGPD preceitua que "[o] *responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo («responsabilidade»).*", consagrando o princípio da responsabilidade.

O preceito acomete dois deveres distintos ao responsável pelo tratamento: (i) atuar sempre no estrito cumprimento dos princípios elencados no artigo 5.º, n.º 1; e (ii) conseguir demonstrar o cumprimento desses princípios, em particular perante a autoridade de controlo e os tribunais. [186]

O artigo 24.º, n.º 1, do RGPD acrescenta que:

> *"(…) tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis", cabe ao responsável pelo tratamento aplicar "as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o Regulamento*".

Nas palavras de MENEZES CORDEIRO[187], as expressões inglesas *accountability* e *compliance* permitem ter uma noção mais clara do objetivo e da relevância deste princípio, aferível ou previsto em alguns normativos do RGPD, v.g., artigos 24.º, n.º 1, 30.º (Registo das atividades de tratamento) ou 33.º (Notificação de uma violação de dados pessoais à autoridade de controlo).

A nível internacional, o princípio da responsabilidade, no âmbito da temática da proteção de dados, foi originalmente mencionado nas *Guidelines* da OCDE, adotadas em 23 de setembro de 1980 [188] tendo a sua relevância vindo:

> *"(…) a ser discutida em inúmeros fóruns internacionais dedicados à matéria de proteção de dados. Em especial, destaca-se a Opinion 3/2010 on the principle of accountability, emitida pelo "Grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais" contemplado no artigo 29.º da Diretiva 95/46/CE (G29)20, na qual foi defendida a introdução deste princípio na revisão do regime geral*

[185] Manual da Legislação Europeia sobre Proteção de Dados *ob cit*., p. 152.
[186] CORDEIRO; António Menezes - *Direito de proteção de dados (…),* ob. cit., p. 161.
[187] *Ibidem*
[188] Cfr. Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais ("Diretrizes sobre a Privacidade"), disponíveis em: https://www.oecd.org/sti/ieconomy/15590254.pdf [acedido em 21.06.2023].

de proteção de dados, com o objetivo de reafirmar e reforçar a responsabilidade do responsável pelo tratamento." [189]

Não se trata, porém, de vincular os responsáveis pelo tratamento a um novo princípio – que já existia por força da necessidade da aplicação de medidas que protejam a privacidade – mas o de promover a adoção de medidas práticas e concretas que assegurem o efetivo cumprimento dos princípios já existentes.[190]

Por outro lado, o dever de comprovar o cumprimento do RGPD não consubstancia uma inversão do ónus da prova. Na eventualidade de o Responsável pelo Tratamento não o conseguir fazer, será apenas responsável pelo incumprimento do dever de comprovar.[191]

3.5. DIREITOS DOS TITULARES DOS DADOS

Os diversos artigos que compõe o Capítulo III do RGPD, sob a epígrafe, «*Direitos dos Titulares dos Dados»* concretizam explicitamente os direitos que assistem às pessoas singulares no tratamento dos seus dados pessoais. Sem prejuízo, os três primeiros artigos do citado capítulo corporizam não apenas direitos, mas também deveres do responsável pelo tratamento[192].

Quando o titular dos dados exerce algum dos direitos previstos nos artigos 15.º a 22.º[193] do RGPD, o responsável pelo tratamento deve, sem demora injustificada e no prazo de um mês a contar da data da receção do pedido, fornecer as informações sobre as medidas tomadas no exercício desses direitos. No entanto, o prazo pode ser prorrogado até dois meses, pela complexidade e o número de pedidos (n.º 3 do art.º 12.º do RGPD). O mesmo sucede quando o responsável pelo tratamento não der seguimento ao pedido efetuado pelo titular (n.º 4 do presente artigo). As comunicações entre o responsável pelo tratamento e o titular dos dados, relacionadas com o exercício dos direitos devem ser fornecidas gratuitamente. Não obstante, em casos de pedidos manifestamente infundados ou excessivos, o responsável pelo tratamento

[189] *Cfr.* LOPES, Teresa Vale – Responsabilidade e Governação das Empresas no âmbito do novo Regulamento sobre a Proteção de Dados, Anuário da Proteção de Dados 2018, Coord. Francisco Pereira Coutinho / Graça Canto Moniz. Universidade Nova de Lisboa. Faculdade de Direito. CEDIS, Centro de I & D sobre Direito e Sociedade, Lisboa. 2018, p. 52.

[190] Ibidem, p. 53.

[191] CORDEIRO; António Menezes - *Direito de proteção de dados (…),* ob. cit., p. 162.

[192] Nomeadamente os artigos 12.º (Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados), 13.º (Informações a facultar quando os dados pessoais são recolhidos junto do titular) e 14.º (Informações a facultar quando os dados pessoais não são recolhidos junto do titular), todos do RGPD.

[193] Pese embora a versão portuguesa mencione o artigo 20.º ao invés do 22.º, considerando as versões dos demais países, parece tratar-se de lapso de escrita.

pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos ou a recusar o seguimento ao pedido (n.º 5 do art.º 12.º do RGPD).

3.5.1. DIREITO À INFORMAÇÃO

O titular dos dados tem o direito de obter informação relativa ao modo como os seus dados pessoais são usados e sobre os seus direitos, de forma clara, transparente e facilmente compreensível (*cfr*. art.º 12.º do RGPD). Esta disposição concretiza o «novo» princípio da transparência, introduzido no artigo 5.º, n.º 1, al. a), apenso aos princípios da licitude e lealdade, o qual remete não para o acesso à informação, mas para a transmissão de informação de acordo com os critérios da compreensibilidade, conforme dispõe o considerando (58).[194]

Ainda que não estabeleça um procedimento estritamente formal, o artigo 12.º do RGPD, aduz os elementos da transparência, exigindo que o responsável pelo tratamento adote as medidas adequadas na transmissão de qualquer comunicação a respeito do tratamento e que a mesma seja prestada de modo (i) conciso, (ii) transparente; (iii) inteligível; (iv) de fácil acesso; e (v) utilizando uma linguagem clara e simples.[195]

Essas informações podem ser prestadas por meios escritos, eletrónicos ou orais (art.º 12.º, n.º 1), devendo o responsável pelo tratamento facilitar o exercício dos direitos a que aludem os artigos 15.º a 22.º (art.º 12.º, n.º 2) devendo, mediante pedido do titular, o responsável informar as medidas tomadas, no prazo máximo de um mês, prorrogável nos termos do prescrito pelo artigo 12.º, n.º 3. Estas informações são tendencialmente gratuitas, salvo solicitação de cópias adicionais ou quando os pedidos sejam manifestamente infundados ou excessivos (art.º 12.º, n.º 5).

Adiante, os artigos 13.º e 14.º do RGPD concretizam, respetivamente, o conteúdo mínimo das informações sobre o tratamento dos dados, que devem ser facultadas no momento da sua recolha junto do titular[196] ou, não sendo esta efetuada junto do mesmo, dentro de um prazo variável, consoante as circunstâncias do caso. Estes artigos comungam da mesma *ratio* e fundamentos dogmáticos porquanto ambos respeitam ao dever de informação, que decorre do direito à autodeterminação e

[194] PINHEIRO, Alexandre Sousa et al. **-** Comentário ao Regulamento (…), ob.cit., p. 341.
[195] CORDEIRO; António Menezes – Comentário ao Regulamento (…), ob.cit., p. 149.
[196] Designadamente as mencionadas no artigo 13.º, n.º 1, al. a) a f), donde se destacam, a título exemplificativo, a identidade e os contactos do responsável pelo tratamento ou do seu representante; os contactos do encarregado da proteção de dados; as finalidades do tratamento e o fundamento jurídico que subjaz ao tratamento; interesses legítimos do responsável pelo tratamento ou de um terceiro; os destinatários ou categorias de destinatários dos dados. O n.º 2 do mesmo artigo enumera ainda outras informações adicionais, necessárias para garantir um tratamento equitativo e transparente.

constituem um corolário do n.º 2 do artigo 8.º da Carta, encontrando, de igual modo, guarida no artigo 35.º da CRP.[197]

A tabela infra sumariza e distingue as exigências dos artigos 13.º e 14.º:

Tabela 1 - Informações a prestar ao titular no momento da recolha dos dados pessoais

	RECOLHA DIRETA (ARTIGO 13.º)	**RECOLHA INDIRETA (ARTIGO 14.º)**
QUE INFORMAÇÃO?	Identidade e os contactos do responsável pelo tratamento e/ou do seu representante	
	Se a comunicação de dados constitui ou não uma obrigação legal ou contratual e as eventuais consequências de não fornecer esses dados	
	Os contactos do encarregado da proteção de dados (DPO)	
	As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento	
	Os destinatários ou categorias de destinatários dos dados pessoais, se os houver	
	Prazo de conservação	
	A transferência para países terceiros, se aplicável	
	A existência do direito de acesso, retificação, apagamento e limitação do tratamento	
	Se o tratamento se basear no consentimento, a informação que pode retirar o consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado	
	A existência do direito de não sujeição a decisões automatizadas, incluindo a definição de perfis	
	O direito à portabilidade dos dados	
	O direito ao conhecimento da existência de uma violação de dados	
		Fontes dos dados
	Direito a reclamar a uma autoridade de controlo	
TIPO DE TRATAMENTO?	Tratamento inicial e eventual tratamento posterior	
QUANDO?	No momento da recolha	No momento da recolha, caso esta tenha sido feita mediante o preenchimento de formulário eletrónico on-line; Num prazo razoável após receção dos dados (nunca superior a 30 dias ou aquando do primeiro contacto com o titular dos dados)
COMO?	Informação concisa, transparente, clara e precisa; Por escrito ou qualquer outro meio adequado	
NEM SEMPRE É NECESSÁRIO	O titular já tem acesso a toda a informação	
		Quando a prestação da informação não é possível ou exige esforços desproporcionais

Fonte: **MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão (2017)**[198]

3.5.2. DIREITO DE ACESSO

O artigo 15, n.º 1 do RGPD prescreve que o titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam

[197] CORDEIRO; António Menezes – *Comentário ao Regulamento (…),* ob. cit., p. 159.
[198] Conteúdo extraído e adaptado de MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão – *Regulamento geral de Proteção de Dados – Manual Prático.* Lisboa: Vida Económica Editorial. 2017, pp. 27-28.

respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos mesmos, bem como a outras informações legalmente previstas. [199]

Este direito[200], pela sua relevância, é distinguido como o principal direito do titular dos dados, na medida em que permite o exercício de outros direitos, mormente os direitos de retificação, apagamento, limitação do tratamento, portabilidade e oposição.[201]

Importa, também referir que este direito desdobra-se em diversos direitos menores e inerentes obrigações de cumprimento pelo responsável pelo tratamento[202], i.e., (i) direito de aceder aos dados pessoais objeto de tratamento[203]; (ii) direito de obter um conjunto de informações acessórias a esse tratamento[204]; (iii) direito à informação das garantias adequadas, quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional e (iv) o direito à obtenção de cópias dos dados pessoais.[205]

Na resposta a um pedido de acesso, o responsável pelo tratamento deve facultar informações referentes à origem dos dados tratados quando os mesmos não tenham sido recolhidos junto do titular e na medida em que tais informações estejam disponíveis e não tenham sido eliminadas com o objetivo de eximir à comunicação. Esta obrigação decorre dos princípios da lealdade, da transparência e da responsabilidade.[206]

Conforme fixado pela jurisprudência do TJUE, como é exemplo o Acórdão Rijkeboer[207], visando garantir o efeito útil dos direitos conferidos aos titulares dos dados, entendeu-se que o direito em questão:

---

[199] São elas as fixadas nas alíneas a) a h) do mesmo dispositivo legal, a saber: *a) As finalidades do tratamento dos dados; b)As categorias dos dados pessoais em questão; c)Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; f)O direito de apresentar reclamação a uma autoridade de controlo; g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados; h)A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados."*

[200] Também previsto no n.º 1 do artigo 35.º da CRP, à semelhança do direito à retificação e atualização e o direito ao conhecimento sobre a finalidade da recolha e tratamento dos dados pessoais.

[201] PINHEIRO, Alexandre Sousa et al. - Comentário ao Regulamento Geral de Proteção de Dados. Coimbra: Edições Almedina, 2018, p. 359.

[202] Que deve fornecer um conjunto de informações específicas acerca do tratamento, designadamente as previstas nas alíneas a) a h) do n.º 1 do art. 15.º do RGPD.

[203] n.º 1 do art. 15.º do RGPD

[204] artigos 13.º e 14.º do RGPD

[205] *Ibidem*, p. 360.

[206] Manual da Legislação Europeia sobre Proteção de Dados *ob cit*., p. 247.

[207] Conforme o já citado Acórdão do TJUE, de 7 de maio de 2009, no âmbito do processo C-553/07.

> *"(…) deve necessariamente abranger o passado. Com efeito, se assim não fosse, a pessoa interessada não estaria em condições de eficazmente exercer o seu direito de obter a retificação, supressão ou bloqueio dos dados que se presume serem ilícitos ou incorretos ou de intentar uma ação em justiça e de ser ressarcida pelo prejuízo sofrido*".

Trata-se de um direito que não comporta exceções, salvo quanto ao previsto n.º 4 do artigo 15.º e considerando (63), ambos do RGPD[208], relativamente à possibilidade do seu exercício colidir, de forma desproporcionada, com direitos e liberdades de terceiros.

3.5.3. DIREITO DE RETIFICAÇÃO

Nos termos do artigo 16 do RGPD, o titular dos dados tem o direito de obter:

> "*(…) sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional*."

O direito à retificação acha-se associado ao princípio da exatidão, previsto no artigo 5.º, n.º 1, al. d) do RGPD e abrange (i) o direito a exigir, sem demora injustificada, a retificação dos dados inexatos; (ii) o direito a, atendendo às finalidades do tratamento, exigir que os dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.[209]

Sobre o assunto, o considerando (39), *in fine*, prescreve que, no sentido de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deve fixar os prazos para o apagamento ou a revisão periódica, bem como adotar "*(…) todas as medidas razoáveis para que os dados pessoais inexatos sejam retificados ou apagados."*

Na persecução da supramencionada revisão periódica ou no momento em que tal se justifique, o titular dos dados solicita a retificação dos seus dados junto do responsável pelo tratamento, mediante pedido, acompanhado da documentação justificativa correspondente (*Vd*. considerandos (59) e (65)).[210] A respeito dos pedidos de retificação cumpre evidenciar que no Acórdão *Cemalettin Canli c. Turquia*[211], o

[208] Que referem, respetivamente que "*O direito de obter uma cópia a que se refere o n.º 3 não prejudica os direitos e as liberdades de terceiros*" e que "(…) *Esse direito não deverá prejudicar os direitos ou as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software*."
[209] CORDEIRO; António Menezes - *Direito de proteção de dados (…),* ob. cit., p. 269-270.
[210] PINHEIRO, Alexandre Sousa et al. - *Comentário ao Regulamento (…),* ob. cit., p. 363.
[211] TEDH, Acórdão *Cemalettin Canli c.* Turquia de 18 de novembro de 2008, petição n.º 22427/04, n.ºs 33 e 42 a 43, disponível em: CEMALETTİN CANLI c. TURQUIE (N° 2) (coe.int) [acedido em 20.07.2023]

requerente e titular dos dados solicitou a alteração do relatório e dos registos policiais respeitantes a anteriores processos penais que não resultaram qualquer condenação, tendo o seu pedido sido indeferido. Sem prejuízo, o TEDH entendeu que as informações constantes do relatório policial estavam abrangidas pelo âmbito do artigo 8.º da CEDH, uma vez que as informações públicas sistematicamente recolhidas e armazenadas em arquivos detidos pelas autoridades também podem estar abrangidas pelo conceito de «vida privada».

Insta, por último, salientar que de acordo com o disposto no artigo 19.º do RGPD, sob a epígrafe «*Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento*»[212]**,** é salvaguarda a necessidade de a retificação ser comunicada a cada terceiro destinatário dos dados, salvo se essa comunicação for impossível ou implicar um esforço desproporcionado.

3.5.4. DIREITO AO APAGAMENTO DOS DADOS («DIREITO A SER ESQUECIDO»)

O artigo 17.º, n.º 1 do RGPD dispõe que, verificadas determinadas situações[213], o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais e este tem a obrigação o fazer, sem demora injustificada.

Subjacente à obrigação de apagamento está, assim, a inexistência de qualquer fundamento que sustente o tratamento, i.e., quando: (i) se acha alcançada a finalidade do tratamento (na prossecução dos princípios da minimização dos dados e da limitação da conservação); ii) o consentimento do titular é revogado[214]; (iii) o titular se opõe ao tratamento, não existindo interesses legítimos prevalecentes ou os dados são tratados para efeitos de comercialização direta; (iv) quando o tratamento não está

[212] Onde se dispõe que "*O responsável pelo tratamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido em conformidade com o artigo 16.º, o artigo 17.º, n.º 1, e o artigo 18.º, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. Se o titular dos dados o solicitar, o responsável pelo tratamento fornece-lhe informações sobre os referidos destinatários*."

[213] Previstas no artigo 17.º, n.º 1, alíneas a) a f), designadamente quando: "*a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2; d) Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1.".*

[214] Contrariamente ao que sucede com os direitos de personalidade, a revogação do consentimento pelo titular dos dados não o obriga a indemnizar os prejuízos causados às legitimas expectativas da outra parte (cf. artigo 81.º. n.º 2 do CC).

sustentado num dos fundamentos de licitude previstos no artigo 6.º do RGPD; (v) o apagamento resulte de uma obrigação legal.

Quando os dados tiverem sido tornados públicos, nos termos do artigo 17.º, n.º 2 do RGPD, o titular tem o direito de exigir ao responsável pelo tratamento que informe os demais responsáveis que lhes foi solicitado o apagamento das ligações[215] para esses dados, bem como o apagamento de eventuais cópias ou reproduções.

Para MENEZES CORDEIRO[216], o artigo 17.º parece consagrar dois direitos: (i) ao apagamento (art.º 17.º, n.º 1) e (ii) um direito *sui generis*[217] ao esquecimento (art.º 17.º, n.º 2), emergindo este último como o reconhecimento da insuficiência do apagamento em face das especificidades da internet.

Atento o disposto no artigo 19.º do RGPD («*Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento*»), é salvaguarda a necessidade de comunicação do apagamento a cada terceiro, a quem os dados tenham sido transmitidos, salvo se essa comunicação for impossível ou implicar um esforço desproporcionado.

Importa, todavia, salientar que o artigo 17.º, n.º 3 do RGPD prevê exceções ao direito a ser esquecido, abrangendo as situações em que o tratamento de dados pessoais seja necessário: (i) ao exercício da liberdade de expressão e de informação; (ii) ao cumprimento de uma obrigação legal que exija o tratamento previsto pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; (iii) por motivos de interesse público no domínio da saúde pública; (iv) para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos; (v) para efeitos de declaração, de exercício ou de defesa de um direito num processo judicial.

---

[215] Relativamente aos dados pessoais publicados em jornais oficiais, importa atender às condições previstas no artigo 25.º da Lei n.º 58/2019, de 8 de agosto, em particular o disposto nos respetivos números 4 e 5, que dispõem que "*4 - O direito ao apagamento de dados pessoais publicados em jornal oficial tem natureza excecional e só se pode concretizar nas condições previstas no artigo 17.º do RGPD, nos casos em que essa seja a única forma de acautelar o direito ao esquecimento e ponderados os demais interesses em presença. 5 - O disposto no número anterior realiza-se através da desindexação dos dados pessoais em motores de busca, sempre sem eliminação da publicação que faz fé pública*."

[216] CORDEIRO; António Menezes - *Direito de proteção de dados (…),* ob. cit., p. 274.

[217] É assim classificado pelo Autor porquanto o artigo 17.º, n.º 2 apenas prevê o exercício do direito de apagamento junto do responsável pelo tratamento e não do público em geral, pelo que a comunicação prevista neste dispositivo não parece fazer emergir na esfera jurídica dos outros responsáveis pelo tratamento uma obrigação de apagamento. Do exposto decorre que caberá ao titular requerê-lo individualmente.

A este respeito, no Acórdão *Google Spain*[218], o TJUE analisou se a Google estava, ou não, obrigada a remover as ligações respeitantes ao requerente, tendo decidido que, em determinadas condições, as pessoas têm o direito de solicitar que os seus dados pessoais sejam apagados. Este direito pode ser invocado quando as informações respeitantes a uma pessoa forem inexatas, inadequadas, não pertinentes ou excessivas para as finalidades do tratamento dos dados. Sem prejuízo, o Tribunal reconheceu que este direito não é absoluto, mas deve ser conciliado com outros direitos, em especial o interesse público em aceder a determinada informação.

Na sequência do supramencionado Acórdão, o Grupo de Trabalho do Artigo 29.º adotou orientações sobre a sua aplicação[219], as quais abrangem uma lista de critérios comuns a utilizar pelas autoridades de controlo no tratamento de reclamações relativas a pedidos de eliminação de dados, esclarecendo o eventual impacto do seu exercício e orientando no sentido da ponderação dos direitos. Uma vez que o direito a ser esquecido não é absoluto, deve ser ponderado casuisticamente, sendo que a decisão pode variar em função da situação concreta.[220]

3.5.5. DIREITO À LIMITAÇÃO DO TRATAMENTO

Nos termos do artigo 18.º, n.º 1 do RGPD, quando se apliquem determinadas situações[221], o titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento.

O artigo 4.º, 3), do RGPD define «Limitação do tratamento», como "*a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro*;". Trata-se de uma medida com caráter temporário em que o responsável

[218] TJUE, acórdão de 13 de maio de 2014 no processo C-131/12, Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GS], n.os 55 a 58. Disponível em: eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0131 [acedido em 20.07.2023]

[219] GT Artigo 29.º (2014), Guidelines on the implementation of the CJEU judgment on «Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González» C-131/12, WP 225, Bruxelas, 26 de novembro de 2014. Disponível em: wp225_en.pdf (europa.eu) [acedido em 20.07.2023]

[220] Manual da Legislação Europeia sobre Proteção de Dados *ob cit*., p. 255.

[221] Previstas nas alíneas a) a d) daquele dispositivo, designadamente quando o titular dos dados: a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial; d) Se tiver oposto ao tratamento nos termos do artigo 21.º, n.º 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

restringe o tratamento de dados pessoais, podendo socorrer-se de diferentes métodos, v.g., os previstos no considerando (67) do RGPD.[222]

Salvo quanto à conservação dos dados, nos termos do artigo 18.º, n.º 2 do RGPD, enquanto o tratamento estiver limitado, o responsável apenas pode proceder ao tratamento dos dados: (i) com o consentimento do titular; (ii) para efeitos de declaração, exercício ou defesa de um direito num processo judicial; (iii) na defesa dos direitos de outra pessoa singular ou coletiva; ou (iv) por motivos ponderosos de interesse público da União ou de um Estado-Membro.

De acordo com o previsto no artigo 18.º, n.º 3 do RGPD, o responsável pelo tratamento deve notificar o titular dos dados antes de ser anulada a limitação do referido tratamento.

O responsável pelo tratamento deve comunicar qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a cada destinatário a quem os dados pessoais tenham sido transmitidos, na medida em que tal não seja impossível ou desproporcional e, se o titular dos dados pedir informações sobre esses destinatários, o responsável pelo tratamento deve fornecer-lhe estas informações, em conformidade com o prescrito pelo artigo 19.º do RGPD.

3.5.6. DIREITO DE PORTABILIDADE

O artigo 20.º, n.º 1 do RGPD refere que, sob determinadas situações[223], o titular dos dados tem o direito de: (i) obter os dados pessoais que forneceu a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática; (ii) transmitir esses mesmos dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir.

O considerando (68) clarifica o preceito, salientando que:

> "*Os responsáveis pelo tratamento de dados deverão ser encorajados a desenvolver formatos interoperáveis* [224] *que permitam a portabilidade dos dados. Esse direito*

[222] Onde se refere que "*Para restringir o tratamento de dados pessoais pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio web dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados. Deverá indicar-se de forma bem clara no sistema que o tratamento dos dados pessoais se encontra sujeito a restrições.*".

[223] Quando: a) O tratamento se basear no consentimento dado nos termos do artigo 6.º, n.º 1, al. a), ou do artigo 9.º, n.º 2, al. a), ou num contrato referido no artigo 6.º, n.º 1, al. b); e b) o tratamento for realizado por meios automatizados.

[224] O conceito de interoperabilidade**,** *lato sensu,* traduz-se na capacidade dos sistemas de informação para trocarem dados e permitirem a partilha de informação. (*cfr.* Comissão Europeia, «Sistemas de

> *deverá aplicar-se também se o titular dos dados tiver fornecido os dados pessoais com base no seu consentimento ou se o tratamento for necessário para o cumprimento de um contrato. Não deverá ser aplicável se o tratamento se basear num fundamento jurídico que não seja o consentimento ou um contrato*.".

Este «novo» direito foi concebido com um *ratio* de dimensão individual e económica baseada, por um lado, no reforço do controlo dos dados em ambiente digital pelo respetivo titular e, por outro lado, pela simplificação da transmissão direta e facilitação dos fluxos de dados, como forma de estimular a concorrência e promover a confiança na economia digital. [225] O seu exercício depende, todavia, dos meios técnicos que os responsáveis pelo tratamento disponham, suscitando ainda outras questões quanto à sua aplicabilidade, nomeadamente em relação aos dados anonimizados.

3.5.7. DIREITO DE OPOSIÇÃO

O artigo 21.º do RGPD concede ao titular dos dados o direito de opor-se ao tratamento dos seus dados pessoais por motivos relativos à sua própria situação particular.

Não se trata, porém, de um direito geral de oposição, salvo quanto ao tratamento de dados para efeitos de comercialização direta, incluindo atividades de definição de perfis com ela conexionadas, nos termos do artigo 21.º, n.ºs 2 e 3 do RGPD[226] [227].

O exercício deste direito pressupõe a existência de um tratamento de dados legítimo que tenha como fundamento de licitude a prossecução do interesse público[228], a realização de interesses legítimos do responsável pelo tratamento ou de terceiro[229] ou as condições previstas no art.º 6.º, n.º 4 (tratamento para finalidades distintas daquelas para os quais os dados pessoais foram recolhidos).[230]

Assim, de acordo com o artigo 21.º, n.º 1, do RGPD, a oposição fundada em motivos relacionados com a situação particular do titular apenas é invocável quando o tratamento se baseia nos fundamentos de licitude acima mencionados.

Nesta conformidade, o considerando (69) do RGPD explica que o tratamento lícito baseado nestes motivos não impede o exercício do direito de se opor ao tratamento,

---

informação mais sólidos e mais inteligentes para controlar as fronteiras e garantir a segurança», COM (2016) 205 final, 2 de abril de 2016.

[225] MONIZ, Graça Canto - Direitos do titular dos dados pessoais: o direito à portabilidade. Anuário da Proteção de dados. Coord. Francisco Pereira Coutinho / Graça Canto Moniz. Universidade Nova de Lisboa. Faculdade de Direito. CEDIS, Centro de I & D sobre Direito e Sociedade, Lisboa. 2018, pp.23-25. ISBN: 978-972-99399-5-2.

[226] Manual da Legislação Europeia sobre Proteção de Dados *ob cit*., p. 260.

[227] Em sentido contrário a este entendimento, *vd.* CORDEIRO; António Menezes – *Comentário ao Regulamento (…),* ob. cit., p. 215.

[228] *Cfr.* art.º 6.º, n.º 1, al. e) do RGPD

[229] *Cfr.* art.º 6.º, n.º 1, al. f) do RGPD.

[230] PINHEIRO, Alexandre Sousa [et al.] - *Comentário ao Regulamento (…),* ob. cit., p. 385.

competindo ao responsável pelo tratamento provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses, direitos e liberdades do titular dos dados.

Sobre este assunto, o TJUE dispôs que, «regra geral», os direitos do titular dos dados prevalecem sobre os interesses económicos do responsável pelo tratamento dos dados, dependendo da «natureza da informação em questão e da sua sensibilidade para a vida privada da pessoa em causa, bem como do interesse do público em dispor dessa informação»[231].

Com efeito, atendendo a que se trata do reconhecimento do direito à autodeterminação, o seu exercício não é absoluto[232], tão-pouco a sua aplicação será universal. Acha-se, primeiramente, dependente do juízo de ponderação entre os citados motivos imperiosos e legítimos invocados pelo responsável pelo tratamento, em contraposição aos interesses, direitos e liberdades do titular. Por essa razão, o artigo 6.º, n.º 1, alíneas e) e f) e n.º 4 preveem expressamente quatro situações que podem justificar a não aplicabilidade deste direito.[233]

Por último, insta salientar que o titular dos dados pode também opor-se ao tratamento dos dados para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1[234], salvo se o mesmo for necessário à prossecução de atribuições de interesse público. [235]

3.5.8. DECISÕES INDIVIDUAIS AUTOMATIZADAS, INCLUINDO DEFINIÇÃO DE PERFIS

O artigo 22.º, n.º 1, do RGPD prevê que o titular dos dados *"(…) tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar*."

As decisões automatizadas incluem a definição de perfis, definido no artigo 4.º, 4) do RGPD, qualquer meio de tratamento automatizado de dados pessoais que utilize os dados recolhidos *"(…) avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho*

[231] TJUE, acórdão de 13 de maio de 2014, processo C-131/12, Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GS], n.º 81, disponível em: eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0131 [acedido em 01.07.2023]

[232] Excetuando as situações de tratamento para efeitos de comercialização direta (cfr. art.º 21.º, n.ºs 2 e 3). O considerando (70) trata desta matéria, salientando que o direito de oposição, neste caso, pode ser exercido a todo o tempo e de modo gratuito.

[233] MONIZ, Graça Canto, *ob. cit.*, p. 19.

[234] *Cfr.* art.º 21.º, n.º 6 do RGPD.

[235] PINHEIRO, Alexandre Sousa [et al.] - *Comentário ao Regulamento (…),* ob. cit. p. 386.

profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;"[236].

Sem prejuízo, o n.º 2 do mesmo artigo estatui que as decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente as pessoas podem ser aceitáveis se: (i) forem necessárias para a celebração ou para a execução de um contrato entre o responsável pelo tratamento dos dados e o titular dos dados; (ii) se o titular dos dados der o seu consentimento explícito (iii) se forem autorizadas por lei. Nas duas primeiras situações devem os direitos, liberdades e interesses legítimos do titular dos dados ser salvaguardados de forma adequada (cfr. artigo 22.º, n.º 3).

Este artigo tem como desiderato a proteção do titular perante a circunstância de uma decisão ser tomada, exclusivamente, com base numa avaliação automatizada, impedindo o uso de certos resultados do tratamento que não tenham intervenção humana. Trata-se de evitar que o titular dos dados *"(…) se torne um mero sujeito passivo e que a responsabilidade por decisões não seja atribuída a programas de computador (…)"*[237].

A doutrina tem suscitado dúvidas quanto à natureza jurídica do artigo 22.º atendendo a que, por um lado, a sua redação e ordem sistemática parece posicioná-lo no rol de direitos dos titulares, mas, por outro lado, o seu conteúdo, assente numa proibição geral de decisões automatizadas, indica requisitos de licitude adicionais aos consagrados em geral no RGPD.[238]

Destarte, é assegurado que o titular tem o direito a obter a intervenção humana no tratamento dos seus dados, exprimir a sua opinião[239] e exigir uma explicação sobre a lógica da decisão, podendo sindicá-la. E, como de resto, não se tratando de um direito absoluto, o seu âmbito de aplicação é determinado pelo fundamento jurídico que subjaz ao tratamento**,** devendo o responsável adotar as medidas adequadas para

[236] O Grupo de Trabalho do Artigo 29.º forneceu orientações adicionais sobre a utilização de decisões automatizadas nos termos do RGPD, *cfr.* Grupo de Trabalho do Artigo 29.º (2017), Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, WP 251, 3 de outubro de 2017, disponíveis em: https://ec.europa.eu/newsroom/article29/items/612053 (acedido em 18.08.2023).

[237] CORDEIRO; António Menezes – *Comentário ao Regulamento (…)*, ob. cit., p. 222.

[238] *Ibidem*, p. 223.

[239] De acordo com o Relatório Explicativo da Convenção n.º 108 modernizada, n.º 75 e artigo 9.º, n.º 1, al. c), a exigência de considerar a opinião do titular dos dados quando as decisões se baseiam exclusivamente em meios de tratamento automatizado indica que estes têm o direito de impugnar tais decisões, e deviam poder contestar qualquer inexatidão nos dados pessoais que o responsável pelo tratamento utiliza, e contestar a adequação de qualquer perfil que lhe seja aplicado. Todavia, uma pessoa não pode exercer este direito se a decisão automatizada for autorizada por uma lei, à qual está sujeito o responsável pelo tratamento, que também estabelece medidas para proteger os direitos, liberdades e interesses legítimos do titular dos dados. Além disso, os titulares dos dados têm o direito de ser informados, a pedido, da fundamentação subjacente ao tratamento de dados.

salvaguardar os direitos e liberdades fundamentais do titular, mormente, a intervenção humana e a participação do titular no processo de decisão e na sua contestação. [240]

3.5.9. RECLAMAÇÃO E RECURSO

O artigo 77.º do RGPD, assevera o direito de apresentar reclamação a uma autoridade de controlo, sem colocar em crise o recurso a outras vias de recurso administrativo ou judicial.[241] Os artigos 78.º e 79.º asseguram, respetivamente, o direito à ação judicial contra uma autoridade de controlo e contra um responsável pelo tratamento ou subcontratante.

O sistema de contencioso do direito a proteção de dados atribui ao titular dos dados três vias alternativas, a saber, (i) reclamar junto das autoridades de controlo; (ii) litigar junto dos tribunais administrativos, quando existam propósitos petitórios ou impugnatórios; (iii) litigar junto dos tribunais cíveis, nomeadamente com propósitos ressarcitórios.[242]

Por seu turno, o artigo 32.º da LE, sob a epígrafe «tutela administrativa» refere que:

> "*Sem prejuízo do direito de apresentação de queixa à CNPD, qualquer pessoa pode recorrer a meios de tutela administrativa, designadamente de cariz petitório ou impugnatório, para garantir o cumprimento das disposições legais em matéria de proteção de dados pessoais, nos termos previstos no Código do Procedimento Administrativo*.".

O artigo 46.º, n.º 1 da mesma Lei dispõe que "*Quem utilizar dados pessoais de forma incompatível com a finalidade determinante da recolha é punido com pena de prisão até um ano ou com pena de multa até 120 dias*".

Em resultado das disposições ora transcritas, o titular dos dados tem ao seu dispor quatro meios de defesa distintos: (i) reclamar junto da CNPD (cfr. artigo 77.º do RGPD); (ii) litigar junto dos tribunais administrativos, em especial contra as decisões da CNPD (cfr. artigo 78.º do RGPD) ou as decisões de outras entidades integrantes da Administração Pública; (iii) litigar junto dos tribunais cíveis, nomeadamente com propósitos ressarcitórios (cfr. artigo 82.º do RGPD e 33.º da LE) e (iv) apresentar queixas-crime, nos termos do artigo 46.º e ss da LE. [243]

[240] MONIZ, Graça Canto, *ob. cit.*, p. 20.
[241] Sobre este assunto, o artigo 57.º, n.º 2 do RGPD, por seu turno, estabelece que as autoridades de controlo devem facilitar a apresentação de reclamações por parte de qualquer titular de dados, organismo, organização ou associação diligenciando, ademais, no sentido de disponibilizar formulários de reclamação eletrónicos, sem inviabilizar o recurso a outros meios de comunicação.
[242] CORDEIRO; António Menezes – *Comentário ao Regulamento (…)*, ob. cit., p. 482.
[243] *Ibidem*, p. 630.

4. *DATA COMPLIANCE* NA PERSPETIVA DO SETOR PÚBLICO: RESPONSABILIDADE E GOVERNAÇÃO

4.1. OS PRINCIPAIS INTERVENIENTES NO NOVO MODELO DE CONTROLO DA CONFORMIDADE

4.1.1. O RESPONSÁVEL PELO TRATAMENTO: NOÇÃO E RESPONSABILIDADE

O artigo 4.º, n.º 7 do RGPD define «Responsável pelo tratamento» ou «*controller*»[244] como "*a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; (…)*".

O Comité Europeu para a Proteção de Dados (CEPD) pronunciou-se no sentido de que a definição de responsável pelo tratamento contém cinco elementos basilares: (i) «a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo»; (ii) que «determina»; (iii) «individualmente ou em conjunto com outras»; (iv) «as finalidades e os meios»; (v) «de tratamento de dados pessoais». [245]

O primeiro elemento alude ao tipo de entidade que pode ser responsável pelo tratamento, indicando que, em princípio, não existe qualquer restrição quanto ao tipo de pessoa que assuma a função de responsável pelo tratamento, podendo ser uma organização, uma pessoa singular ou um grupo de pessoas singulares.

O segundo elemento respeita à necessidade de o responsável pelo tratamento deter poder decisório sobre os aspetos fundamentais do tratamento de dados pessoais. Esse poder de determinação pode achar-se definido por lei ou resultar de uma análise das circunstâncias ou elementos factuais do caso concreto. A fim de aferir deste último, deve proceder-se à análise das operações de tratamento e entender quem as determina, questionando-se por que razão se está a realizar o tratamento e quem decidiu que o tratamento deveria ser realizado para uma finalidade específica.

No que tange ao terceiro elemento, importa considerar que no artigo 4.º, n.º 7, onde se refere que o responsável pelo tratamento é a pessoa que «individualmente ou em conjunto com outras» determina as finalidades e os meios do tratamento, é admitida a possibilidade de determinação das finalidades e os meios do tratamento por mais do que um interveniente. Do exposto resulta que várias entidades diferentes podem agir como responsáveis pelo tratamento em relação ao mesmo tratamento, estando cada

[244] Como é designado na versão original do RGPD.

[245] *Vd*. CEPD, Orientações n.º 07/2020, sobre os conceitos de responsável pelo tratamento e subcontratante no RGPD. Versão 2.0., adotadas em 7 de julho, p. 11. Disponíveis em: eppb_guidelines_202007_controllerprocessor_final_pt.pdf (europa.eu) [acedido em 08.08.2023]

uma delas sujeita às disposições aplicáveis em matéria de proteção de dados, mesmo que não tome todas as decisões relativas às finalidades e aos meios.

O quarto elemento consiste na parte substantiva do conceito de responsável pelo tratamento e relaciona-se com o seu objeto da influência, ou seja, o que um responsável pelo tratamento deve determinar para ser qualificado como tal, i.e., «as finalidades e os meios» do tratamento. [246]

Por último, o quinto elemento requer que as finalidades e os meios determinados pelo responsável pelo tratamento respeitem ao «tratamento de dados pessoais». Com efeito, no artigo 4.º, n.º 2 do RGPD define-se «tratamento de dados» pessoais como «*uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais*». Nesta conformidade, o conceito de «responsável pelo tratamento» é passível de resultar de uma operação única de tratamento ou a um conjunto de operações, podendo englobar o tratamento em questão na sua globalidade ou limitar-se a uma etapa específica no tratamento.[247]

Já para ALEXANDRE PINHEIRO [248], a noção de «responsável pelo tratamento» decompõe-se apenas em três grupos constituintes, a saber: (i) o elemento (não-) personalista; (ii) a determinação das finalidades e dos meios de tratamento; e (iii) a possibilidade de que tal determinação seja individual ou conjunta.

Com o primeiro elemento pretende-se definir um centro de imputação de responsabilidade, o que significa que não é necessário que o responsável pelo tratamento assuma uma forma jurídica específica ou tenha, sequer, personalidade jurídica, para que a responsabilidade pelo tratamento lhe seja imputada. Do exposto decorre que o conceito de responsável pelo tratamento é alheio à categorização, i.e., forma ou natureza jurídica, que cada Estado concede às pessoas.[249] Importa salientar que nas pessoas coletivas, públicas e privadas, o responsável pelo tratamento é a própria pessoa e não o respetivo representante, sem prejuízo da sua sujeição aos mecanismos civis, criminais ou administrativos aplicáveis.[250]

---

[246] De acordo com o CEPD, a determinação da «finalidade» do tratamento está reservada ao «responsável pelo tratamento», pelo que quem tomar esta decisão é, de facto, o responsável pelo tratamento. Já a determinação dos «meios» do tratamento pode ser delegada pelo responsável pelo tratamento, desde que estejam apenas em causa questões técnicas ou organizativas. As questões substanciais que sejam essenciais para a licitude do tratamento estão reservadas ao responsável pelo tratamento. *Ibidem*, p.p. 14-15.

[247] *Ibidem*, p.p. 11-20.

[248] PINHEIRO, Alexandre [et al.] – *Comentário ao Regulamento (…), ob. cit.,* p. 139.

[249] No mesmo sentido, *vd.* CORDEIRO, A. Barreto Menezes - *Direito da Proteção de Dados (…), ob. cit.,* p. 307.

[250] No entanto, nas situações em que o trabalhador utilize os dados para a prossecução de fins próprios ou fora do âmbito das atividades da entidade empregadora, para todos os efeitos legais, será considerado responsável pelo tratamento. *Ibidem*, p. 308.

O segundo elemento, por seu turno, estabelece a noção de finalidade e meios de tratamento, que devem ser interpretadas, respetivamente, como a faculdade de controlar, determinar e/ou decidir os termos em que decorrem as operações de tratamento e os recursos técnicos e tecnológicos para as concretizar.

Por fim, o último elemento, remete-nos para a faculdade das finalidades e meios de tratamento poderem ser determinadas conjuntamente, ou seja, que duas ou mais entidades (pessoas singulares ou coletivas, autoridade pública, agência ou organismo) sejam consideradas responsáveis pelo tratamento, nos termos preconizados pelo artigo 26.º do RGPD.[251] Para o Autor, trata-se de uma questão relevante porquanto a clarificação dos sujeitos envolvidos nas operações de tratamento dos dados pessoais é preponderante para a imputação de deveres e de responsabilidades.

Por outro lado, no que se refere à responsabilidade da figura do responsável pelo tratamento, insta evidenciar o disposto no artigo 24º, n.º 1 do RGPD que estipula que:

> "*Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades*".[252]

O normativo em questão evidencia, de modo inequívoco, que a obrigação de garantir o cumprimento das disposições do RGPD relativas ao tratamento de dados recai sobre o responsável pelo tratamento. Por seu turno, o n.º 2 do mesmo dispositivo determina que as aludidas medidas *"(…) incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento*", remetendo para a adoção de códigos de conduta ou de procedimento de certificação aprovados, nos termos previstos nos artigos 40.º e 42.º do RGPD, respetivamente. A adoção destes instrumentos assume potenciais meios de demonstração de cumprimento das obrigações do responsável pelo tratamento. Mais se exige que o responsável pelo tratamento adote ou desenvolva medidas técnicas e organizativas que garantam um

[251] PINHEIRO, Alexandre [et al.] – *Comentário ao Regulamento (…),* ob. cit., p. 407.

[252] Para Mafalda Miranda Barbosa quando "*(…) um determinado sujeito lida com dados alheios, assume uma esfera de risco/responsabilidade, devendo adotar as medidas de cuidado – consagradas pelo legislador – no sentido de garantir a sua incolumidade. Não o fazendo, a primitiva esfera de responsabilidade (responsabilidade pelo outro, ou pelos dados do outro) convola-se numa outra esfera, mais ampla, de responsabilidade, no sentido da liability (responsabilidade perante o outro)*". *Cfr*. Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil – Revista de Direito Comercial. 2018, p. 439. Disponível em: 1 (squarespace.com). [acedido em 01.09.2023].

nível de segurança adequado ao risco. Nos termos do disposto no artigo 32.º, n.º 1 do RGPD, tais medidas podem compreender a adoção de vários mecanismos, tais como (i) a pseudonomização e a cifragem dos dados pessoais; (ii) medidas que assegurem a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; (iii) medidas que asseverem a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; (iv) a definição de um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Em caso de ocorrência de uma violação de dados pessoais, em conformidade com o previsto no artigo 33º, n.º 1 do RGPD, o responsável pelo tratamento deve notificar a autoridade de controlo de tal facto, podendo, para o efeito, utilizar o formulário disponibilizado pela própria CNPD na sua página oficial da internet.[253] Sobre esta matéria, importa atender às orientações do Grupo de Trabalho do Artigo 29.º [254] e do Comité Europeu para a Proteção de Dados.[255]

Sempre que se conclua que a violação de dados pessoais é suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento está obrigado a comunicar a violação de dados pessoais ao titular dos dados sem demora injustificada, nos termos do disposto no artigo 34º, n.º 1 do RGPD e nos moldes preconizados pelo artigo 33º, n.º 3, alíneas b), c) e d) do mesmo diploma.

Por último, importa ainda referir que assiste ao titular dos dados o direito de apresentação de queixa e ou de reclamação junto da autoridade de controlo. Com efeito, preceitua o artigo 77.º do RGPD que os titulares dos dados têm o direito a apresentar reclamação a uma autoridade de controlo, mormente a do Estado-membro da sua residência habitual, do seu local de trabalho ou do local onde foi alegadamente praticada a infração, se o titular dos dados considerar que o tratamento dos dados pessoais que lhe diga respeito viola o Regulamento. O direito à reclamação não colide com o recurso à via administrativa[256] ou judicial, nos termos do n.º 1 do artigo 77º do

[253] CNPD, Formulário de Notificação de Violação de Dados Pessoais, disponível em: Notificações de violação de dados pessoais (cnpd.pt) [acedido em 01.09.2023].

[254] GT29, «Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679», de 6 de fevereiro de 2018, (WP250 rev.1) https://www.cnpd.pt/media/zgkec1q0/data-breach- wp250rev01_pt.pdf [acedido em 01.09.2023].

[255] CEPD, Orientações 01/2021 sobre exemplos da notificação de uma violação de dados pessoais Adotadas em 14 de dezembro de 2021 Versão 2.0, disponíveis em edpb_guidelines_012021_pdbnotification_adopted_pt.pdf (europa.eu) [acedido em 02.09.2023].

[256] De acordo com o artigo 32.º da LE, qualquer pessoa pode recorrer a meios de tutela administrativa, designadamente de cariz petitório ou impugnatório, para garantir o cumprimento das disposições legais

RGPD, quer contra a autoridade de controlo[257] ou contra o responsável pelo tratamento/subcontratante. [258]

4.1.1.1. A RESPONSABILIDADE ADMINISTRATIVA PELO TRATAMENTO ILÍCITO DE DADOS PESSOAIS

Como se viu, o conceito de responsável pelo tratamento é um conceito funcional, que visa atribuir responsabilidade àqueles que detêm, efetivamente, poder decisório, aferido através de uma análise factual e não formal.

Sem prejuízo, partindo da própria definição, é responsável pelo tratamento, entre outras, a pessoa coletiva pública, que individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento dos dados pessoais.

O artigo 4.º, n.º 7 do RGPD, *in fine*, refere que a identificação do responsável pelo tratamento "*(…) ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro*".

Por conseguinte, o artigo 2.º, n.º 1 da LE abrange os tratamentos de dados pessoais realizados em território nacional efetuados, entre outras, por entidades de natureza pública "*(…) mesmo que o tratamento de dados pessoais seja efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público*".

Com efeito, em termos gerais, a lei pode impor às entidades públicas a obrigação de conservação e fornecimento de determinados dados. Nestas situações, a lei, ao invés de nomear diretamente o responsável pelo tratamento ou de definir os critérios para a sua nomeação, por via do cumprimento das atribuições que lhe são legalmente acometidas, impõe a obrigação de tratamento de determinada informação pessoal. [259]

Nestas circunstâncias, o responsável pelo tratamento nas entidades públicas é a própria entidade, que tem a obrigação de tratamento dos dados pessoais, devendo decidir «porquê» e «como» os dados pessoais são tratados.

Verifica-se, todavia, que frequentemente os organismos públicos designam uma pessoa específica responsável pela aplicação da atividade de tratamento, normalmente o seu dirigente superior máximo – titular do órgão de direção superior -,

em matéria de proteção de dados pessoais, nos termos previstos no Código do Procedimento Administrativo.

[257] Artigo 78.º do RGPD (Direito à ação judicial contra uma autoridade de controlo) e artigo 34.º, n.º 1 da LE.

[258] Artigo 79.º do RGPD (Direito à ação judicial contra um responsável pelo tratamento ou um subcontratante) e artigo 34.º, n.º 3 da LE.

[259] CEPD, Orientações 07/2020 sobre os conceitos de responsável pelo tratamento e subcontratante no RGPD Versão 2.0 Adotadas em 7 de julho, disponíveis em: eppb_guidelines_202007_controllerprocessor_final_pt.pdf (europa.eu) [acedido em 05.09.2023].

porquanto a este compete, em primeira linha, garantir a prossecução das atribuições cometidas ao respetivo serviço, assegurando o seu bom desempenho através da otimização de recursos e promovendo a satisfação dos destinatários da sua atividade.[260]

Contudo, mesmo que uma pessoa singular seja designada para assegurar o cumprimento das regras de proteção de dados, esta pessoa não será o responsável pelo tratamento, mas atuará por conta da entidade jurídica (empresa ou organismo público) que será, em última instância, responsável em caso de violação das regras na sua capacidade de responsável pelo tratamento.[261]

Aqui chegados, importa realçar o estatuído no artigo 82.º, n.º 2 do RGPD, que estabelece que "[q]*ualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento*", acrescentando que o mesmo sucede com o subcontratante, na medida em que não tenha cumprido as obrigações que lhe são dirigidas especificamente no RGPD ou se não tiver seguido as instruções lícitas do responsável pelo tratamento.

O considerando (146) do RGPD, por seu turno, esclarece que o responsável pelo tratamento ou o subcontratante deve "*(…) reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o presente regulamento*", podendo, todavia, ser exonerado dessa responsabilidade caso comprove que o dano não lhe é imputável. A noção de dano deve ser interpretada de acordo com a jurisprudência do Tribunal de Justiça e refletir os objetivos do RGPD. [262]

Destarte, o artigo 33.º, n.º 3 da LE dispõe que a Lei n.º 67/2007, de 31 de dezembro, na sua redação em vigor [263], - que estabelece o regime da Responsabilidade Civil Extracontratual do Estado e Pessoas Coletivas de Direito Público (RRCEE) -, é aplicável quando esteja em causa um dano devido ao tratamento ilícito de dados ou

[260] *Cfr*. Artigo 3.º do Estatuto do Pessoal Dirigente dos Serviços e Organismos da Administração Pública, aprovado pela Lei n.º 2/2004, de 15 de janeiro, na sua redação em vigor. O artigo 1.º, n.º 5 do Estatuto salvaguarda ainda a existência de outros Estatutos previstos em legislação específica.

[261] CEPD, Orientações n.º 07/2020, *cit.,* p. 11.

[262] O aludido considerando acrescenta ainda que os titulares dos dados devem *"(…) ser integral e efetivamente indemnizados pelos danos que tenham sofrido. Sempre que os responsáveis pelo tratamento ou os subcontratantes estiverem envolvidos no mesmo tratamento, cada um deles deverá ser responsabilizado pela totalidade dos danos causados. Porém, se os processos forem associados a um mesmo processo judicial, em conformidade com o direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido. Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento".*

[263] Com as alterações introduzidas pela Lei n.º 31/2008, de 17 de julho.

qualquer outro ato que viole disposições do RGPD ou da própria LE em matéria de proteção de dados pessoais.

Sobre este assunto importa salientar que o artigo 22.º da CRP prescreve, desde logo, que:

> "*O Estado e as demais entidades públicas são civilmente responsáveis, em forma solidária com os titulares dos seus órgãos, funcionários ou agentes, por ações ou omissões praticadas no exercício das suas funções e por causa desse exercício, de que resulte violação dos direitos, liberdades e garantias ou prejuízo para outrem*".

Para GOMES CANOTILHO e VITAL MOREIRA, o artigo 22.º da CRP tem como finalidade salvaguardar o direito fundamental a que os danos causados pelo Estado ou pelas entidades públicas sejam devidamente compensados, não se resumindo apenas a uma (…) *lógica indemnizatória-ressarcitória decalcada da responsabilidade do direito civil*". [264]

No entendimento do professor MARCELO REBELO DE SOUSA:

> "*A responsabilidade civil administrativa é o conjunto de circunstâncias da qual emerge, para a administração e para os seus titulares de órgãos, funcionários ou agentes, a obrigação de indemnização dos prejuízos causados a outrem no exercício da atividade administrativa*". [265]

A classificação de responsabilidade civil administrativa é baseada em diversos critérios, podendo haver lugar a responsabilidade civil da Administração Pública por atos de gestão pública (atos e regulamentos administrativos) ou por atos de gestão privada, revestindo particular interesse nos casos de responsabilidade contratual. [266]

Por sua vez, o artigo 271.º da CRP consagra o princípio da responsabilização civil, criminal e disciplinar dos funcionários e agentes da Administração Pública por ações ou omissões resultantes do exercício da função administrativa. Com efeito, estabelece o n.º 1, sob a epígrafe «responsabilidade dos funcionários e agentes», que:

> "*Os funcionários e agentes do Estado e das demais entidades públicas são responsáveis civil, criminal e disciplinarmente pelas ações ou omissões praticadas no exercício das suas funções e por causa desse exercício de que resulte violação dos direitos ou interesses legalmente protegidos dos cidadãos*".

[264] CANOTILHO, Gomes; MOREIRA, Vital - *Constituição da República Portuguesa Anotada*, Volume I, 4.ª edição, Coimbra, 2007, p. 425.

[265] REBELO DE SOUSA, Marcelo; SALGADO DE MATOS, André, - *Direito Administrativo Geral - Atividade Administrativa*, Tomo III, 2ª edição (reimp.), D. Quixote, Lisboa, 2016, p. 477.

[266] A responsabilidade civil administrativa pode ser classificada de três formas: (i) quanto à imputação do prejuízo, a responsabilidade pode ser delitual, pelo risco ou por facto ilícito; (ii) quanto à natureza da posição jurídica subjetiva violada, a responsabilidade pode ser contratual ou extracontratual; (iii) quanto ao ramo do direito pela qual é regulada, a responsabilidade civil pode ser por ato de gestão pública ou por ato de gestão privada. *Ibidem*, p. 482 e seguintes.

Considerando a temática do presente estudo, cingir-nos-emos à matéria da responsabilidade civil extracontratual[267], por atos de gestão pública, centrada na responsabilidade extracontratual delitual ou aquiliana, que emerge da violação de normas que impõem deveres de ordem geral e correlativamente de direitos absolutos do lesado, i.e., a violação de normas gerais que tutelam interesses alheios, de deveres genéricos de respeito.[268] Assim, insta, nesta sede e de modo sumário, aferir se a responsabilidade civil extracontratual por atos de gestão pública dos quais resultem a violação de dados pessoais incide na pessoa coletiva pública e nos titulares de órgãos ou agentes, ou se apenas nestes últimos.

Nas palavras de MARCELO REBELO DE SOUSA, "*O critério relevante é o da imputação: há responsabilidade administrativa pelos prejuízos provocados por atos que sejam imputados a uma pessoa coletiva administrativa (atos funcionais)*" [269].

A matéria da responsabilidade civil extracontratual do Estado e das pessoas coletivas de direito público é, como se mencionou, regulada pelo RRCEE. No que respeita à responsabilidade por facto ilícito estabelece o supramencionado regime: (i) a responsabilidade exclusiva do Estado e demais pessoas coletivas de direito público pelos danos que decorrem de ações ou omissões ilícitas, cometidas com culpa leve, pelos titulares dos seus órgãos e funcionários públicos, no exercício da função administrativa e por causa desse exercício[270]; (ii) a responsabilidade dos titulares e funcionários, em que estes são pessoalmente responsáveis pelos danos que resultem de ações ou omissões ilícitas, por eles praticadas com dolo ou com culpa grave, isto é, com diligência e zelo manifestamente inferiores àqueles a que se encontravam obrigados em razão do cargo [271]; (iii) a responsabilidade solidária do Estado e demais pessoas coletivas de direito público com os titulares dos seus órgãos e funcionários públicos, se as ações ou omissões tiverem sido cometidas por estes com dolo ou com

[267] Deixando de parte a responsabilidade contratual.

[268] Neste sentido, vd. Acórdão do Supremo Tribunal de Justiça, 2.ª secção, Processo 1674/07.7TVLSB.P1.S1 (relator Távora Vítor) de 23.12.2012, disponível em: Acórdão do Supremo Tribunal de Justiça (dgsi.pt), [acedido em 06.09.2023], onde se refere que a responsabilidade extracontratual ou aquiliana resulta da prática de factos ilícitos culposos violadores de direitos ou interesses alheios juridicamente protegidos, causadores de prejuízos a outrem; como resulta dos seus próprios termos, esta responsabilidade gera-se fora do círculo de uma relação obrigacional entre as partes. Muito embora em pouco se traduza, no tocante aos respectivos requisitos, a diferença entre os dois tipos de responsabilidade supra-referidos, certo é que no que concerne ao ónus da prova existe entre ambas uma diferença fundamental; na responsabilidade civil obrigacional a culpa presume-se, o que não sucede na responsabilidade extra-contratual ou aquiliana em que cabe ao lesado provar a culpa do lesante.

[269] REBELO DE SOUSA, Marcelo; SALGADO DE MATOS, André, *ob cit*., p.485.

[270] Cfr. artigo 7.º, n.º 1 do RRCEE.

[271] Cfr. artigo 8.º, n.º 1 do RRCEE.

culpa grave, no exercício das suas funções e por causa desse exercício[272]; (iv) o direito de regresso do Estado e demais pessoas coletivas de direito público contra os titulares dos órgãos e funcionários públicos, sempre que suportem qualquer indemnização de forma solidária com os titulares de órgãos [273].

A este respeito insta salientar que no artigo 7.º, n.º 1 e 8.º, n.º 2 do RRCEE são estabelecidos os requisitos necessários ao enquadramento no conceito de atos correspondentes ao «exercício da função administrativa» (ato funcional), impondo a necessidade de o ato ser praticado (i) pelo titular de órgão, funcionário ou agente da pessoa coletiva; (ii) no exercício das funções do titular de órgão, funcionário ou agente e (iii) por causa desse exercício.

Assim, o dever de indemnizar pelos danos causados ao titular dos dados é suscetível de recair exclusivamente sobre a pessoa coletiva a quem é imputado o facto que gerou o prejuízo ou, solidariamente, com o titular de órgão, funcionário ou agente que tenha praticado o ato.

Por outro lado, para que qualquer entidade pública incorra em responsabilidade civil por facto ilícito, devem verificar-se os seguintes pressupostos cumulativos: (i) o facto voluntário; (ii) a ilicitude, (iii) a culpa, (iv) o dano e o (v) nexo de causalidade [274].

Quanto à responsabilidade exclusiva da entidade pública, de acordo com o artigo 7.º, n.º 4 do RRCEE verifica-se a existência de funcionamento anormal do serviço nas situações em que, atendendo às circunstâncias e a padrões médios de resultado, seja razoável exigir ao serviço uma atuação suscetível de evitar os danos produzidos.[275]

Nos termos do artigo 8.º, n.º 1 da RRCEE, os titulares de órgãos, funcionários e agentes são responsáveis pelos danos que resultem de ações ou omissões ilícitas, por

[272] Cfr. artigo 8.º, n.º 2 do RRCEE.
[273] Cfr. artigo 8.º, n.º 3 do RRCEE.
[274] Para uma maior análise quanto à verificação de cada um dos mencionados pressupostos, sugere-se a leitura de OTERO, Paulo - *Causas de exclusão da responsabilidade civil extracontratual da Administração Pública por facto ilícito*. Faculdade de Direito da Universidade de Lisboa. Lisboa. 2021. Disponível em: Causas_de_exclusao_da_responsablidade.pdf (ulisboa.pt) [acedido em 06.09.2023].
[275] Para Marcelo Rebelo de Sousa há situações em que, apesar de ser objetivamente comprovável que um determinado dano se produziu em virtude da má organização ou do mau funcionamento de um serviço público, não é possível identificar o autor ou os autores dos factos. Por conseguinte, não é possível verificar os pressupostos da responsabilidade civil, na parte em que competia formular os juízos de dolo ou negligência dos quais depende o preenchimento do pressuposto culpa da responsabilidade civil. Nestas situações admite-se a responsabilização da pessoa coletiva a que pertença o serviço em causa sem necessidade de apuramento da culpa individual. Por outro lado, Fernandes Cadilha, entende que a "Culpa do Serviço" compreende não só a culpa coletiva, atribuível a um deficiente funcionamento do serviço, mas também a culpa anónima, resultante de um concreto comportamento de um agente cuja autoria não seja possível determinar. *Cfr.* CADILHA, Carlos Alberto Fernandes - *Regime da responsabilidade civil extracontratual do Estado e demais entidades públicas: anotado* Coimbra: Coimbra Editora, 2008, pp. 132 e 133.

eles cometidas com dolo ou com diligência e zelo manifestamente inferiores àqueles a que se encontravam obrigados em razão do cargo (i.e., culpa grave) [276].

Em conformidade com o prescrito pelo artigo 9.º, n.º 1 são tidas por ilícitas as ações ou omissões dos titulares de órgãos, funcionários e agentes que violem disposições ou princípios constitucionais, legais ou regulamentares ou infrinjam regras de ordem técnica ou deveres objetivos de cuidado e de que resulte a ofensa de direitos ou interesses legalmente protegidos, existindo igualmente ilicitude quando a ofensa de direitos ou interesses legalmente protegidos resulte do funcionamento anormal do serviço, segundo o disposto no n.º 3 do artigo 7.º. De acordo com o artigo 10.º, n.º 1 do RRCEE, a culpa dos titulares de órgãos, funcionários e agentes deve ser apreciada pela diligência e aptidão que seja razoável exigir, em função das circunstâncias de cada caso, de um titular de órgão, funcionário ou agente zeloso e cumpridor.

O Estado e as demais pessoas coletivas de direito público são responsáveis de forma solidária com os respetivos titulares de órgãos, funcionários e agentes, se as ações ou omissões referidas no artigo 8.º, n.º 1 do RRCEE tiverem sido cometidas por estes no exercício das suas funções e por causa desse exercício.

O artigo 3.º, n.º 1 do RRCEE estatui que quem esteja obrigado a reparar um dano deve reconstituir a situação que existiria se não se tivesse verificado o evento que obriga à reparação sendo, em conformidade com o n.º 2 do mesmo preceito, a indemnização fixada em dinheiro quando a reconstituição natural não seja possível, não repare integralmente os danos ou seja excessivamente onerosa.

Nesta sede importa salientar que segundo JOÃO CAUPERS[277], a eventual contribuição do lesado para a produção do facto danoso ou para o agravamento dos danos (i.e., concorrência da culpa do lesado), pode conduzir à redução ou mesmo exclusão do direito à indemnização. Assim, considera-se existir culpa do lesado sempre que este não tenha utilizado os meios processuais ao seu alcance para eliminar o ato jurídico gerador dos prejuízos.[278] Esta distinção é crucial para a repartição da responsabilidade. Do exposto decorre que a responsabilidade do Estado ou outra entidade pública é exclusiva quando: (i) o autor da conduta ilícita haja atuado no exercício da função administrativa e por causa desse exercício, com culpa leve (*cfr*.

[276] "*O juízo de culpa pressupõe a existência de um comportamento padrão a observar em determinadas circunstâncias sobre o qual se há-de aferir a conduta do agente traduzindo-se esse juízo numa censura - desconformidade entre aquele comportamento que o agente podia e devia ter tido e aquilo que efectivamente realizou*." Cfr. Acórdão do Supremo Tribunal Administrativo (STA) de 09.10.2014 , Processo n.º 0279/14 (relator Costa Reis), disponível em: Acordão do Supremo Tribunal Administrativo (dgsi.pt) [acedido em 06.09.2023].

[277] CAUPERS, João - *A Responsabilidade do Estado e Outros Entes Públicos*, Faculdade de Direito da Universidade Nova de Lisboa, p. 84.

[278] Cfr. artigo 4.º do RRCEE.

artigo 7.º, n.º 1); (ii) os danos causados sejam imputáveis ao funcionamento anormal do serviço, mas não tenham resultado de um comportamento concretamente determinado ou não seja possível apurar a respetiva autoria (*cfr*. artigo 7.º, n.º 3).

Já quando o autor da conduta ilícita haja atuado com dolo ou culpa grave, no exercício das suas funções e por causa desse exercício, o Estado ou outra entidade pública são solidariamente responsáveis com o titular do órgão, funcionário ou agente[279]. Mantendo-se a regra de que o Estado ou outra entidade pública poderá ser obrigado a pagar a totalidade da indemnização determinada pelo tribunal, conserva-se também o direito de regresso, relativo às quantias que deveriam ter sido pagas pelo titular do órgão, funcionário ou agente. Sublinhe-se ainda que o direito de regresso corresponde a um poder vinculado, que a Administração tem obrigatoriamente de exercer.

Por fim, estabelecem os artigos 8.º, n.º 3, e 6.º, n.º 1 do RRCEE que o exercício do direito de regresso, nos casos em que se encontra previsto na lei é obrigatório, sem prejuízo do procedimento disciplinar a que haja lugar.

4.1.2. O SUBCONTRATANTE

O artigo 4.º, n.º 8 do RGPD preceitua que «subcontratante» é "*uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes*;".

O «subcontratante» atua, assim, como mandatário do «responsável pelo tratamento», na medida em que se obriga a praticar um ou mais atos jurídicos por contra doutrem, conforme previsto no artigo 1157.º do Código Civil. É, ademais, titular de uma posição fiduciária, na medida em que está obrigado a atuar sempre no melhor interesse do beneficiário da relação, i.e., o responsável pelo tratamento.[280]

Para se aferir da distinção entre «responsável pelo tratamento» e «subcontratante» importa considerar os seguintes indícios que apontam para a pessoa do responsável pelo tratamento: (i) utilização discricionária dos dados pessoais; (ii) junção dos dados próprios aos dados que lhe foram transmitidos; (iii) aplicação dos dados transmitidos para propósitos próprios ou distintos dos originais; (iv) recolha de dados diretamente junto dos titulares; (v) assunção de responsabilidades autónomas no tratamento dos dados.[281]

[279] *Cfr.* artigo 8.º, n.º 2 do RRCEE.
[280] CORDEIRO, A. Barreto Menezes - *Direito da Proteção de Dados (…), ob. cit.*, p. 309.
[281] *Ibidem*.

No considerando (81) e no artigo 28.º, n.º 1, ambos do RGPD, refere-se que o responsável pelo tratamento deve recorrer exclusivamente a subcontratantes que ofereçam garantias suficientes - [em termos de conhecimentos especializados, fiabilidade e recursos] -, relativamente à execução de medidas técnicas e organizativas que cumpram os requisitos legais nesta matéria, em particular no que tange à segurança do tratamento. O n.º 5 do mesmo dispositivo salienta que o subcontratante pode comprovar o cumprimento das exigências legais por via da desmonstração do cumprimento de um código de conduta ou um procedimento de certificação mencionados nos artigos 40.º e 42.º do RGPD, respetivamente.

O artigo 28.º, n.º 3 do RGPD regimenta pormenorizadamente a forma e o conteúdo do contrato que rege a relação entre o responsável pelo tratamento e o subcontratante, tendo previsto a possibilidade de a Comissão estabelecer cláusulas contratuais-tipo relativamente ao se conteúdo essencial.[282]

De acordo com o artigo 28.º, n.º 4, a subcontratação num outro subcontratante está sujeita a autorização escrita do responsável pelo tratamento e rege-se pelo contrato celebrado entre o responsável pelo tratamento e subcontratante.

4.1.3. RESPONSÁVEIS CONJUNTOS

O artigo 26.º, n.º 1, 1.ª parte, do RGPD prevê que**,** nas situações em que dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento.

O mesmo entendimento era já extraível do conceito de «responsável pelo tratamento», estatuído no artigo 4.º, ponto 7 do RGPD, onde se prevê a possibilidade de uma pluralidade de sujeitos. Este conceito admite a determinação conjunta das finalidades e/ou meios de tratamento, i.e., que duas ou mais entidades (pessoas singulares ou coletivas, uma autoridade pública, uma agência ou outro organismo), sejam consideradas responsáveis pelo tratamento.[283]

Envolvendo várias entidades pode, todavia, suceder que a cada uma das partes sejam reconhecidos diferentes níveis de controlo da finalidade e/ou dos meios de tratamento, bem como a sua intervenção pode ocorrer em diferentes momentos do tratamento. Nessa medida, e sem prejuízo do facto de cada uma delas ser autónoma no que tange

[282] O que verificou com a publicação da Decisão de Execução (UE) 2021/915 da Comissão, de 4 de junho de 2021, relativa às cláusulas contratuais-tipo entre os responsáveis pelo tratamento de dados pessoais e os subcontratantes nos termos do artigo 28.º , n.º 7, do RGPD e do artigo 29.º , n.º 7, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, disponível em:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021D0915&from=EN [acedido em 07.09.2023].

[283] PINHEIRO, Alexandre [et al.] – *Comentário ao Regulamento (…),* ob. cit., p. 408.

à faculdade de determinação das finalidades e dos meios de tratamento, a repartição diferenciada das obrigações demanda uma regulamentação formal da relação de tratamento, efetivada pelo acordo previsto no artigo 26.º, n.ºs 1 e 2. [284]

Com efeito, como refere MENEZES CORDEIRO, no regime de imputação e repartição de responsabilidades são regulados os tratamentos conjuntos de dados, não sendo necessário que todas as partes:

> *"(…) contribuam com a mesma intensidade. Todavia, o disposto no art.º 26.º é claro ao exigir que cada um deles esteja envolvido no processo de determinação das finalidades e dos meios: podem estar envolvidos em diferentes fases desse tratamento e em diferentes graus*". E, acrescenta o mesmo Autor, que "*É irrelevante se apenas um dos sujeitos têm o controlo físico do sistema que procede aos tratamentos ou se, para o exterior, tudo se desenrola como se o tratamento fosse realizado por apenas um responsável. Os propósitos prosseguidos podem não ser os mesmos, mas deverá existir um qualquer tipo de relação (…)*". [285] [286]

Nestes termos, é possível que mais do que uma parte tenha uma influência decisiva sobre se e como o tratamento ocorre - através de uma decisão comum[287] ou através de decisões convergentes[288] que se complementam e são necessárias para o tratamento pelo facto de terem um impacto tangível na determinação das finalidades e dos meios.[289]

Quanto ao conteúdo do contrato, o RGPD estabelece algumas obrigações e possibilidades dos responsáveis conjuntos em relação aos titulares dos dados e à autoridade de controlo, devendo o acordo, designadamente: (i) refletir corretamente as

---

[284] *Ibidem*

[285] CORDEIRO, A. Barreto Menezes - *Direito da Proteção de Dados (…), ob cit.,* pp. 311-314;

[286] Sobre este assunto importa sublinhar que o facto de uma das partes não ter acesso aos dados pessoais tratados não é suficiente para excluir a responsabilidade conjunta pelo tratamento. Veja-se, sobre o assunto, o Acórdão do TJUE, de 10.07.2018, processo C-25/17 «Testemunhas de Jeová», ECLI:EU:C:2018:551, n.º 75, disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=342512 [acedido em 07.09.2023], onde se considerou que uma comunidade religiosa deve ser considerada conjuntamente responsável com os seus membros pregadores pelo tratamento efetuado por estes últimos no âmbito de uma atividade de pregação porta a porta. Entendeu o Tribunal que não era necessário que a comunidade tivesse acesso aos dados em questão, ou devesse ser demonstrado que essa comunidade deu orientações escritas ou instruções a respeito desse tratamento aos seus membros. A comunidade participou na determinação das finalidades e dos meios, organizando e coordenando as atividades dos seus membros, o que ajudou a alcançar o objetivo da comunidade de testemunhas de Jeová. Além disso, a comunidade tinha, de um modo geral, conhecimento de que tais tratamentos se verificaram para efeitos da divulgação da sua fé.

[287] Significa decidir em conjunto e compreende a existência de uma intenção comum de acordo.

[288] Resulta da jurisprudência do TJUE sobre o conceito de responsáveis conjuntos pelo tratamento. As decisões podem ser consideradas convergentes em relação às finalidades e aos meios se forem complementares e forem necessárias para que o tratamento se realize de tal modo que têm um impacto tangível na determinação das finalidades e dos meios do tratamento e não se relacionam com outros aspetos da relação comercial entre as partes. Para identificar decisões convergentes devemos questionar se o tratamento não seria possível sem a participação de ambas as partes nas finalidades e nos meios no sentido de que o tratamento por cada uma das partes é indissociável, ou seja, intrinsecamente ligado.

[289] CEPD, Orientações 07/2020*, cit*.

funções e relações dos responsáveis conjuntos em relação aos titulares dos dados, em particular no que diz respeito ao exercício dos direitos do titular dos dados e aos seus deveres de prestação de informações previstas nos artigos 13.º e 14.º [290]; (ii) O conteúdo do acordo deve ser disponibilizado ao titular dos dados, assegurando que este conhecimento da «essência do acordo»; (iii) indicar um ponto de contacto para os titulares dos dados, conforme previsto no artigo 26.º, n.º 1, pese embora não tenha caráter obrigatório; (iv) a forma como comunicarão com as autoridades competentes de controlo da proteção dos dados, que pode incluir a consulta prevista no artigo 36.º do RGPD, a notificação de uma violação de dados pessoais e a designação de um encarregado da proteção de dados.

Os titulares dos dados, independentemente dos termos do acordo, podem exercer os seus direitos em relação e cada um dos responsáveis pelo tratamento, nos termos do artigo 26.º, n.º 3.

Relativamente à responsabilidade conjunta e à sua articulação com a responsabilidade do RT na esfera da Administração Pública, importa referir que, decorrente das atribuições que são legalmente acometidas às entidades públicas, não raras vezes a lei estabelece uma tarefa ou impõe a obrigação de recolha e tratamento de determinados dados. Nessas situações, embora indiretamente, estabelece quem é o responsável pelo tratamento, pelo que a análise da determinação da responsabilidade conjunta demanda uma apreciação rigorosa e casuística.

4.1.4. O EPD/DPO NAS ENTIDADES PÚBLICAS: DESIGNAÇÃO (OBRIGATÓRIA) E FUNÇÕES

O EPD desempenha um papel fundamental na garantia de conformidade com o RGPD, na medida em que está no escopo das suas competências garantir que o responsável pelo tratamento cumpre todas as obrigações legais nesta matéria, sendo o ponto de contacto da entidade com a autoridade de controlo nacional e funcionando como mediador junto do titular dos dados.[291] [292]

[290] O modo como as obrigações são organizadas no acordo devem espelhar cabalmente a realidade subjacente ao tratamento.

[291] MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão, ob. cit., p. 55.

[292] O artigo 39.º, n.º 1 do RGPD estabelece o conteúdo funcional mínimo do EPD, i.e., informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações; controlar a conformidade do RGPD com outras disposições de proteção de dados e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes; prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlar a sua realização nos termos do artigo 35.º; cooperar com a autoridade de controlo; constituir-se como ponto de contacto para a autoridade de controlo sobre questões relacionadas com o

Com efeito, o artigo 37.º, n.º 1, al. a) do RGPD determina a designação obrigatória de um EPD sempre que o tratamento de dados seja efetuado por uma autoridade ou um organismo público, excetuando os tribunais[293] no exercício da sua função jurisdicional[294].

A LE, por seu turno, estabelece no seu artigo 12.º, os critérios que regem essa designação**,** determinando no seu n.º 3 que, independentemente de quem seja o responsável pelo tratamento**,** existe, pelo menos, um EPD: (i) por cada ministério ou área governativa, no caso do Estado, sendo designado pelo respetivo ministro, com faculdade de delegação em qualquer secretário de Estado que o coadjuvar[295]; (ii) Por cada secretaria regional, no caso das regiões autónomas, sendo designado pelo respetivo secretário regional, com faculdade de delegação em dirigente superior de 1.º grau[296]; (iii) por cada município, sendo designado pela câmara municipal, com faculdade de delegação no presidente e subdelegação em qualquer vereador[297]; (iv) Nas freguesias em que tal se justifique, nomeadamente naquelas com mais de 750 habitantes, sendo designado pela junta de freguesia, com faculdade de delegação no presidente; (v) Por cada instituto público, entidade administrativa independente, Banco de Portugal, Instituição de ensino superior público, empresa do Estado e dos setores empresariais regionais e locais, e associação pública, sendo designado pelo respetivo órgão executivo, de administração ou gestão, com faculdade de delegação no respetivo presidente[298].

Sem prejuízo do que precede, o artigo 12.º, n.º 4 da LE refere que pode ser designado o mesmo EPD para vários ministérios ou áreas governativas, secretarias regionais, autarquias locais ou outras pessoas coletivas públicas, em conformidade com o determinado pelo artigo 37.º, n.º 3 do RGPD.

Relativamente perfil do EPD, importa evidenciar que**,** nos termos do disposto no artigo 37.º, n.º 5 do RGPD, deve este ser designado:

> *"(…) com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de*

tratamento, incluindo a consulta prévia a que se refere o artigo 36.º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.

[293] De acordo com o Considerando (97) do RGPD, o conceito de «tribunal» deve ser interpretado em sentido lato, de modo a incluir todas as autoridades judiciais independentes.

[294] Para MENEZES CORDEIRO, *Direito da Proteção de Dados (…), ob. cit.*, p. 361, da menção «no exercício da sua função jurisdicional» apenas pode resultar que no exercício das demais funções, v.g. administrativas, é necessária a designação de um EPD.

[295] *Crf*. Artigo 12.º, n.º 3 al. a) da LE.

[296] *Crf*. Artigo 12.º, n.º 3 al. b) da LE.

[297] *Crf*. Artigo 12.º, n.º 3 al. c) da LE.

[298] *Crf*. Artigo 12.º, n.º 1 e n.º 3, al. d) do mesmo artigo da LE.

dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39.º".[299]

Não obstante, resulta claro do artigo 12.º n.º 1 da LE que os requisitos necessários à designação do EPD são os previstos no artigo 37.º, n.º 5 do RGPD, "*não carecendo de certificação profissional para o efeito*".

O incumprimento da obrigação de nomear um EPD, constitui contraordenação grave punida com coima nos termos do artigo 38.º da LE[300].

4.2. A SEGURANÇA DOS DADOS PÚBLICOS

4.2.1. ENQUADRAMENTO LEGAL DOS REQUISITOS DE SEGURANÇA

A temática da segurança da informação, incluindo dos dados pessoais, apela à realidade prática da fidedignidade da informação e do acesso à mesma "(…) *que pode ser obrigatório, conforme ou não conforme à lei e, se desconforme, pode configurar mesmo, entre outros ilícitos, um crime e, como já foi dito (Snowden), até um crime contra a humanidade*". [301]

A legislação nacional e europeia aprovada nas últimas décadas tem evidenciado preocupações em assegurar a segurança da informação, em particular a segurança das redes e da informação, interoperabilidade digital e privacidade de dados pessoais,

[299] O Considerando (97) do RGPD complementa os requisitos descritos, salientando que o responsável pelo tratamento deve ser assistido por "*um especialista em legislação e prática de proteção dados no controlo do cumprimento do presente regulamento a nível interno*" e "[o] *nível necessário de conhecimentos especializados deverá ser determinado, em particular, em função do tratamento de dados realizado e da proteção exigida para os dados pessoais tratados pelo responsável pelo seu tratamento ou pelo subcontratante*".

[300] Em conformidade com o previsto no artigo 44.º, n.º 2 e n.º 3 da LE, durante três anos a contar da sua entrada em vigor, *i.e*, 09.08.2022, as entidades públicas podiam solicitar à CNPD, mediante pedido devidamente fundamentado, dispensa da aplicação da coima, facto que não prejudica a aplicação os demais poderes de correção da CNPD.

[301] A fidedignidade e a segurança da informação comportam três elementos essenciais: a autoria, a genuinidade e a integridade, tanto que, para além do crime de falsificação, no Código Penal, até a tutela nos novos domínios digitais foi reforçada com a previsão específica do crime de falsidade informática, na Lei do Cibercrime. Por outro lado, a ilegitimidade de acesso aos dados armazenados num sistema informático pode constituir, entre outros, um crime de acesso ilegítimo estatuído na Lei n.º 109/2009, de 15 de Setembro, no seu artigo 6.º, ou um crime de violação de correspondência ou de telecomunicações previsto no artigo 194.º do Código Penal, em particular no seu n.º 2, ou, ainda, um crime de violação de segredo de correspondência ou de telecomunicações de acordo com o disposto nas alíneas a) a c) do artigo 384.º do Código Penal, designadamente quando estejamos perante funcionário de serviços de telecomunicações, e, claro, consoante as circunstâncias e se estivermos a falar do direito interno. *Cfr.* ABREU, Carlos Pinto de. *Breves notas sobre segurança da informação, acesso a dados e privacidade*. C&R - Revista de Regulação e Concorrência. Lisboa, n. 35, 2018, p. 48, disponível em: https://www.concorrencia.pt/sites/default/files/imported-magazines/CR_35_Carlos_Pinto_de_Abreu.pdf [acedido em 12.09.2023].

respetivamente: RNID - Regulamento Nacional de Interoperabilidade Digital, Diretiva UE 2016/1148 e Regulamento (UE) 2016/679. [302]

O artigo 32.º do RGPD estabelece um dever de segurança no tratamento dos dados pessoais, que deve ser assegurado quer pelo responsável pelo tratamento, quer pelo(s) subcontratante(s), caso exista(m).

Este dever de aplicar medidas técnicas e organizativas adequadas a assegurar a segurança dos dados acha-se positivado no artigo 32.º, n.º 1 do RGPD, sendo a manifestação do mais amplo dever de tratamento dos dados conforme o direito aplicável (perspetiva formal) e em respeito pelos direitos à autodeterminação informacional dos titulares dos dados (perspetiva material).[303]

Este dever decorre, conforme se verificou, da aplicação do princípio da integridade e da confidencialidade, previsto no 5.º, n.º 1, al. f) do RGPD, sendo exigível que o responsável pelo tratamento adote as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco[304] competindo-lhe, ainda, nos termos do artigo 5.º, n.º 2 do RGPD, demonstrar que cumpre as exigências legais nesta matéria, i.e., que as atividades de tratamento de dados da sua organização acompanham os princípios de tratamento de dados. É o designado princípio da Responsabilidade Pró-ativa ou de *Accountability*[305]. Por conseguinte, o responsável pelo tratamento, nos termos do prescrito pelo artigo 24.º, n.º 1 do RGPD, considera a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e

[302] SANTOS, Luísa Varandas dos; MARQUES, Mário Monteiro. Gestão de Risco Aplicada à Segurança da Informação. Cyberlaw by CIJIC – Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa. Lisboa, n. 7, 2019. Disponível em: https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_7.pdf [acedido em 12.09.2023]

[303] CORDEIRO; António Menezes – *Comentário ao Regulamento (…),* ob. cit., p. 268.

[304] Cfr. artigo 32.º, n.º 1 e considerando (83), ambos do RGPD.

[305] Este princípio viu o seu reconhecimento explícito, enquanto «dever de prestar contas» sobre o cumprimento das medidas que põem em prática os princípios [materiais] acima enunciados, nas diretrizes da Organização de Cooperação e Desenvolvimento Económico (OCDE) regulamentadoras da proteção da vida privada, adotadas em 1980. Em 2010, a Opinião 3/2010 sobre o Princípio da Responsabilidade Pró-ativa ou do *Accountability* do Grupo de trabalho do Artigo 29.º reforçou esse entendimento. Em 2015, também a CNIL (*Commission Nationale Informatique et Libertés*) aprovou uma norma de cumprimento em matéria de proteção de dados, no qual define as regras e as normas que devem gerir (implantar e desenvolver) uma organização para garantir uma gestão eficaz em consonância com os princípios de proteção de dados. Com efeito, entendeu aquela entidade que as organizações que demonstrarem cumprir com o legalmente determinado, serão distinguidas com um selo de cumprimento do princípio da responsabilidade pró-ativa", por esta emitido. Este desenvolvimento marca uma distinção em relação ao que foi a pretensão do legislador na Diretiva da CE de 95 em relação ao RGPD**,** porquanto a pretensão inicial era evitar a infração dos direitos dos interessados e o princípio consignado no RGPD é antecipar o cumprimento como forma de evitar a lesão ou violação dos direitos dos titulares. Trata-se de uma questão relevante na medida em que a não adoção de alguma das medidas ou a violação de alguma obrigação imposta pelo RGPD pode ocasionar uma sanção sem que se verifique, sequer, a existência de uma lesão dos direitos, liberdades dos titulares dos dados. Cfr. RAMOS, Fernando, *El principio de Accountability o de Responsabilidad Proactiva*, DPO & It Law, 2017. Disponível em: El principio de Accountability o de Responsabilidad Proactiva - DPO & it law (dpoitlaw.com) [acedido em 04.10.2023].

gravidade podem ser variáveis**,** aplicando "(…) *as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades*.".

As aludidas medidas devem, ainda, nos termos do artigo 25.º, n.º 1, ser aplicadas desde a conceção e por defeito, tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis. O responsável pelo tratamento emprega, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do RGPD e proteja os direitos dos titulares dos dados.

Sucede, porém, que o RGPD, ao remeter para a aplicação das «medidas técnicas e organizativas adequadas» limita-se a definir conceitos genéricos**,** não se vislumbrando a obrigatoriedade de aprovação de normas de segurança vinculativas.

Regista-se, além do mais, uma omissão quanto à metodologia que as Organizações devem adotar para implementar processos de gestão de risco, deixando a cargo das mesmas a adoção de processos de cerificação voluntários que possam contribuir para o cumprimento da legislação em vigor na prevenção contra ameaças. Assim, a maior parte das entidades tem recorrido às normas standard ISO "Internacional Organization for Standardization. [306] [307]

Nesta conformidade, as medidas a adotar devem ser determinadas em função de critérios casuísticos, resultantes das análises de risco a que aludem os artigos 25.º, n.ºs 1 e 2 e 32.º, n.º 1, ambos do RGPD, ou, encontrando-se preenchidos os pressupostos para a realização das avaliações de impacto previstas no artigo 35.º. [308]

[306] SANTOS, Luísa Varandas dos; MARQUES, Mário Monteiro, *ob. cit.,* p. 14.

[307] Mormente as normas da «família» ISO/IEC 27000, cujo objetivo é o de "(…) proporcionar os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação". Compreende diversas normas específicas, destacando-se a ISO/IEC 27001 (Bases para a implementação de um SGSI em uma organização), a ISO/IEC 27002 (Certificação profissional), a ISO 27017 (orientações sobre medidas de segurança da informação para computação em cloud) ou a ISO/IEC 27005 (Norma sobre gestão de riscos do SGSI). *Cfr.* NP EN ISO/IEC 27000:2018 — Information technology: Security techniques — Information security management systems — Overview and Vocabulary. Disponível em: Padrões disponíveis publicamente (iso.org) [acedido em 05.10.2023].

[308] Nesse sentido, MASSENO, Manuel David – Segurança na proteção dados, algumas reflexões. Webinar 3 anos de aplicação do RGPD: Balanço, Perspetivas Futuras e Boas Práticas na Administração Pública. CCDR. Algarve. 26.05.2021, disponível em

Alguns esquemas autorregulatórios, como códigos de conduta[309] ou a certificação[310] [311]podem ser concebidos por entidades com competência legal para representar determinados setores de atividade, como uma forma eficiente de apoio no cumprimento das disposições do RGPD de forma, i.e., correspondendo às especificidades próprias daquele setor, sendo eventualmente eficaz em termos de custos. [312] A aprovação de códigos de conduta está sujeita a procedimentos de supervisão pela Comissão Nacional de Proteção de Dados, com supervisão à escala europeia pela Comissão, sem prejuízo desta última poder dotar códigos de conduta de aplicabilidade geral na UE ou aprovar normas técnicas e regras para reconhecer as certificações [313].

Sobre este assunto importa, todavia, salientar que a observância dos códigos de conduta, não obstante nos termos do disposto no artigo 32.º, n.º 3 do RGPD, sirva para demonstrar o cumprimento das obrigações, não isenta uma entidade de eventuais responsabilidades, sem prejuízo do facto de, na aplicação da coima ser considerado o grau de responsabilidade do responsável pelo tratamento ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos 25.º e 32.º.[314]

---

https://ipbeja.academia.edu/ManuelDavidMasseno/Privacy,-Cybersecurity-and-Cybercrime-Laws [acedido em 24.09.2023].

[309] Previstos nos artigos 40.º (códigos de conduta) e 41.º (supervisão dos códigos de conduta) do RGPD. Sobre este assunto, importa atender às Diretrizes n.º 1/2019, do CEPD, relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679, Versão 2.0, de 4 de junho de 2019. Disponíveis em: edpb_guidelines_201901_v2.0_codesofconduct_pt.pdf (europa.eu) [acedido em 24.09.2023].

[310] Prevista nos artigos 42.º (certificação) e 43.º (organismos de certificação) do RGPD.

[311] Quando uma operação de tratamento por um responsável pelo tratamento ou subcontratante é certificada em conformidade com o artigo 42.º, os elementos que contribuem para demonstrar a conformidade com o artigo 25.º, n.ºs 1 e 2, são os processos de conceção, ou seja, o processo de determinação dos meios de tratamento, a governação e as medidas técnicas e organizativas para aplicar os princípios de proteção de dados. Os critérios de certificação da proteção de dados são determinados pelos organismos de certificação ou pelos proprietários de sistemas de certificação e, em seguida, aprovados pela autoridade de controlo competente ou pelo CEPD. *Cfr.* Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados desde a Conceção e por Defeito Versão 2.0 Adotadas em 20 de outubro de 2020, p. 31. Disponível em: EDPB_Guidelines_20201020_Art25DataProtectionbyDesignbyDefault_V2.0_PT.docx (europa.eu) [acedido em 24.09.2023].

[312] Conforme o previsto no artigo 40.º, n.º 2, do RGPD, os códigos de conduta podem regimentar, mormente, acerca do: (i) tratamento equitativo e transparente; (ii) dos legítimos interesses dos responsáveis pelo tratamento em contextos específicos; (iii) da recolha de dados pessoais; a pseudonimização dos dados pessoais; (iv) da informação prestada às pessoas e o exercício dos direitos das pessoas; (v) das informações prestadas às crianças e a sua proteção (incluindo procedimentos para obter o consentimento dos pais); (vi) das medidas técnicas e organizativas, incluindo a proteção de dados «desde a conceção» e «por defeito» e medidas de segurança; (vii) da notificação de violações; (viii) da transferência de dados para países terceiros; ou (ix) dos procedimentos de resolução de litígios.

[313] Com efeito, a Comissão pode, através de um ato de execução, decidir que um código transnacional aprovado será de aplicabilidade geral na União, e deve assegurar a publicidade adequada, caso essa aplicabilidade seja declarada. *Cfr.* CEPD, Diretrizes n.º 1/2019, *cit*., p. 23.

[314] Cfr. Considerando (81) e artigo 83.º, n.º 2, al. d) do RGPD.

Nesta conformidade, no que tange em concreto às medidas de segurança dos dados específicas para a Administração Pública**,** insta evidenciar o disposto no artigo 29.º, n.º 7 da LE[315], que refere que no âmbito do tratamento de dados de saúde e dados genéticos, "[a]*s medidas e os requisitos técnicos mínimos de segurança inerentes ao tratamento de dados são aprovados por portaria dos membros do Governo responsáveis pelas áreas da saúde e da justiça (…)"*, bem como os preceitos constantes da Resolução do Conselho de Ministros n.º 41/2018, de 28 de março[316], que aprova os requisitos técnicos mínimos das redes e sistemas de informação[317] e procedimentos a adotar de modo a cumprir as normas do RGPD.

Todavia, conforme referido, inexistindo ainda normas de segurança completas que cubram integralmente o RGPD, reveste utilidade significativa a ISO 27001 [318], que define um sistema de gestão de segurança de informação de acordo com a estrutura organizacional, com as políticas, as atividades de planeamento, as responsabilidades, as práticas, os procedimentos, os processos e os recursos.[319] [320] A ISO 27001 detém

[315] Em cumprimento do prescrito pelo artigo 9.º. n.º 4 do RGPD, que prevê que os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde.

[316] Publicado em *Diário da República*, série I, n.º 62, de 28.03.2018, p.p. 1424-1430.

[317] A RCM 41/2018, de 28 de março vincula apenas a Administração Direta do Estado, sem prejuízo da mesma poder ser empregue noutros domínios como referencial normativo, conforme se refere na respetiva nota justificativa, onde se dispõe que o Governo recomenda a adoção daquelas medidas pelo setor empresarial do Estado.

[318] A norma ISO/IEC 27001 visa a adoção, pelas organizações, de um conjunto de requisitos, processos e controlos com o objetivo de mitigar e gerir adequadamente os riscos da organização.

[319] *Cfr*. PINHEIRO, Alexandre [et al.] – *Comentário ao Regulamento (…), ob.cit.,* p. 449.

[320] A norma integra duas componentes, na primeira acham-se definidas as regras e os requisitos de cumprimento da norma e a segunda (Anexo) compreende um conjunto de controlos que as organizações devem adotar, em diferentes áreas e nas mais diversas temáticas da segurança da informação, desde a governação com a definição de políticas da segurança da informação, ao cumprimento das obrigações legais nas matérias da segurança da informação e ainda da privacidade. A problemática da proteção de dados pessoais integra um dos *items* relativos à conformidade, através do disposto no controlo A.18.1.4 – Privacidade e proteção de dados pessoais. As extensões desta norma, *v.g.* ISO/IEC 27002:2013 (Tecnologia da informação – técnicas de segurança – código de boas práticas para a gestão da segurança da informação), revistas e completadas pela norma ISO/IEC 27701:2019 (Técnicas de segurança - Extensão das normas ISO/IEC 27001:2022 Segurança da informação, cibersegurança e proteção da privacidade — Sistemas de gestão de segurança da informação — Requisitos e da ISO/IEC 27002:2022 Segurança da informação, segurança cibernética e proteção da privacidade - Controlos de segurança da informação. Também outras normas revestem significância na implementação de um processo de gestão de risco, tais como a ISO/IEC 31000 – *Risk management*. Nesse sentido, vd. GT29, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, p. 20. Disponível em: wp248 rev.01 pt (cnpd.pt) [Acedido em 10.10.2023], onde se refere que "*O considerando 90 do RGPD enuncia vários elementos da AIPD que se sobrepõem a elementos bem definidos da gestão do risco (p. ex. ISO 31000). Em matéria de gestão dos riscos, uma AIPD destina-se a «gerir os riscos» para os direitos e as liberdades das pessoas singulares, utilizando os seguintes processos: - estabelecendo o contexto: «tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco»; - avaliando os riscos: «avaliar a probabilidade ou gravidade particulares do elevado risco»; - dando resposta aos riscos: «atenuar esse risco» e «assegurar a proteção dos dados pessoais» e «comprovar a observância do presente regulamento»*".

inúmeros requisitos em comum com o RGPD, a saber: (i) Classificação de dados[321]; (ii) Cooperação com as autoridades[322]; (iii) Gestão de Ativos[323]; (iv) Proteção de dados logo no início do processo[324]; Registo de Atividades[325].

A este respeito importa registar que a avaliação do risco de privacidade comporta duas dimensões que devem ser consideradas, a individual e a organizacional. Do exposto decorre a necessidade de avaliar o impacto do risco de privacidade não só para o titular dos dados, mas também para a organização, sendo possível efetuar duas abordagens, i.e., a abordagem baseada em eventos (análise macroscópica) e a abordagem baseada em ativos (análise detalhada dos ativos, ameaças e vulnerabilidades).[326]

No que respeita ao anexo A da versão em vigor, que descreve os controlos (preventivos, detetivos e corretivos) de segurança a adotar para tratamento dos riscos de segurança de informação, importa salientar que a mesma está organizada da seguinte forma: i) A.5 Controlos Organizacionais (37 controlos); ii) A.6 Controlos Pessoais (8 controlos); iii) A.7 Controlos Físicos (14 controlos); A.8 Controlos Tecnológicos (34 controlos). Em relação à versão anterior, foram introduzidos 11 novos controlos relativos «Threat Intelligence»; «Segurança da Informação para Uso de Serviços na Cloud»; «Prontidão de TIC para a Continuidade de Negócio»; «Monitorização da Segurança Física»; «Gestão de Configurações»; «Eliminação da Informação»; «Mascaramento de Dados»; «Prevenção de Fuga de Dados»; «Atividades de Monitorização»; «Filtragem Web» e «Código Seguro».[327]

Para além das normas standard identificadas é ainda de atender ao regime jurídico em matéria cibersegurança, aprovado pela Lei n.º 46/2018, de 13 de agosto, que

[321] Os processos de implementação da ISO 27001 e do RGPD implicam a classificação de dados de acordo com o nível de importância, sendo que quanto mais importantes forem, mais protegidos devem ser.

[322] Ambos os diplomas preveem a cooperação com as autoridades competentes nesta matéria de proteção da informação, comprometendo-se a notificar eventuais violações.

[323] A ISO 27001 e o RGPD têm como finalidade a adequada gestão dos ativos organizacionais e definem responsabilidades, i.e., ambos identificam os dados recolhidos, a sua origem, acesso e local de armazenamento.

[324] Ambos definem processos de segurança da informação desde a conceção e por defeito.

[325] A documentação de aspetos fundamentais do processo de gestão da informação é exigida na ISO 27001 e no RGPD, demonstrando o seu comprometimento com a segurança e privacidade dos dados recolhidos. Ao exposto acresce ainda, entre outros, a necessidade de consentimento explicito; a formação e sensibilização dos trabalhadores.

[326] Esta última encontra-se alinhada com a ISO/IEC 27005:2022 - Segurança da informação, segurança cibernética e proteção da privacidade — Orientação sobre gestão de riscos de segurança da informação, e consiste em identificar os ativos, as ameaças, os controlos existentes, as vulnerabilidades e as consequências. Relativamente aos ativos importa salientar, os dados pessoais, os sistemas de informação que tratam dados pessoais, as bases de dados que contenham dados pessoais, os hardwares que tratam dados pessoais e outros, tais como a reputação da entidade.

[327] Cfr. ISO/IEC 27001:2022.

estabelece o regime jurídico da segurança do ciberespaço [328], o Decreto-Lei n.º 65/2021, de 30 de julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança[329] e a Lei n.º 93/2021, de 20 de dezembro, que estabelece o regime legal de proteção de denunciantes de infrações[330].

A respeito do regime jurídico da segurança do ciberespaço importa ainda evidenciar que o seu âmbito de aplicação, previsto no artigo 2.º da supramencionada Lei, abrange toda a Administração Pública[331], bem como as entidades mencionadas no artigo 2.º, n.º 1, alíneas b) a e) [332] encontrando-se a primeira e os operadores de infraestruturas críticas, nos termos do artigo 14.º, n.º s 1 e 2 do normativo em questão, juridicamente vinculados à adoção das medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, as quais devem garantir um nível de segurança adequado ao risco, tendo em conta os progressos técnicos mais recentes.

Nesta conformidade, sem prejuízo do facto de os requisitos de segurança serem os definidos nos termos previstos em legislação própria (*cfr*. art.º 12.º, n.º 1), permite-se "*(…) a utilização de normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia.",* designadamente as normas ISO/IEC 27001 e ISO/IEC 27002 (*Cfr.* art.º 12.º n.º 3).

[328] Transpondo a Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União [Diretiva NIS / SRI], prevê a definição de requisitos de segurança, através de "legislação própria" (Art.º 12.º n.º 1).

[329] Em execução do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019.

[330] Em cujo artigo 2.º, n.º 1 integra, no conceito de infração, qualquer "*ato ou omissão contrário a regras constantes dos atos da União Europeia referidos no anexo da Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, a normas nacionais que executem, transponham ou deem cumprimento a tais atos ou a quaisquer outras normas constantes de atos legislativos de execução ou transposição dos mesmos, incluindo as que prevejam crimes ou contraordenações, referentes aos domínios de: (…) x) Proteção da privacidade e dos dados pessoais e segurança da rede e dos sistemas de informação;".*

[331] Que inclui (i) o Estado; (ii) As regiões autónomas; (iii) As autarquias locais; (iv) As entidades administrativas independentes; (v) Os institutos públicos; (vi) As empresas públicas e (vii) as associações públicas, conforme artigo 2.º, n.º 1, al. a) e n.º 2.

[332] Mormente, os operadores de infraestruturas críticas; os operadores de serviços essenciais; os prestadores de serviços digitais e quaisquer outras entidades que utilizem redes e sistemas de informação.

4.2.2. MEDIDAS TÉCNICAS E ORGANIZATIVAS A ADOTAR PELO RESPONSÁVEL PELO TRATAMENTO E PELO SUBCONTRATANTE

4.2.2.1. A PSEUDONIMIZAÇÃO, A ANONIMIZAÇÃO E A CIFRAGEM

A segurança da informação na sociedade digital moderna constitui condição *sine qua non* para a implementação das regras do RGPD, exigindo o maior investimento possível por parte das organizações, não só em sistemas mais modernos, seguros e eficazes, mas também em termos de recursos humanos.

A segurança da informação compreende e segurança física e a segurança lógica, englobando a recolha, consentimento, tratamento, transferência, arquivos físicos e digitais, destruição, i.e., todo o ciclo de vida de um determinado dado pessoal. [333]

Como se viu, o artigo 32.º do RGPD associa a segurança dos dados pessoais aos direitos e liberdades das pessoas singulares, exigindo que as entidades, através do RT ou subcontratante**,** apliquem as medidas técnicas e organizativas adequadas para assegurar um nível de segurança ajustado ao risco, e destinadas a aplicar com eficácia os princípios da proteção de dados.

Nesta sede relevam, desde logo, os princípios da minimização dos dados e da limitação da conservação previstos no artigo 5.º, n.º 1, alíneas c) e d), respetivamente, que determinam que os dados pessoais tratados devem ser os «adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados» e ser «conservados de forma que permita a identificação dos titulares apenas durante o período necessário para as finalidades para as quais são tratados». Estas medidas aplicam-se não só à quantidade dos dados recolhidos, mas também à extensão do tratamento, ao prazo de conservação e à acessibilidade assegurando que, por defeito, os dados não sejam disponibilizados, sem intervenção humana, a um número indeterminado de pessoas singulares.

Assim, visando a preservação dos direitos dos titulares dos dados e a minimização dos riscos de quebra da privacidade, o RGPD introduz um conceito de gestão do tratamento de dados pessoais baseado num maior controlo sobre todas as fases do tratamento, i.e., desde a recolha até à eliminação. E, sem prejuízo da previsão da necessidade de eliminação dos dados logo que atingidas as finalidades do tratamento (ou o prazo legal da respetiva conservação), também aconselha algumas medidas técnicas e organizativas.

[333] Saldanha, Nuno. *RGPD: Guia para uma auditoria de conformidade. Dados, Privacidade, Implementação, Controlo e Compliance.* FCA Editora de Informática, Lda. Lisboa. 2019, p. 131.

A pseudonimização consiste no tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável. [334]

Esta técnica facilita o cumprimento dos deveres impostos pelo RGPD e permite reduzir os riscos de divulgação, podendo ser alcançada de um modo simples, v.g., com a separação dos dados e a sua colocação debaixo da alçada de diferente sujeito ou entidades. Distingue-se da anonimização porquanto, nesta última, não é tecnicamente possível identificar o titular dos dados.[335]

Sem prejuízo de se tratar de uma técnica legalmente prevista e potencialmente aplicável, entre outras, para "*fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos*", conforme previsto no artigo 89.º n.º 1 do RGPD, comporta riscos de re-identificação maiores que a anonimização, nomeadamente quanto à "inversão não autorizada da pseudonimização"[336] tornando necessária, ou muito aconselhável, uma pseudonimização forte, incluindo os quase-identificadores[337], já próxima das técnicas de cifragem. [338] [339]

A anonimização é uma técnica aplicada aos dados pessoais com a finalidade de atingir uma desidentificação irreversível. Pressupõe que os dados tenham sido recolhidos e tratados em conformidade com a legislação aplicável relativa à conservação de dados num formato identificável. Neste contexto, o processo de anonimização, ou seja, o tratamento de dados pessoais para atingir a respetiva anonimização, constitui um tratamento posterior.[340] O RGPD é omisso quanto a esta

[334] *Cfr.* artigo 4.º, n.º 5 do RGPD. Os Considerandos (26), (28), (29), (75), (78), (85) e (156) do RGPD também sugerem a utilização desta medida.
[335] Neste sentido, CORDEIRO; António Menezes – *Comentário ao Regulamento (…), ob. cit.,* p. 87-88.
[336] De acordo com o Considerando (26) do RGPD, os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica.
[337] Combinações de atributos relacionados com um titular dos dados ou um grupo de titulares dos dados. *Cfr.* Parecer n.º 5/2014 do GT 29 sobre as técnicas de anonimização (WP 216), p. 13, disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf [acedido em 02.10.2023].
[338] *Ibidem.* p. 24-25.
[339] Nesse sentido, MASSENO, Manuel David, *cit*.
[340] Neste sentido, vd. Parecer 05/2014 do GT29, cit., p. 7.

técnica. [341] Já a Lei n.º 26/2016, de 22 de agosto, que aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos e a LE do RGPD, ambas transpostas para o ordenamento jurídico de Diretivas do Parlamento Europeu e do Conselho, aludem à técnica da anonimização sem, contudo, procederem à sua definição.[342]

Nos termos do artigo 4.º, n.º 1 do RGPD "*é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador (…)*". Ora, conforme dispõe o Considerando (26) do RGPD, *in fine:*

> "*(…) Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação*."

Atendendo a que, com a evolução tecnológica**,** passou a ser possível a reidentificação[343] e que o legislador não definiu o conceito de anonimização sem possibilidade de reversão, conclui-se que se trata de uma técnica arriscada e a sua aplicação carece de medidas de gestão de risco a um nível elevado. [344] Do exposto resulta que sempre que a tecnologia permita uma identificação, ainda que potencial, pois o critério é de ser uma pessoa "identificável", é de aplicar o regime jurídico da proteção de dados pessoais, do qual emerge a responsabilidade do responsável pelo tratamento, nos termos já elencados.

No setor público, para se avaliar os riscos de reidentificação, entre outros, devem ser ponderados os seguintes fatores/conceitos: (i) outros dados que estejam à disposição do público em geral ou de outros indivíduos ou organizações e a suscetibilidade de os dados a publicar poderem ser associados a outros conjuntos de dados; (ii) a probabilidade de serem efetuadas tentativas de reidentificação (alguns tipos de dados

[341] Sem prejuízo, o considerando (26) da Diretiva 95/46/CE, ao dispor que «*para anonimizar quaisquer dados, têm de lhes ser retirados elementos suficientes para que deixe de ser possível identificar o titular dos dados. Mais precisamente, os dados têm de ser tratados de forma que já não possam ser utilizados para identificar uma pessoa singular utilizando «o conjunto dos meios suscetíveis de serem razoavelmente utilizados*» previa a definição da mesma, seja pelo responsável pelo tratamento, seja por terceiros".

[342] Neste sentido, *vd.* GUIMARÃES, Rui [et al] - Reutilização de Registos Clínicos para Investigação Científica: Questões Jurídicas Relacionadas com a Autorização dos Titulares e a Anonimização. Ata Med. Port. 2018 jun. p. 299. Disponível em: https://doi.org/10.20344/amp.10147 [acedido em 02.10.2023].

[343] Mormente com base nas analíticas de *Big Data*, sobretudo através de correlações com outros conjuntos de dados disponíveis. Para uma melhor compreensão sobre o assunto, sugere-se a leitura do Parecer 6/2013, de 5 de junho do GT 29, sobre a dados abertos e reutilização de informações do setor público (ISP) e o Parecer n.º 5/2014, de 10 de abril, sobre as técnicas de anonimização.

[344] Cfr. MASSENO, Manuel David, *cit.*

despertarão mais o interesse de potenciais intrusos do que outros); e (iii) a probabilidade de sucesso de eventuais tentativas de reidentificação, tendo em conta a eficácia das técnicas de anonimização propostas. Uma vez feita a avaliação dos riscos de reidentificação, depois de realizado o teste da reidentificação, o organismo do setor público está em condições de decidir se o conjunto de dados pode ser considerado anonimizado, ou seja, se já não contém dados pessoais.[345]

Por outro lado, a cifragem de dados pessoais (criptografia) corresponde ao ato de criar códigos que permitem que determinado dado seja mantido em segredo, i.e., converte dados e informações num formato que somente poderá ser descodificado por utilizadores que possuírem autorizações, impedindo o acesso a informações sensíveis por aqueles que não sejam devidamente autorizados[346]. Pese embora sem definição legal, a técnica surge mencionada: (i) no artigo 6.º, n.º 4, al. e) do RGPD, a respeito do tratamento de dados para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos e não tenham sido realizados com base no consentimento do titular; (ii) no artigo 32.º, n.º 1, al. a), sobre segurança no tratamento; (iii) no artigo 4.º, n.º 12) genericamente, acerca do conceito de «violação de dados pessoais» e; (iv) no artigo 34.º, n.º 3, al. a), sobre a aplicação das medidas de proteção adequadas aos dados pessoais afetados pela violação de dados pessoais. Embora seja suscetível de assegurar a confidencialidade dos dados**,** não garante a integridade e disponibilidade, daí que as medidas de segurança devam ter um caráter cumulativo, de modo a que seja possível assegurar a confidencialidade, a integridade, a disponibilidade e a resiliência permanentes dos sistemas e dos serviços de tratamento; a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; e incluam um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.[347]

Sem prejuízo, esta técnica é institucionalmente recomendada na União Europeia, ainda que no domínio da *soft law*. É o caso do Conselho, como mostra a Resolução do Conselho sobre encriptação – Segurança através da encriptação e segurança apesar

[345] Parecer 6/2013 do GT29, sobre a dados abertos e reutilização de informações do setor público (ISP), de 05.06.2013, p. 16 e 19, disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_pt.pdf [acedido em 02.10.2023].

[346] LEAL, Victor Moreira Mulin. A tecnologia Blockchain como plataforma de interoperabilidade na União Europeia? Um estudo a partir da Decisão (UE) 2015/2240**.** *In* SILVEIRA, Alessandra; ABREU, Joana R. S. Covelo; COELHO, Larissa (Eds.). UNIO Ebook Interop 2019: O Mercado Único Digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: Pensamento Sábio - Associação para o conhecimento e inovação / Universidade do Minho - Escola de Direito, p.29, disponível em: https://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf [acedido em 02.10.2023].

[347] Conforme preceitua o artigo 32.º, n.º 1 do RGPD.

da encriptação.[348] [349] No mesmo sentido, regista-se também a Diretiva UE 2022/2055 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022[350], relativa às medidas destinadas a assegurar um elevado nível comum de cibersegurança em toda a União[351] e que abrange o setor da Administração Pública (a nível central tal como definidas pelos Estados-Membros em conformidade com o direito nacional), bem como a Carta Portuguesa de Direitos Humanos na Era Digital[352], que refere expressamente "*Todos têm direito a comunicar eletronicamente usando a criptografia e outras formas de proteção da identidade ou que evitem a recolha de dados pessoais, designadamente para exercer liberdades civis e políticas sem censura ou discriminação*."[353], reforçando os direitos fundamentais à privacidade nas comunicações e à proteção de dados pessoais. Sem prejuízo, teria sido recomendável a sua qualificação como uma lei de bases, para que a mesma fosse suscetível de produzir "*plenos efeitos transformadores do nosso ordenamento (Art.ºs 34.º n.º 4, 35.º e 112.º n.º 2, da Constituição da República)*". [354]

4.2.2.2. OUTRAS MEDIDAS ORGANIZATIVAS E DE SEGURANÇA

Várias entidades e Autores tomaram a iniciativa de divulgar um conjunto de medidas que se constituem como «boas práticas» a adotar nesta matéria, sem prejuízo da ausência de natureza vinculativa das mesmas.

Desde logo, a CNPD[355], enquanto autoridade de controlo nacional e na prossecução das respetivas atribuições[356], atendendo aos frequentes ataques a sistemas de

[348] Disponível em: pdf (europa.eu) [acedido em 02.10.2023].
[349] Insta ressalvar que a cifragem «forte», pelas implicações que pode ter em termos de segurança e combate à criminalidade, é avaliada de diferentes perspetivas pelas Instituições e das agências da União Europeia, como ocorreu, reiteradamente, com a Declaração Conjunta da Europol e da ENISA, de 20 de maio de 2016, sobre "uma investigação criminal lícita que respeite a proteção dos dados no século XXI", a Resolução sobre "a luta contra a cibercriminalidade", do Parlamento Europeu, de 3 de outubro de 2017 (2017/2068(INI) e, mais ainda, a "Declaração sobre a cifragem e o seu impacto na proteção das pessoas singulares [físicas] relativamente ao tratamento dos seus dados pessoais na EU", de 11 de abril de 2018, do GT 29. Nesse sentido, *vd.* MASSENO, Manuel David. A segurança dos dados na LGPD brasileira: uma perspetiva europeia, desde Portugal. Revista do Direito. Santa Cruz do Sul, v. 3, n. 50, jan./abr. 2020. ISSN 1982-9957, p. 96, disponível em: https://cejur.emnuvens.com.br/cejur/article/view/346/181 [acedido em 02.10.2023].
[350] Publicada no Jornal Oficial da UE a 27 de dezembro de 2022.
[351] Que visa harmonizar e reforçar as obrigações em matéria de cibersegurança e de notificação em caso de incidente estabelecendo, entre outras, medidas destinadas a alcançar um elevado nível de resiliência das entidades críticas para assegurar a prestação de serviços essenciais no território a União e melhorar o funcionamento do mercado interno. (*cfr.* artigo 1.º, n.º 1, al. e)).
[352] Aprovada pela Lei n.º 27/2021, de 17 de maio.
[353] *Cfr.* artigo 8.º, n. º 1.
[354] MASSENO, Manuel David. Segurança na proteção dados, algumas reflexões (…) *cit***.**
[355] DIRETRIZ/2023/1 da CNPD, sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais, disponível em: https://www.cnpd.pt/decisoes/diretrizes/ [acedido em 08.10.2023].
[356] Nomeadamente a definida na alínea d) do n.º 1 do artigo 57.º do RGPD, em conjugação com o artigo 3.º da LE.

informação verificados nos últimos anos, entendeu oportuno sensibilizar os responsáveis pelos tratamentos e os subcontratantes para as suas obrigações no domínio da segurança dos tratamentos de dados pessoais[357]. Preveniu, todavia, para o facto de estas medidas não possuírem um caráter exaustivo e serem forçosamente dinâmicas, pela sua direta dependência do desenvolvimento tecnológico, estando, por isso, sujeitas a eventuais futuras e oportunas atualizações.

Assim, devem os RT adaptar os seus modelos de negócio ou de gestão pública e os respetivos meios técnicos e organizativos para assegurar o efetivo cumprimento da lei e a devida proteção dos dados pessoais e da esfera de interesses, direitos e liberdades dos titulares dos mesmos. Para tal, serão úteis as normas ISO/IEC já mencionadas, quer na avaliação de risco para a privacidade ou na avaliação de impacto na privacidade.[358]

Sem prejuízo do que antecede, tendo em vista o cumprimento das obrigações previstas no artigo 32.º, n.ºs 1 e 2, do RGPD, consoante o que for adequado às características e sensibilidade dos tratamentos de dados pessoais efetuados e às especificidades da organização, sugere a CNPD a aplicação de medidas relativas à segurança do tratamento de dados pessoais, divididas em duas partes: (i) medidas organizativas (quinze)[359] e (ii) medidas técnicas, estas últimas demarcadas entre medidas de autenticação (duas) [360], medidas relacionadas com infraestrutura e

[357] Decorrentes da exploração ilícita (i) das vulnerabilidades das infraestruturas, da falta de formação dos utilizadores para detetarem campanhas de *phishing* que permitem depois a distribuição de *malware*, com especial relevância para os ataques de *ransomware* e (ii) da ausência de consciencialização dos responsáveis pelos tratamentos quanto aos riscos para os direitos dos titulares dos dados que a falta de investimento em mecanismos de segurança acarreta.

[358] Privacy Impact Assessment – PIA, que**,** de acordo com a norma ISO/IEC 29001:2011 (ISO/IEC, 2011b)**,** é um "*processo de identificação, análise e avaliação dos riscos no que diz respeito ao processamento de dados pessoais identificáveis*".

[359] Sumariamente elencadas: 1) Definir e exercitar regularmente o plano de resposta a incidentes e recuperação do desastre; 2) Classificar a informação de acordo com o nível de confidencialidade e sensibilidade e adotar as medidas organizativas e técnicas adequadas à classificação; 3) Documentar as políticas de segurança; 4) Adotar procedimentos de análise para a monitorização dos fluxos de tráfego na rede; 5) Definir políticas de gestão de palavras-passe seguras; 6) Criar uma política de gestão de ciclo de vida dos utilizadores; 7) Adotar alarmística que permita identificar situações de acesso, tentativas ou utilização indevida; 8) Definir, numa fase inicial, as melhores práticas de segurança de informação a adotar, quer em fase de desenvolvimento de software, quer em fase de testes de aceitação; 9) Realizar auditorias de segurança de TI e avaliações de vulnerabilidade (testes de penetração) sistemáticos; 10) Verificar se as medidas de segurança definidas estão em prática, garantindo que são eficazes e atualizando-as regularmente; 11) Documentar e corrigir as vulnerabilidades de segurança detetadas sem demora; 12) Tomar as medidas necessárias para garantir o pleno cumprimento do artigo 33.º do RGPD, em particular no que diz respeito ao desenvolvimento de uma política interna para lidar e documentar eventuais violações de dados pessoais; 13) Fomentar junto dos colaboradores uma cultura de privacidade e segurança da informação; 14) Dar a conhecer aos trabalhadores o dever de confidencialidade a que estão sujeitos pelo facto de tratarem dados pessoais; 15) Avaliar periodicamente as medidas de segurança, técnicas e organizativas, internas e proceder à sua atualização e revisão sempre que necessário.

[360] 1) Utilizar credenciais fortes com palavras-passe longas; 2) Equacionar a aplicação de autenticação multifator.

sistemas (quatro)[361], medidas respeitantes a ferramentas de correio eletrónico (nove)[362], medidas de proteção contra malware (três)[363] medidas sobre utilização de equipamentos em ambiente externo (oito)[364], medidas sobre armazenamento de documentos em papel que contenham dados pessoais (cinco)[365] e medidas sobre transporte de informação que integre dados pessoais (duas).[366]

Não obstante, podem também servir de referencial os contributos para a adequação das organizações ao RGPD, publicados pelo Gabinete Nacional de Segurança[367], que

[361] 1) Garantir que os sistemas operativos de servidores e terminais se encontram atualizados, bem como todas as aplicações (por exemplo, browser e plugins); 2) Manter atualizado o firmware dos equipamentos de rede; 3) Desenhar e organizar os sistemas e a infraestrutura por forma a segmentar ou isolar os sistemas e as redes de dados para prevenir a propagação de malware dentro da organização e para sistemas externos; 4) Robustecer a segurança dos postos de trabalho e servidores, através do bloqueio a acesso a sítios inseguros, dos redireccionamentos suspeitos através de motores de busca, ficheiros e aplicações infetadas com malware; realizar inspeção periódica do estado e utilização dos recursos do sistema monitorizar a utilização do software instalado; ativar e conservar os registos de auditoria (log); validar os acessos por IP aos servidores que estão expostos ao público; alterar o porto configurado por omissão para o protocolo de acessos remotos (RDP).

[362] 1) Definir de forma clara e inequívoca políticas e procedimentos internos sobre o específico envio de mensagens de correio eletrónico contendo dados pessoais; 2) Equacionar a criação de listas de distribuição ou grupos de contacto, com o objetivo de prevenir a divulgação dos endereços dos destinatários em operações de envio massivo de mensagens de correio eletrónico; 3) Equacionar a criação de regras com o objetivo de adiar/atrasar a entrega de mensagens de correio eletrónico contendo dados pessoais, mantendo-as na 'Caixa de Saída' por um tempo determinado, permitindo verificações de conformidade, após clique em 'Enviar'; 4) Encriptar com código, ao qual só o destinatário tenha acesso, os emails e/ou anexos enviados que contenham dados pessoais; 5) Confirmar com o destinatário, antes de envio de e-mail contendo dados pessoais, o endereço de email preferencial para contacto; 6) Realizar ações de formação no sentido de capacitar os trabalhadores a operar os mecanismos de envio de mensagens de correio eletrónico de acordo com os procedimentos definidos, sensibilizando-os para os erros mais comuns, potencialmente suscetíveis de originar violações de dados pessoais e incentivando-os à dupla verificação; 7) Reforçar o sistema de alerta da ferramenta de alarmística utilizada pela entidade, para assegurar visibilidade imediata sobre a criação por utilizadores de regras de encaminhamento automático de e-mails para contas externas; 8) Reforçar o sistema com ferramentas antiphishing e antispam, que permitam bloquear ligações e/ou anexos com código malicioso; 9) Adotar controlos de segurança que permitam classificar e proteger as mensagens de correio eletrónico sensíveis.

[363] 1) Utilizar encriptação segura especialmente no caso de credenciais de acesso, de dados especiais, de dados de natureza altamente pessoal ou de dados financeiros; 2) Criar um sistema de cópias de segurança (backup) atualizado, seguro e testado, totalmente separado das bases de dados principais e sem acessibilidade externa; 3) Reforçar o sistema com ferramentas antimalware que inclua a capacidade de o verificar e detetar, bem como o bloqueio em tempo real de ameaças do tipo ransomware.

[364] 1) Armazenar dados em sistemas internos, protegidos com medidas de segurança apropriadas, e acessíveis remotamente através mecanismos de acesso seguro (VPN); 2) Permitir acessos apenas por VPN; 3) Bloquear as contas após várias tentativas inválidas de login; 4) Ativar a autenticação multifator para os utilizadores dos equipamentos; 5) Aplicar cifragem dos dados no sistema operativo; 6) Sempre que for aplicável, ativar a funcionalidade de "remote wipe" e "find my device"; 7) Efetuar cópias de segurança automáticas das pastas de trabalho, quando o equipamento se encontra ligado à rede da entidade; 8) Definir regras claras e adequadas para a utilização de equipamentos em ambiente externo.

[365] 1) Utilizar papel e impressão que seja durável; 2) Conservar documentação em local com controlo de humidade e temperatura; 3) Armazenar, devidamente organizados, os documentos que contêm dados pessoais sensíveis em local fechado, resistente ao fogo e inundação; 4) Controlar os acessos, com registo das respetivas data e hora, de quem acede e do(s) específico(s) documento(s) acedido(s). 5) Destruir os documentos através de equipamento específico que garanta a destruição "segura";

[366] 1) Adotar medidas para impedir que, no transporte de informação com dados pessoais, estes possam ser lidos, copiados, alterados ou eliminados de forma não autorizada; 2) Utilizar encriptação segura no transporte, em dispositivos de massa ou arquivo potencialmente permanente (CD/DVD/PEN USB).

[367] O Manual de Boas Práticas em matéria de Proteção de Dados do GNS divide-se em três partes, a saber: Parte I - Deveres e Responsabilidades das Organizações; Parte II - Contributos para Políticas e

reúne conceitos, informações e metodologias, com base nas melhores práticas adotadas na União Europeia e NATO relativas à segurança da informação e que deve ser entendido como um complemento aos requisitos técnicos mínimos que visam garantir uma arquitetura de segurança das redes e sistemas de informação que constam da Resolução de Conselho de Ministros nº. 41/2018 e outros disponíveis.[368]

Procedimentos e Parte III - Segurança Física, disponível em: GNS - Gabinete Nacional de Segurança [acedido em 08.10.2023].

[368] V.g., Saldanha, Nuno*, ob. cit*., 2019, p.p. 131-139.

5. CONCLUSÕES

O percurso evolutivo do direito à privacidade permite-nos evidenciar uma alteração de perspetiva da tutela da pessoa e uma crescente adequação ao desenvolvimento tecnológico. Com efeito, com o presente estudo foi possível demonstrar que a atual conceção do direito à proteção de dados surgiu da necessidade de proteger a privacidade individual - ou a reserva da vida privada -, por via do resguardo da informação de natureza pessoal, cujo tratamento exige maiores salvaguardas porquanto respeita à intimidade de cada indivíduo.

E se a ideia de privacidade surge originariamente nos EUA como uma manifestação de interesse individual em «ser deixado só» é, contudo, na Europa que a evolução legislativa que tutela este direito prospera, no contexto das barbáries cometidas contra integridade e dignidade do ser humano aquando da II.ª Guerra Mundial. Neste quadro, para além da proteção legal, o direito à privacidade reclama pela proteção moral de toda a sociedade e de todos os indivíduos que a constituem assentando, por isso, na dignidade da pessoa humana.

Foi patenteado que a evolução tecnológica despertou ainda mais para a defesa da vida privada e para a necessidade de a proteger e acomodar novas realidades, transformando-a num direito fundamental, de modo a impor uma efetiva organização legislativa e administrativa que garanta o direito à vida privada dos cidadãos e a proteção dos seus dados pessoais.

Por conseguinte, demonstrou-se que o desenvolvimento da personalidade confere ao indivíduo o direito de autodeterminação no que respeita à informação da esfera da sua vida privada, podendo este limitá-la de modo voluntário. Nestes termos, em função da personalidade individual e do caso concreto, poderão vislumbrar-se diferentes conceções do que é informação de natureza privada.

Assim, a atual perspetiva do direito decorre essencialmente da consciencialização acima aduzida e da concernente evolução legislativa ocorrida nos países europeus em quatro gerações legislativas, com início na celebração da CEDH, e demais instrumentos jurídicos evidenciados, destacando-se a relevante contribuição alemã no que tange ao desenvolvimento vivenciado nesta matéria.

Em resposta às progressivas ameaças à segurança dos dados das pessoas na sociedade da informação, ocasionadas pelo tendencialmente crescente tratamento automatizado de dados, o RGPD veio alterar o paradigma, introduzindo um conjunto de obrigações para as entidades que tratam dados pessoais, incluindo a Administração Pública.

Evidenciou-se que a maior parte dos dados pessoais tratados no setor público assentam no cumprimento de obrigações jurídicas ou na medida do necessário para realizar tarefas por motivos de interesse público ou no exercício de autoridade pública de que está investida.

Sem prejuízo, aquando do tratamento dos dados pessoais, estas entidades devem respeitar os princípios fundamentais estabelecidos no RGPD, nomeadamente o tratamento equitativo e lícito, limitação da finalidade, minimização dos dados e conservação dos dados**,** e informar previamente os titulares dos dados acerca do tratamento, nomeadamente as suas finalidades, os tipos de dados recolhidos, os destinatários dos dados e os seus direitos em matéria de proteção de dados.

Constatou-se, ademais, que é o responsável pelo tratamento quem deve assegurar o cumprimento destes princípios e demais desideratos aplicáveis e, bem assim, assegurar que o tratamento dos dados pessoais é realizado em conformidade com a lei, i.e., garantindo que são aplicadas as medidas técnicas e organizativas adequadas para proteger os dados pessoais. Se tal não se verificar, as entidades responsáveis pelo tratamento e/ou os seus representantes podem ser responsabilizados pelos danos causados ao titular dos dados.

Caso sejam subcontratadas partes do tratamento a uma organização externa, deve existir um contrato ou outro ato jurídico que garanta que o subcontratante apresenta garantias suficientes da aplicação de medidas técnicas e organizativas adequadas que cumpram as normas do RGPD.

As administrações públicas têm, ainda, a obrigação de nomear um encarregado da proteção de dados**,** embora seja possível nomear um único encarregado da proteção de dados para vários organismos públicos, que poderão**,** assim**,** partilhar os seus serviços ou subcontratar esta tarefa a um EPD externo.

Para garantir a segurança dos dados públicos, o responsável pelo tratamento considera a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados e, tem em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis. Em função desta apreciação - para além de assegurar a aplicação dos requisitos técnicos mínimos das redes e sistemas de informação exigidos ou recomendados a todos os serviços e entidades da Administração direta e indireta do Estado -, deve adotar uma série de medidas,

algumas delas exemplificadas no RGPD, que visam diminuir o risco de exposição dos titulares dos dados.

A este respeito, o artigo 32.º do RGPD preceitua que o responsável pelo tratamento e o subcontratante devem implementar medidas técnicas e organizacionais apropriadas para assegurar um nível de segurança adequado ao risco, designadamente, entre outros: i) a pseudonimização e encriptação dos dados pessoais; ii) a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos meios de tratamento; iii) a capacidade de reestabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; iv) um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Para que tal seja possível, é necessário adotar uma metodologia ajustada a cada realidade concreta, que permita identificar, responder e recuperar de incidentes que envolvam dados pessoais, adaptar-se e aprender com os mesmos, aumentando a resiliência dos sistemas de informação, de acordo com os padrões internacionais, sem prejuízo da eventual aplicação das medidas sugeridas pelas entidades competentes, mormente pela CNPD.

Trata-se da implementação de um sistema de controlo interno que permita relacionar as atividades diárias de tratamento de dados pessoais com a gestão do risco e que atue na cibersegurança, na segurança física e na segurança lógica.

Nesta matéria, o RGPD estimula o uso de esquemas de certificação constantes da família da norma ISO/IEC 27000, com o propósito de demonstrar que uma entidade gere ativamente a segurança dos dados pessoais tratados, por via da aplicação das práticas que têm evidenciado melhores resultados e se constituem como padrões internacionais.

Este esquema regulatório abrange três dimensões – pessoas, processos e tecnologia-, facilitando não só a defesa dos riscos tecnológicos, mas também outros tipos de vulnerabilidades e ameaças comuns, tais como, as decorrentes da falta de formação dos trabalhadores ou, até, da existência de procedimentos desadequados.

Com a implementação desta norma, as entidades beneficiam da obtenção de um sistema de gestão de segurança da informação permanentemente monitorizado, transversal e adaptado à própria estratégia e cultura.

A ISO 27001 aborda a importância da gestão da continuidade de negócios, fornecendo um conjunto de controlos que, não obstante a impossibilidade de obter a certificação,

podem servir de referencial, coadjuvando as entidades no sentido de acautelar a disponibilização indevida de dados pessoais em caso de incidente de segurança, protegendo a informação crítica.

Do mesmo modo, sendo aplicável a qualquer tipo de risco, a ISO 31000 pode, também, coadjuvar uma correta adequação ao RGPD porquanto descreve o processo de gestão dos riscos, fornecendo diretrizes para a respetiva administração. No quadro do RGPD, esta norma é basilar para a implementação de uma efetiva gestão de riscos, que permita identificar, analisar e tratar os riscos associados ao tratamento de dados pessoais.

Sem prejuízo, constituem-se como medidas organizativas e de segurança potencialmente empregáveis, as recomendadas pelas entidades competentes, bem como as sugeridas pela doutrina, desde que adequadas à finalidade que se pretende alcançar, i.e., a conformidade com o RGPD.

Os dados públicos – onde se incluem os dados pessoais recolhidos e tratados pela AP - constituem ativos críticos organizacionais que cumpre assegurar, protegendo-os de ameaças e vulnerabilidades, assegurando não só os direitos e liberdades dos titulares dos dados pessoais, mas também salvaguardando a continuidade e bom funcionamento da atividade do setor público, nomeadamente a prossecução das missões e atribuições legalmente acometidas a cada organismo do Estado.

Conclui-se, assim, que esta temática deve ser encarada de um modo holístico e o risco examinado em diferentes perspetivas, devendo existir um processo interno de mitigação que garanta o cumprimento normativo ou permita dirimir os riscos em função da probabilidade e impacto para a organização e para os titulares dos dados.

Esta análise e as medidas adotadas, quando coerentes em face do caso concreto, constituem evidências perante a autoridade de controlo, permitindo atenuar a responsabilidade do responsável pelo tratamento.

REFERÊNCIAS BIBLIOGRÁGICAS:

MANUAIS DOUTRINÁRIOS:

ANDRADE, José Carlos Vieira de - *Os direitos fundamentais na Constituição portuguesa de 1976.* 4.ª Ed. Coimbra: Almedina. 2009;

ASCENSÃO, José de Oliveira - A reserva da intimidade da vida priva e familiar. *Revista da Faculdade de Direito da Universidade de Lisboa*. Coimbra Editora, Vol. 43, n.º 1. 2002;

CADILHA, Carlos Alberto Fernandes - *Regime da responsabilidade civil extracontratual do Estado e demais entidades públicas: anotado* Coimbra: Coimbra Editora, 2008;

CAMPOS, Diogo Leite de. - *Direitos da Personalidade*. Lisboa: Associação Académica da Universidade Autónoma de Lisboa. 1991;

CANOTILHO, Gomes; MOREIRA, Vital - *Constituição da República Portuguesa Anotada*, Volume I, 4.ª edição, Coimbra, 2007;

CAUPERS, João - *A Responsabilidade do Estado e Outros Entes Públicos*, Faculdade de Direito da Universidade Nova de Lisboa;

CORDEIRO; António Menezes - *Tratado de Direito Civil IV***.** 4.ª Ed., rev. e atual. Coimbra: Almedina, 2017;

CORDEIRO; António Menezes - *Direito de proteção de dados à Luz do RGPD e da Lei n.º 58/2019.* Coimbra: Almedina. 2020;

CORDEIRO, A. Barreto Menezes [et al.] - Comentário ao regulamento geral de proteção de dados e à Lei nº 58/2019*.* - Coimbra: Almedina, 2021;

DRAY, Guilherme Machado - *Direitos de Personalidade*. Anotações ao Código Civil e ao Código do Trabalho Coimbra: Almedina. 2006;

MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão – *Regulamento geral de Proteção de Dados – Manual Prático.* Lisboa: Vida Económica Editorial. 2017;

NOVAIS, Jorge Reis - *A dignidade da pessoa humana: dignidade e inconstitucionalidade*. Vol. II, Coimbra: Almedina, 2017;

PINHEIRO, Alexandre Sousa - *Privacy e Proteção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional.* Lisboa: Faculdade de Direito da Universidade de Lisboa. 2011. Dissertação de Doutoramento em Ciências Jurídico-Políticas;

PINHEIRO, Alexandre [et al.] – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina. 2018;

PINTO, Carlos Mota - *Teoria Geral do Direito Civil*, 3.ª Ed. Atualizada. Coimbra: Coimbra Editora, 1996. ISBN 972-32-0383-9;

PINTO, Paulo Mota - *Direitos de Personalidade e Direitos Fundamentais: estudos*. 1.ª Edição. Coimbra: Gestlegal, 2018;

SALDANHA, Nuno. *RGPD: Guia para uma auditoria de conformidade. Dados, Privacidade, Implementação, Controlo e Compliance.* FCA Editora de Informática, Lda. Lisboa. 2019.

SAMPAIO, José Adércio Leite. Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998., p. 254. ISBN: 8573082178;

SOUSA, Rabindranath Capelo de - *O Direito Geral de Personalidade*, 1.ª ed. (reimpressão), Coimbra: Coimbra editora. 2011;

VASCONCELOS, Pedro Pais de - *Teoria Geral do Direito Civil*, 5.a ed., Coimbra: Almedina, 2008;

VASCONCELOS, Pedro Pais de - *Direito de Personalidade*. Coimbra: Almedina. 2014;

REBELO DE SOUSA, Marcelo; SALGADO DE MATOS, André, - *Direito Administrativo Geral - Atividade Administrativa*, Tomo III, 2ª edição (reimp.). Lisboa: D. Quixote. 2016.

ARTIGOS DE PUBLICAÇÕES EM SÉRIE:

LOPES, Teresa Vale – Responsabilidade e Governação das Empresas no âmbito do novo Regulamento sobre a Proteção de Dados, Anuário da Proteção de Dados, Coord. Francisco Pereira Coutinho / Graça Canto Moniz. Universidade Nova de Lisboa. Faculdade de Direito. CEDIS, Centro de I & D sobre Direito e Sociedade, Lisboa. 2018. ISBN: 978-972-99399-5-2;

GOMES, Manuel Januário da Costa - O problema da salvaguarda da privacidade antes e depois do computador. Boletim do Ministério da Justiça. Ministério da Justiça. Lisboa. N.319 (out.1982);

MONIZ, Graça Canto - Direitos do titular dos dados pessoais: o direito à portabilidade. Anuário da Proteção de dados. Coord. Francisco Pereira Coutinho / Graça Canto Moniz. Universidade Nova de Lisboa. Faculdade de Direito. CEDIS, Centro de I & D sobre Direito e Sociedade, Lisboa. 2018. ISBN: 978-972-99399-5-2;

TEIXEIRA, Maria Leonor - Proteção de dados e big data: Os desafios líquidos do pós-panoptismo. Revista do Ministério Público. Lisboa. N.º 159 (jul./set. 2019);

DOCUMENTOS ELETRÓNICOS:

Agência dos Direitos Fundamentais da União Europeia - Manual da Legislação Europeia sobre Proteção de Dados [em linha]. Luxemburgo: Serviço das Publicações da União Europeia (2022), disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_pt.pdf ISBN 978-92-871-9825-9;

ASCENÇÃO, José de Oliveira - A dignidade da pessoa e o fundamento dos direitos humanos. Estudos em Homenagem ao Prof. Doutor Martim de Albuquerque. Revista da Ordem dos Advogados (ROA) [Em linha]. Ano 68, Vol. I. (2008). Disponível em: https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados-roa/ano-2008/ano-68-vol-i/doutrina/jose-oliveira-ascensao-a-dignidade-da-pessoa-e-o-fundamento-dos-direitos-humanos/;

BARBOSA, Mafalda Miranda. Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil – Revista de Direito comercial [Em linha]. 2018, p. 439, disponível em: 1 (squarespace.com)

CORREIA, Victor - Sobre o direito à Privacidade. O Direito [Em linha]. Almedina: Lisboa. Ano 146.º, n.º 1 (2014), disponível em: https://www.cidp.pt/revistas/direito/O%20Direito%20(2014)%20I%20TEXTO.PDF;

COOLEY, Thomas - A treatise on the law of torts, or the wrongs which arise independent of contract. Callaghan and company [Em linha]. Chicago (1879), disponível em: https://repository.law.umich.edu/books/11/

CRUZ, Marco Aurélio Cunha e; MENDES, Marina Letycia - Aproximações do paradigma libertário do "right to privacy" norte-americano. Revista Brasileira de Direito Civil em Perspetiva [Em linha]. Curitiba. Volume 2, N.º 2 (Jul./Dez. 2016), disponível em: Aproximações do Paradigma Libertário do "Right to Privacy" Norte-Americano | Cruz | Revista Brasileira de Direito Civil em Perspectiva (indexlaw.org). e-ISSN: 2526-0243;

DIAS FERREIRA, Diogo - Trabalhador, reserva da intimidade da vida privada e «redes sociais. Nótulas reflexivas sobre um delicado problema juslaboral, Revista da Ordem dos Advogados [Em linha]. Lisboa. Ano 80 (Jul./Dez. 2020), p. 586**,** disponível em: https://portal.oa.pt/media/132093/diogo-figueiredo-perfeito-dias-ferreira.pdf;

DONEDA, Danilo - Da privacidade à proteção dos dados pessoais [Em linha]. Rio de Janeiro: Renovar, (2006), disponível em: https://www.academia.edu/23345535/Da_privacidade_%C3%A0_prote%C3%A7%C3%A3o_de_dados_pessoais;

DONEDA, Danilo - A Proteção dos dados pessoais como um direito fundamental. Revista Espaço Jurídico [em linha], Joaçaba, Vol. 12, n.º 2 (jul./dez. 2011), disponível em: https://www.researchgate.net/publication/277241112_A_protecao_dos_dados_pessoais_como_um_direito_fundamental/link/5934045faca272fc553c4abe/download;

FERRAZ JUNIOR, Tércio Sampaio - Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Cadernos de direito constitucional e ciência política [Em linha]. Ano 1. São Paulo: Revista dos Tribunais (1992), disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231;

GLANCY, Dorothy - The invention of the right to privacy. Arizona Law Review [Em linha]. Vol. 21, n.º 1 (1979), disponível em: https://law.scu.edu/wp-content/uploads/Privacy.pdf;

GODKIN, Edward L. - The rights of the citizen, IV – to his own reputation. *Scribner´s Magazine*, Vol. 8, n. 1 (1890), *apud* SEIPP, David J. - The Right to Privacy in Nineteenth Century America. Harvard Law Review [Em linha]. Vol. 94, (1981), p. 1909. Disponível em https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=2613&context=faculty_scholarship;

GUIMARÃES, Rui [et al] - Reutilização de Registos Clínicos para Investigação Científica: Questões Jurídicas Relacionadas com a Autorização dos Titulares e a Anonimização. Ata Med. Port. (jun 2018), disponível em: https://doi.org/10.20344/amp.10147;

HIRATA, Alessandro - Direito à privacidade. Enciclopédia jurídica da PUC-SP [Em linha]. Coord. De Celso F. Campilongo, Alvaro A. Gonzaga e André L. Freire. Tomo: Direito Administrativo e Constitucional. 1.ª Ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade;

LEAL, Victor Moreira Mulin. A tecnologia Blockchain como plataforma de interoperabilidade na União Europeia? Um estudo a partir da Decisão (UE) 2015/2240**.** *In* SILVEIRA, Alessandra; ABREU, Joana R. S. Covelo; COELHO, Larissa (Eds.). UNIO Ebook Interop 2019: O Mercado Único Digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: Pensamento Sábio - Associação para o conhecimento e inovação / Universidade do Minho - Escola de Direito, disponível em:

https://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf;

MACEDO, Fernanda; BUBLITZ, Michelle; RUARO, Regina - A privacy norte-americana e a relação com o direito brasileiro. Revista Jurídica Cesumar [Em linha]. Vol. 13, n.º 1 (jan./jun. 2013), p. 161-178. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/2666/1898; ISSN 1677-64402;

MASSENO, Manuel David. A segurança dos dados na LGPD brasileira: uma perspetiva europeia, desde Portugal**.** Revista do Direito. Santa Cruz do Sul, v. 3, n. 50, jan./abr. 2020. ISSN 1982-9957, p. 96, disponível em: https://cejur.emnuvens.com.br/cejur/article/view/346/181;

MASSENO, Manuel David – Segurança na proteção dados, algumas reflexões. Webinar 3 anos de aplicação do RGPD: Balanço, Perspetivas Futuras e Boas Práticas na Administração Pública. CCDR Algarve.26.05.2021, disponível em: (99+) Da segurança na proteção dados, algumas reflexões [na Administração Pública portuguesa] | Manuel David Masseno - Academia.edu

NETO, Eugênio Facchini - A noção de privacy na jurisprudência da suprema corte norte-americana: existe um conceito unificador? Revista de Direito Brasileira [Em linha]. Vol. 25, N.º 10 (2020) Florianólopis, SC. p.419-420. Disponível em: A NOÇÃO DE PRIVACY NA JURISPRUDÊNCIA DA SUPREMA CORTE NORTE-AMERICANA: EXISTE UM CONCEITO UNIFICADOR? | Neto | Revista de Direito Brasileira (indexlaw.org)

OTERO, Paulo - *Causas de exclusão da responsabilidade civil extracontratual da Administração Pública por facto ilícito*. Faculdade de Direito da Universidade de Lisboa. Lisboa. 2021. Disponível em: Causas de exclusao da responsablidade.pdf (ulisboa.pt)

PEIXOTO, Erick L. C.; JÚNIOR, Marcos E. – Breves Notas Sobre a Ressignificação da Privacidade. Revista Brasileira de Direito Civil – RBDCivil [Em linha]. Vol. 16. (Abr./jun.2018) Belo Horizonte, p. 39. Disponível em: https://www.academia.edu/36820607/BREVES_NOTAS_SOBRE_A_RESSIGNIFICA%C3%87%C3%83O_DA_PRIVACIDADE_BRIEF_NOTES_ON_THE_RESSIGNIFICATION_OF_PRIVACY

Presidência do Conselho de Ministros: Gabinete Nacional de Segurança. RGPD e a Segurança das Redes e Sistemas de Informação [Em linha]. Parte I, II e III (2018), disponível em: GNS - Gabinete Nacional de Segurança;

RAMOS, Fernando, *El principio de Accountability o de Responsabilidad Proactiva*, DPO & It Law, 2017. Disponível em: El principio de Accountability o de Responsabilidad Proactiva - DPO & it law (dpoitlaw.com);

SANTOS, Luísa Varandas dos; MARQUES, Mário Monteiro. Gestão de Risco Aplicada à Segurança da Informação. Cyberlaw by CIJIC – Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa. Lisboa, n. 7, 2019. Disponível em: https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_7.pdf

WARREN, Samuel D.; BRANDEIS, Louis D. – The Right to privacy. Harvard Law Review [Em linha]. Vol. 4, n.º 5 (Dez.1980) pp. 193-220, disponível em: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents

ZANINI, Leonardo – O surgimento e o desenvolvimento do *right of privacy* nos Estados Unidos. Revista Jurídica Luso-Brasileira [Em linha]. Centro de Investigação do Direito Privado. Lisboa. Ano 1, N.º 4 (2015), pág. 791. Disponível em https://www.cidp.pt/revistas/rjlb/2015/4/2015_04_0791_0817.pdf ISSN: 2183-539X.

JURISPRUDÊNCIA:

Acórdão do Tribunal Europeu dos Direitos do Homem (TEDH), de 18.11.2008, petição n.º 22427/04, *Cemalettin Canli c.* Turquia, disponível em: CEMALETTİN CANLI c. TURQUIE (N° 2) (coe.int)

Acórdão do Tribunal de Justiça da União Europeia (TJUE), de 16.12.2008, Processo C-73/07, *Satamedia*, disponível em: eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62007CJ0073

Acórdão do Tribunal de Justiça da União Europeia (TJUE), de 07.05.2009, processo C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=74028&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=597837

Acórdão do Tribunal de Justiça da União Europeia (TJUE), de 13.05.2014, processo C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GS]*, disponível em: eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0131

Acórdão do Tribunal de Justiça da União Europeia (TJUE), de 10.07.2018, processo C-25/17 «*Testemunhas de Jeová*», disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=342512

Acórdão do Supremo Tribunal de Justiça (STJ), de 03.03.2010, Proc. n.º 886/07.8PSLSB.L1.S1 (relator Santos Cabral), disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/25061d49157a048c8025770a002ed7d7?OpenDocument;

Acórdão do Supremo Tribunal de Justiça (STJ), de 23.12.2012, Processo 1674/07.7TVLSB.P1.S1 (relator Távora Vítor), disponível em: Acórdão do Supremo Tribunal de Justiça (dgsi.pt)

Acórdão do Supremo Tribunal de Justiça (STJ), de 30.05.2019, Processo n.º 336/18.4T8OER.L1.S1 (relator Catarina Serra), disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/32d36f4f4a970a598025840a00511a7f?OpenDocument;

Acórdão do Supremo Tribunal Administrativo (STA), de 09.10.2014 , Processo n.º 0279/14 (relator Costa Reis), disponível em: Acordão do Supremo Tribunal Administrativo (dgsi.pt);

Acórdão do Tribunal da Relação de Lisboa (TRL), de 23.02.2017, Processo n.º 23019/16.5T8LSB.L1-8 (relator Isoleta Almeida Costa), disponível em: Acórdão do Tribunal da Relação de Lisboa (dgsi.pt);

LEGISLAÇÃO:

Declaração Universal dos Direitos Humanos (DUDH) da Organização das Nações Unidas, de 10 de dezembro de 1948. [Em linha]. Publicações das Nações Unidas. [Acedido em 25.12.2022]. Disponível em: PT-UDHR-v2023_web.pdf (unric.org);

Convenção Europeia dos Direitos do Homem (CEDH) do Conselho da Europa, de 4 de novembro de 1950. [Em linha]. Conselho da Europa. [Acedido em 27.12.2022]. Disponível https://www.echr.coe.int/Documents/Convention_POR.pdf;

Convenção para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais (ETS 108), do Conselho da Europa, 28 de janeiro de 1981. [Em linha]. Conselho da Europa. [Acedido em 05.02.2023]. Disponível em: https://rm.coe.int/1680078b37;

Convenção Modernizada para a Proteção de Indivíduos em Relação ao Tratamento de Dados Pessoais (Convenção108+) do Conselho da Europa, de 18 de maio de 2018. [Em linha]. Conselho da Europa. [Acedido em 18.04.2023]. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf;

Regulamento (CE) n.º 45/2001 do Parlamento Europeu e Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao

tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. [Em linha]. JO n.º L 008 de 12/01/2001 p. 0001 – 0022. [Acedido em 09.02.2023]. Disponível em: EUR-Lex - 32001R0045 - EN - EUR-Lex (europa.eu);

Regulamento (UE) 2016/679 do Parlamento Europeu e Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. [Em linha]. JOUE n.º L 119/1, de 04.05.2016 [Acedido pela última vez em 10.12.2023]. Disponível em: REGULAMENTO (UE) 2016/ 679 DO PARLAMENTO EUROPEU E DO CONSELHO - de 27 de abril de 2016 - relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/ 46/ CE (Regulamento Geral sobre a Proteção de Dados) (europa.eu);

Diretiva 2002/58/CE do Parlamento Europeu e Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas). [Em linha]. JO n.º L 201 de 31/07/2002, p. 0037 – 0047 [Acedido pela última vez em 09.02.2023]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002L0058;

Diretiva 2006/24/CE do Parlamento Europeu e Conselho, de 15 de março de 2006, 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. [Em linha]. JO n.º L 105, 13.04.2006, p. 54–63. [Acedido em 09.02.2023]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32006L0024;

Diretiva 95/46/CE, de 24 de outubro de 1995 do Parlamento Europeu e Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. [Em linha]. JO n.º L 281 de 23.11.1995, [Acedido pela última vez em 10.12.2023]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046;

Resolução n.º (73) 22 do Comité de Ministros do Conselho da Europa, de 26 de setembro de 1973, relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor privado. [Em linha]. Conselho da Europa. [Acedido em 21.01.2023]. Disponível em https://rm.coe.int/1680502830;

Resolução n.º (74) 29 do Conselho da Europa, de 20 de setembro de 1974, relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de

dados no setor público. [Em linha]. Conselho da Europa. [Acedido em 21.01.2023]. Disponível em: https://rm.coe.int/16804d1c51;

Decisão de Execução (UE) 2021/915 da Comissão, de 4 de junho de 2021, relativa às cláusulas contratuais-tipo entre os responsáveis pelo tratamento de dados pessoais e os subcontratantes nos termos do artigo 28.º, n.º 7, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho e do artigo 29.º, n.º 7, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho [Em linha]. JO n.º L 199, de 07.06.2021, pp. 18-30 [Acedido em 07.09.2023]. Disponível em: EUR-Lex - 32021D0915 - EN - EUR-Lex (europa.eu);

The Privacy Act of 1974 of Senate and House of Representatives of the United States of America [Em linha]. Public Law 93-579, as codified at 5 U.S.C. 552ª. [Acedido em 02.01.2023]. Disponível em: https://dpcld.defense.gov/Portals/49/Documents/Privacy/pa1974.pdf;

Resolução da Assembleia da República n.º 23/93, de 09/07, que aprova, para ratificação, a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal [Em linha]. *Diário da República,* Série I-A, n.º 159, de 9 de julho de 1993. [Acedido em 07.02.2023]. Disponível em: Resolução da Assembleia da República n.º 23/93 | DR (diariodarepublica.pt);

Lei n.º 58/2019 da Assembleia da República, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [Em linha]. *Diário da República,* Série I, n.º 151/2019, de 8 de agosto de 2019 [Acedido em 16.03.2023]. Disponível em: Lei n.º 58/2019 | DR (diariodarepublica.pt);

Lei n.º 26/2016 da Assembleia da República, de 22 de agosto, que aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos [Em linha]. *Diário da República*, Série I, n.º 160, de 22 de agosto de 2016 [Acedido em 18.03.2023]. Disponível em: Lei n.º 26/2016 | DR (diariodarepublica.pt);

Lei n.º 2/2004 da Assembleia da República, de 15 de janeiro, que aprova o Estatuto do Pessoal Dirigente dos Serviços e Organismos da Administração Pública [Em linha]. *Diário da República*, Série I-A, n.º 12, de 15 de janeiro de 2004 [Acedido em 12.09.2023]. Disponível em: Lei n.º 2/2004 | DR (diariodarepublica.pt);

Lei n.º 67/2007, da Assembleia da República, de 31 de dezembro, que estabelece o regime da Responsabilidade Civil Extracontratual do Estado e Pessoas Coletivas de

Direito Público (RRCEE) [Em linha]. *Diário da República*, Série I, n.º 251, de 31 de dezembro de 2007 [Acedido em 12.09.2023]. Disponível em: 0911709120.pdf (dre.pt);

Lei n.º 46/2018 da Assembleia da República, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União [Em linha]. *Diário da República,* Série I, n.º 155, de 13 de agosto de 2018 [Acedido em 25.09.2023]. Disponível em: Lei n.º 46/2018, de 13 de agosto | DR (diariodarepublica.pt);

Decreto-Lei n.º 65/2021, da Presidência do Conselho de Ministros, de 30 de julho, que Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019 [Em linha]. publicado em *Diário da República*, Série I, n.º 147, de 30 de julho de 2021 [Acedido em 25.09.2023]. Disponível em: Decreto-Lei n.º 65/2021 | DR (diariodarepublica.pt);

Lei 93/2021 da Assembleia da República, de 20 de dezembro, que estabelece o regime geral de proteção de denunciantes de infrações, transpondo a Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União [Em linha]. *Diário da República*, Série I, n.º 244, de 20 de dezembro de 2021 [Acedido em 26.09.2023]. Disponível em: 0000300015.pdf (dre.pt);

Resolução n.º 41/2018 do Conselho de Ministros, de 28 de março, que define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais [Em linha]. *Diário da República*, série I, n.º 62, de 28 de março de 2018, pp. 1424 – 1430 [Acedido pela última vez em 15.12.2023]. Disponível em: Resolução do Conselho de Ministros n.º 41/2018 | DR (diariodarepublica.pt);

Despacho n.º 7456/2017 da Presidência do Conselho de Ministros, de 24 de agosto, que determina a criação de um Grupo de Trabalho com o objetivo de preparar a legislação portuguesa para a aplicação do Regulamento Geral de Proteção de Dados em Portugal [Em linha]. *Diário da República*, Série II, n.º 163/2017, de 2017-08-24 [Acedido em 25.07.2023]. Disponível em: 1844018440.pdf (diariodarepublica.pt);

NP EN ISO/IEC 27000:2018 — Information technology: Security techniques: Information security management systems: Overview and Vocabulary. [Acedido em 05.10.2023]. Disponível em: Padrões disponíveis publicamente (iso.org).

RECOMENDAÇÕES, DIRETRIZES E PARECERES:

CdE Recommendation 509 Human rights and modern scientific and technological developments [Em linha]. 1968. [Acedido em 19.01.2023]. Disponível em https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en;

Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais ("Diretrizes sobre a Privacidade") [Em linha]. 1980. [Acedido em 21.06.2023]. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf;

Parecer n.º 4/2007, do Grupo Trabalho Artigo 29 (GT29), de 20 de junho de 2007, sobre o conceito de dados pessoais (WP 136) [Em linha]. [Acedido em 17.04.2023]. Disponível em: 12251/03/EN (europa.eu);

Parecer n.º 6/2013, do Grupo Trabalho Artigo 29 (GT29), de 5 de junho de 2013, sobre a dados abertos e reutilização de informações do setor público (ISP) (WP 207) [Em linha]. [Acedido em 02.10.2023]. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_pt.pdf;

Parecer n.º 5/2014, do Grupo Trabalho Artigo 29 (GT29), de 10 de abril de 2014, sobre técnicas de anonimização (WP 216) [Em linha]. [Acedido em 02.10.2023]. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf;

Guidelines Article 29 Data Protection Working Party, 26 november 2014, on the implementation of the CJEU judgment on «Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González» C-131/12, (WP 225) [Em linha]. [Acedido em 20.07.2023]. Disponível em: wp225_en.pdf (europa.eu);

Orientações do Grupo Trabalho Artigo 29 (GT29), de 29 de novembro de 2017, relativas à transparência na aceção do Regulamento 2016/679 (WP 260) [Em linha]. [Acedido em 20.04.2023]. Disponível em: ARTICLE29 - Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) (europa.eu);

Orientações do Grupo Trabalho Artigo 29 (GT29), de 6 de fevereiro de 2018, sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 (WP250 rev.1) [Acedido em 01.09.2023]. Disponível em: https://www.cnpd.pt/media/zgkec1q0/data-breach-_wp250rev01_pt.pdf;

Diretriz n.º 3/2018, do Comité Europeu para a Proteção de Dados (CEPD), de 12 de novembro de 2018, sobre o âmbito de aplicação territorial do RGPD. [Acedido em 25.08.2023]. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf;

Diretrizes n.º 1/2019, do Comité Europeu para a Proteção de Dados (CEPD), de 4 de junho de 2019, relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679. [Acedido em 24.09.2023]. Disponíveis em: edpb_guidelines_201901_v2.0_codesofconduct_pt.pdf (europa.eu);

Orientações n.º 4/2019, do Comité Europeu para a Proteção de Dados (CEPD), Versão 2.0, adotadas em 20 de outubro de 2020, relativas ao artigo 25.º Proteção de Dados desde a Conceção e por Defeito. [Acedido em 24.09.2023]. Disponível em: EDPB_Guidelines_20201020_Art25DataProtectionbyDesignbyDefault_V2.0_PT.docx (europa.eu);

Orientações n.º 07/2020, do Comité Europeu para a Proteção de Dados (CEPD), de 7 de julho de 2020, sobre os conceitos de «responsável pelo tratamento» e «subcontratante» no RGPD. [Acedido em 08.08.2023]. Disponíveis em: edpb_guidelines_202007_controllerprocessor_final_pt.pdf (europa.eu);

Orientações n.º 01/2021, do Comité Europeu para a Proteção de Dados (CEPD), de 14 de dezembro de 2021, sobre exemplos da notificação de uma violação de dados pessoais [Acedido em 02.09.2023]. Disponíveis em: edpb_guidelines_012021_pdbnotification_adopted_pt.pdf (europa.eu);

Parecer n.º 20/2018, da Comissão Nacional de Proteção de Dados (CNPD), de 2 de maio de 2018, sobre a proposta de Lei 120/XIII/3.ª (GOV). [Acedido em 25.08.2023]. Disponível em: https://www.uc.pt/site/assets/files/475840/20180502_parecer_20_cnpd.pdf;

Deliberação n.º 2019/494, da Comissão Nacional de Proteção de Dados (CNPD), de 3 de setembro de 2019. [Acedido em 16.03.2023]. Disponível em: https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2019&type=2&ent;

Diretriz n.º 1/2023, da Comissão Nacional de Proteção de Dados (CNPD), de 10 de janeiro de 2023, sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais. [Acedido em 08.10.2023]. Disponível em: https://www.cnpd.pt/decisoes/diretrizes/.

BIBLIOGRAFIA NÃO CITADA:

ATAÍDE, Rui P. Coutinho de Mascarenhas. Direito ao esquecimento. Cyberlaw by CIJIC, Lisboa, n. 6, 2019. Disponível em: https://www.cijic.org/wp-content/uploads/2019/05/Rui-Ata%C3%ADde_Direito-esquecimento.pdf;

CABRAL, Rita Amaral - O Direito à Intimidade da Vida Privada (Breve Reflexão acerca do artigo 8.º do Código Civil). In Estudos em Memória do Prof. Doutor Paulo Cunha, Lisboa, 1989;

CASTRO, Catarina Sarmento e. Direito da informática, privacidade e dados pessoais. Coimbra, Almedina, 2005;

CORDEIRO, António Menezes - O Respeito pela Esfera Privada do Trabalhador. In I Congresso Nacional de Direito do Trabalho. Memórias. Coordenação do Prof. Doutor António Moreira, Coimbra: Almedina, maio, 1998;

DRUMMOND, Victor - Internet, Privacidade e Dados Pessoais. Rio de Janeiro: Lúmen Juris, 2003;

FARINHO, Domingos Soares - Intimidade da Vida Privada e Media no Ciberespaço. Coimbra: Almedina, 2006.