A proteção de dados pessoais – o novo paradigma jurídico

Dissertação de Mestrado

Daniela Medeiros Teves

Mestrado em

Ciências Económicas e Empresariais

Ponta Delgada
2019

UNIVERSIDADE DOS AÇORES

Faculdade de Economia e Gestão

Rua da Mãe de Deus

9500-321 Ponta Delgada

Açores, Portugal

A proteção de dados pessoais – o novo paradigma jurídico

Dissertação de Mestrado

Daniela Medeiros Teves

Orientador

Prof. Doutor José Noronha Rodrigues

Dissertação submetida como requisito parcial para obtenção do grau de Mestre em Ciências Económicas e Empresariais, com especialização em Gestão de Recursos Humanos.

"Data is the new oil. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc to create a valuable entity that drives profitable activivity; so must data be broken down, analyzed for it to have value."

Clive Humby, Matemático, 2006[1]

[1] *In* Francisco, D., & Francisco, S., 2019, p.1.

RESUMO

O presente trabalho visa abordar a crescente importância dos dados pessoais, assim como o paradigma de proteção de dados foi-se modificando desde a Declaração Universal dos Direitos do Homem até aos dias de hoje, em que os dados pessoais nunca foram tão valiosos para as organizações e os seus modelos de negócio.

Visa também abordar a "arma" que a União Europeia concebeu para enfrentar a nova sociedade moderna em que os dados pessoais são cada vez mais valiosos, designadamente, o novo Regulamento Geral de Proteção de Dados, assim como as alterações que introduz e implicações para os atuais modelos de negócio.

Por outro lado, o presente trabalho aborda como o novo paradigma de proteção de dados se coaduna com a Administração Pública e, em especial, como se devem relacionar o direito de acesso à informação administrativa, corolário do princípio da administração aberta e o direito à reserva da intimidade da vida privada, corolário do princípio da proteção de dados, tratando-se ambos de princípios fundamentais com previsão constitucional.

O princípio da administração aberta constitui um dos fundamentais princípios que pauta a atividade administrativa, que deverá ser aberta e transparente para os cidadãos. Por sua vez, o princípio da proteção de dados determina que todos os indivíduos têm direito à proteção dos seus dados. O modo como estes princípios têm sido aplicados pelos organismos públicos têm potenciado conflitos de competências e entendimento díspares sobre a temática.

Assim, a presente dissertação pretende abordar a mudança de paradigma jurídico introduzida pelo RGPD. A escolha do tema justifica-se pela sua atualidade, uma vez que cada mais vivemos numa sociedade moderna em que os dados pessoais são considerados o novo petróleo.

Palavras-chave: Dados pessoais, Regulamento Geral de Proteção de dados, tratamento de dados pessoais, documentos nominativos.

ABSTRACT

This paper aims to address the growing importance of personal data, as the way data protection paradigm has changed from the Universal Declaration of Human Rights to the present day, where personal data has never been so valuable to organization and their business models.

It also aims to address the "weapon" that the European Union has designed to address the new modern society where personal data is increasingly valuable, the new General Data Protection Regulation, as well the changes it introduces and implication for current business models.

On the other hand, this paper discusses how the new data protection paradigm fits in with the Public Administration and, in particular, how the right of access to administrative information, corollary of the principle of open administration and the right to privacy, corollary of data protection principle, should be related, both of which are fundamental principles with constitutional provision.

The principle of open administration is one of the fundamental principles that guide administrative activity, which should be open and transparent to citizens. On the other hand, the data protection principle dictates that all individuals have the right to the protection of their data. The way which these principles have been applied by public entities has fostered conflicts of competences and different understanding of the subject.

Thus, this dissertation intends to address the change of legal paradigm introduced by the GDPR. The choice of theme is justified by its relevance, since we live in a modern society in which personal data is considered the new oil.

Keywords: Personal data, General Data Protection Regulation, processing, access to nominative documents.

AGRADECIMENTOS

O caminho até à presente dissertação constituiu uma autêntica montanha-russa de emoções. Ser uma licenciada em Direito num mestrado em Ciências Económicas e Empresarias representou um verdadeiro desafio.

À formação em Direito e à novidade dos conteúdos, alia-se o estatuto de trabalhador estudante. A conciliação de uma carreira profissional e os estudos universitários não constitui tarefa fácil, embora exequível, implica muita dedicação, esforço, sacrifício e descomunal gestão de tempo.

Todavia, ao chegar ao término deste percurso cumpre-me afirmar que a elaboração da presente dissertação de mestrado contou com fundamentais apoios, assim, em primeiro lugar gostaria de endereçar um agradecimento especial ao meu orientador, Professor Dr. José Noronha Rodrigues, por toda a disponibilidade demonstrada, pelos comentários e contributos na realização da dissertação, assim como pelo saber transmitido e por todas as palavras de incentivo, e, em geral, a todos os professores do Mestrado em Ciências Económicas e Empresariais na Universidade dos Açores por toda a ajuda e conhecimentos transmitidos.

Não posso deixar de agradecer aos meus pais, Válter e Lúcia, pela oportunidade que me proporcionaram, pelo apoio incondicional e constante ânimo, à Leila, pelo apoio, palavras sábias e preciosas ajudas nas revisões de cada capítulo e ao André pelo apoio e companheirismo nos momentos de desalento e cansaço.

ÍNDICE

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

AIPD - Avaliação de Impacto sobre a Proteção de Dados
CADA – Comissão Nacional de Acesso a Documentos Administrativos
CNPD – Comissão Nacional de Proteção de Dados
DPO - Data Processor Officer
EPD – Encarregado de Proteção de Dados
GT29 – Grupo de Trabalho do artigo 29.º para a Proteção de Dados
LADA – Lei de Acesso aos Documentos Administrativos
LPDP – Lei de Proteção de Dados Pessoais
PbD – Privacy by design
RAA – Região Autónoma dos Açores
RGPD – Regulamento Geral de Proteção de dados
UE – União Europeia

CAPÍTULO I - INTRODUÇÃO

Com a entrada em vigor com carácter obrigatório a 25 de maio de 2018 do 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, tornou-se necessário que as organizações se adaptem ao novo paradigma de proteção de dados.

O Regulamento Geral de Proteção de dados compõe um marco na evolução do quadro da privacidade no contexto europeu, orientado por uma abordagem filosófica de proteção de dados, baseada no conceito de privacidade enquanto direito fundamental consagrado na Carta dos Direitos Fundamentais da União Europeia, pondo o indivíduo no centro da questão como o efetivo proprietário dos dados. Nesta medida, o Regulamento Geral de Proteção de Dados terá um vasto impacto global no modo comos os dados pessoais são tratados, devolvendo o poder ao titular dos dados, garantindo-lhe uma maior segurança dos seus dados pessoais.

O Regulamento fortalece e expande o regime de proteção de dados europeus, na medida que protege os dados pessoais de todos os residentes da União Europeia, independentemente da localização do tratamento, aumentando amplamente o alcance do novo quadro legal europeu, abrangendo toda a informação que, diretamente ou indiretamente, possam identificar um indivíduo, incluindo identificadores *online* como endereços de *IP, cookies*, dados de localização, estatuindo um conceito de dados muito mais amplo do que a anterior Diretiva.

O amplo âmbito de aplicação territorial e ampla definição de dados pessoais garantem que o Regulamento Geral de Proteção de dados tenha um impacto significativo, constituindo uma oportunidade para muitas organizações melhorarem os seus modelos de

negócios, acarretando inúmeras alterações para o modo de tratamento de dados, assim como um aumento do nível de responsabilidade dos responsáveis pelo tratamento e subcontratantes.

Diferentemente da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, que o RGPD revogou, o regulamento é um ato legislativo da União Europeia que não carece de transposição, tendo aplicabilidade direita e efeito direto no ordenamento jurídico de cada Estado-Membro da União Europeia.

A metodologia adotada na presente dissertação passou pelo estudo comparativo entre o regime de proteção de dados no âmbito da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 e o atual 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, comparação das disposições nacionais, europeias e internacionais na matéria de proteção de dados, assim como análise da Administração Pública e a implementação do referido Regulamento no seu seio.

Na presente dissertação no primeiro capítulo se abordará a evolução legislativa da proteção de dados a nível internacional, europeu e nacional, na medida que o RGPD é o resultado de um acervo legislativo adotado de modo a acautelar na União Europeia a evolução da era digital, tratando-se de uma medida crucial ao reforço dos direitos fundamentais dos cidadãos e à simplificação do comércio no âmbito do mercado único digital, seguindo-se uma análise detalhada dos alterações introduzidas pelo RGPD.

Por fim, no segundo capítulo, abordaremos o modo como o novo regime de proteção de dados se coadunará com o regime da administração pública, na medida em que a Administração pública encontra-se sujeita às regras do RGPD uma vez que no âmbito das competências e atribuições conferidas por lei aos serviços públicos, tem legitimidade para

tratar dados pessoais dos administrandos, devendo esse tratamento ser pautado pelos princípios fundamentais de tratamento de dados pessoais consagrados no RGPD. Abordando-se ainda o modo como o princípio da administração aberta, que prevê o regime de acesso a documentos administrativos, que em muitas situações integram dados pessoais dos administrandos, se conjugará com o regime de proteção de dados introduzido pelo RGPD.

CAPÍTULO II - A PROTEÇÃO DE DADOS: O NOVO REGULAMENTO GERAL DE DADOS PESSOAIS

2.1 Sumário

2.2. Resumo **- 2.3** Introdução; **2.4.** Reforma e evolução legislativa: no contexto internacional, europeu e nacional; **2.4.1.** No contexto Internacional; **2.4.2**. No contexto europeu; **2.4.3.** No contexto nacional; **2.5.** O RGPD: Fundamentais progressos; **2.5.1.** Dados Pessoais; **2.5.2.** Tratamento de dados pessoais; **2.5.3.** Príncpios relativos ao tratamento de dados pessoais; **2.5.4**. Consentimento; **2.5.5.** Novos direitos do titular dos dados; **2.5.6.** Direitos tradicionais; **2.5.7.** Âmbito de aplicação territorial; **2.5.8.** Transferência de dados pessoais para países terceiros; **2.5.9.** Encarregado de protecção de dados; **2.5.10.** *Accountability* - Responsabilidade proativa e autoregulação; **2.5.11.** Avaliação de impacto sobre a proteção de dados e consulta prévia; **2.5.12.** Segurança dos dados pessoais; **2.5.13.** Vias de recurso, responsabilidade e sanções; 2.6**.** Considerações finais.

2.2 Resumo

Neste primeiro capítulo propomo-nos a fazer uma breve viagem pela história da proteção de dados tanto a nível internacional, como a nível europeu e nacional. Finalmente, incindiremos o nosso estudo sobre as principais alterações e evoluções introduzidas pelo RGPD no paradigma da proteção de dados, nomeadamente, no que concerne à definição de dados pessoais, tratamento de dados pessoais, princípios relativos ao tratamento de dados pessoais, consentimento, direitos do titular dos dados, âmbito de aplicação territorial, transferência de dados pessoais para países terceiros, a figura do encarregado de proteção de dados, regime de autorregulação em oposição ao regime heteroregulatório, avaliação de impacto sobre a proteção de dados, consulta prévia, segurança dos dados, assim como o novo quadro sancionatório.

2.3 Introdução

O 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[2], revogou a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995[3], traduzindo-se no resultado do acervo legislativo adotado de modo a acautelar na União Europeia a evolução da era digital, tratando-se de uma medida crucial ao reforço dos direitos fundamentais dos cidadãos e à simplificação do comércio no âmbito do mercado único digital.

2.4 Reforma e evolução legislativa: O contexto internacional, europeu e nacional

As últimas décadas sinalizam uma enorme evolução tecnológica transformadora do modo como os dados pessoais são processados[4]. A par desta evolução tecnológica verifica-se um acréscimo da digitalização da economia acompanhada de um aumento tendencial da importância dos dados pessoais, verificando-se um crescente fluxo de dados pessoais a circular *online,* que alteraram os modelos de negócio utilizados pelas empresas, sendo que o *e-commerce*[5] tem se demostrado extremamente importante no contexto empresarial e na economia digital, na medida em que permite às empresas divulgar e comercializar, a uma escala global, o seu objeto comercial, simplificando a realização de transações de compra e venda de bens e serviços e contribuindo para uma mudança de comportamento do comprador que passa a realizar cada vez mais compras *online*.

---

[2] Jornal Oficial n.º L 119, 4.5.2016, p. 1–88.

[3] Jornal Oficial nº L 281 de 23/11/1995 p. 0031 – 0050.

[4] "Data protection came onto the agenda because of the growing significance of information and communications technologies in both the public and private sectors" (Raab, & Bennett, 1994)

[5] Sobre esta temática refere Bravo (2017, p. 16) que "o mercado proporcionado pelo e-commerce é definido como mercado eletrónico ou e-marketplace e constitui-se como um local online vendedores e compradores, conectados através da Internet, realizam transações comerciais como a venda de bens, serviços ou informações, sendo que o seu desenvolvimento proporciona às empresas um maior número de oportunidades do que aquelas que encontram em mercados tradicionais, (…) este mercado não se restringe a um território, sendo capaz de gerar oportunidades não só para as empresas mas também para os indivíduos, que passaram a ter a possibilidade de comercializar os seus produtos ou serviços online".

A evolução da tecnológica da informação e do panorama social e comercial gerou novos desafios em matéria de proteção dos dados pessoais, sendo que os titulares dos dados disponibilizam cada vez mais os seus dados pessoais, verificando-se um aumento da utilização desses dados pessoais por parte das organizações com o objetivo de desenvolver a sua escala de negócio[6], dado que existe um aumento do valor económico dos dados pessoais, existindo mesmo um mercado para os dados[7].

A par dessa transformação tecnológica verificou-se uma crescente preocupação com os dados pessoais, o que, consequentemente, desencadeou uma evolução legislativa neste ramo, conforme mais à frente se abordará.

Os dados pessoais passaram a ser vistos na economia digital do mesmo modo que o petróleo é visto pela economia industrial, sendo que muitos defendem que os dados pessoais são o novo petróleo[8], conforme Hirsch (2014) explica "a maior parte das pessoas que usa a analogia, fá-lo para transmitir o enorme valor do *Big Data*[9]. Os dados são um recurso essencial que capacita a economia da informação, como o petróleo alimentou a economia industrial. *Big data* promete uma infinidade de novos usos – a identificação e prevenção de pandemias, novos negócios e sectores de negócio, a melhoria da saúde, qualidade e eficiência do atendimento e proteção do meio ambiente" (p.1).

Na linha de Oliveira (2015) "o processo de armazenamento, documentação e uso de informações pessoais transformou-se numa condição *sine qua non* para a formação da nossa sociedade moderna" (p.15).

---

[6] *Cfr.* Considerando 6 do RGPD.

[7] A este propósito referem Silveira, Avelino & Souza (2016, p.219) que "o mercado de dados pessoais é cada vez mais relevante na sociedade informacional e pode ser entendido como as interações económicas voltadas à compra e venda das informações relativas a uma pessoa identificada ou identificável, direta ou indiretamente. O mercado de dados pessoais se baseia nas necessidades de informação das empresas, instituições públicas e usuários finais".

[8] Por exemplo, Clive Humby, em 2006 no seu discurso na Cúpula do ANA Senior Marketer na Kellogg School.

9 *Big data* é definida pelo Lexico Oxford Dictionary como um conjunto de dados extremamente grandes que podem ser analisados computacionalmente de modo a revelar padrões, tendências e associações, especialmente relacionadas com o comportamento e interações humanas. Definição disponível em: https://www.lexico.com/en/definition/big_data

O direito à proteção de dados é um direito que deriva do direito à proteção da vida privada, na medida em que, por maioria de razão, os dados pessoais constituem informações do foro da vida privada de cada um, neste sentido disponha o artigo 1.º da Diretiva 95/47/CE, do Parlamento Europeu e do Conselho de 24 de outubro de 1995. [10/11]

Todavia, e como sublinha o considerando 4[12] do RGPD o direito à proteção de dados não deverá ser concebido como um direito absoluto, devendo ser compensado com outros direitos fundamentais e executado em conformidade com o princípio da proporcionalidade[13].

2.4.1 No contexto internacional

A Declaração Universal dos Direitos do Homem, adotada e proclamada pela Assembleia Geral das Nações Unidas na sua resolução 217A (III) de 10 de dezembro de 1948[14]surgiu depois da 2ª Guerra Mundial, numa altura que "se procurava criar instrumentos concretos que promovessem a paz e o respeito pela dignidade humana"[15], tendo sido pioneira na consagração do direito à privacidade de cada individuo, estabelecendo no seu artigo 12.º que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à proteção da lei".

---

[10] Jornal Oficial nº L 281 de 23/11/1995 p. 0031 – 0050.

[11] Artigo 1 da Diretiva 95/46/CE do Parlamento Europeu e do Conselho: "1 – Os Estados-Membros assegurarão, em conformidade com a presente diretiva, 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."

[12] "O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística."

[13] Na aceção de Vicente (2014, p.15) "o princípio da proporcionalidade, na sua configuração moderna, tem a sua origem na ideia de necessidade, isto é, na exigência de limitação das medidas lesivas ao estritamente necessário para se atingir um determinado fum, fundada no direito do cidadão à menor desvantagem possível".

[14] Publicada no Diário da República, I Série A n.º 57/78, de 9 de março de 1978, mediante aviso do Ministério dos Negócios Estrangeiros.

[15] *Cfr.* "*70 ANOS DA DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS E OS OBJETIVOS DE DESENVOLVIMENTO SUSTENTÁVEL",* Plataforma ONGD, 7 de dezembro de 2018, disponível em: http://www.plataformaongd.pt/noticias/noticia.aspx?id=1347

Por sua vez, a Convenção Europeia dos Direitos do Homem, também conhecida como a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, adotada a 4 de novembro de 1950 pelo Conselho da Europa, e entrado em vigor em 1953, tendo Portugal ratificado esta Convenção a 9 de novembro de 1978, constitui "o primeiro instrumento jurídico vinculativo de direito internacional em matéria de direitos humanos, constituindo o mais perfeito modelo internacional de direitos fundamentais, criado após a Segunda Guerra Mundial perante a falência dos modelos puramente nacionais de defesa de direitos fundamentais" (Alves & Castilho, 2016, p.16) constituindo, assim, o primeiro instrumento juridicamente vinculativo a consagrar o direito à privacidade no seu artigo 8.º[16].

Por sua vez, o Conselho de Europa, enquanto organismo internacional que promove os direitos humanos, onde se incluí a proteção de dados, considerou "desejável alargar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente, o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal suscetíveis de tratamento automatizado"[17], surgindo a Convenção n.º 108, relativamente à proteção das pessoas no que concerne ao tratamento automatizado de dados de carácter pessoal, compondo o primeiro instrumento internacional juridicamente vinculativo adotado em matéria da proteção de dados que protege os indivíduos contra abusos que possam ocorrer aquando da recolha e processamento de dados pessoais, regulando a transferência transfronteiriça de dados pessoais, tendo sido aberta à assinatura em 28 de janeiro de 1981 em Estrasburgo e ratificada por 51 Estados, entrando em vigor na ordem internacional a 1 de outubro de

[16] Artigo 8.º - Direito ao respeito pela vida privada e familiar: "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 infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros".
[17] *Cfr*. Preâmbulo da Convenção n.º 108.

1985, tendo sido alterada a 15 de junho de 1999, de modo a consentir que as Comunidades Europeias acedessem à Convenção, e pelo Protocolo Adicional à Convenção, respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados pessoais, aberto à assinatura a 8 de novembro de 2001 em Estrasburgo.

Considerando o aumento do fluxo transfronteiriço de dados pessoais suscetíveis de tratamento automatizado[18] e a necessidade de conciliar a proteção e respeito pela vida privada, a Convenção n.º 108 do Conselho da Europa visou garantir a proteção do direito à vida privada das pessoas singulares e aos seus dados pessoais "face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito", aberta para assinatura em 1981, anterior à digitalização da informação e do crescimento da importância da internet na sociedade moderna.

A sociedade da informação encontra-se cada vez mais globalizada, sendo que cedo se percebeu que a proteção de dados tem uma importância global[19], tendo impacto nos quatro pontos do globo[20].

---

[18] Nos termos da alínea c) do artigo 2.º da Convenção n.º 180 o tratamento automatizado compreende as operações levadas a cabo com a ajuda de processos automatizados, nomeadamente, registo de dados, aplicação a esses dados de operações lógicas e ou aritméticas, bem como a sua modificação, supressão, extração ou difusão.

[19] Foi da necessidade de conciliar o regime de proteção de dados em países com costumes diferentes que surgiu a decisão da Comissão 2000/520/CE, de 26 de julho de 2000, conhecida por Acordo *Safe Harbor* (disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32000D0520, consultado a 29/09/2019), respeitando "a um processo de autocertificação e cooperação entre o Departamento de Comércio dos EUA e a Comissão Europeia, reconhecido através de uma Decisão da Comissão Europeia. Assim, as entidades com sede nos EUA declaram cumprir com as regras relativa à proteção dos dados pessoais, estabelecidas através da legislação comunitária, fundamentando as operações de entidades que operam nas duas jurisdições e que tratam dados pessoais dos seus clientes e/ou utilizadores" (Raposo, Sá Miranda & Associados, Sociedade de Advogados, R.L, 2015). Todavia, o Tribunal de Justiça da União Europeia no seu acórdão de 6 de outubro de 2015, no processo n.º C-362/04 (disponível em: http://curia.europa.eu/juris/celex.jsf?celex=62004CO0362&lang1=pt&type=TXT&ancre=, consultado a 29/09/2019) declarou a invalidade do acordo *Safe Harbor* nas operações de transferências de dados entre a União Europeia e os EUA.

[20] Neste sentido, o Brasil, inspirado na globalização da económica e nos avanços tecnológicos, promulgou a lei federal n.º 13.709 de 2018 que dispõe sobre a proteção de dados e o tratamento de dados pessoais pelas empresas públicas e privadas, consagrando um marco normativo para a sociedade brasileira: "*é a legislação que mais efetivamente busca solucionar o diálogo necessário entre a preservação e o respeito aos direitos fundamentais da liberdade e da privacidade em uma sociedade informacional com o desenvolvimento econômico e tecnológico e com a inovação*" (disponível em: https://www.ab2l.org.br/lgpd-ou-lpdp-como-denominiar-a-lei-de-protecao-de-dados-brasileira/, consultado a 29/09/2019). Por sua vez, na Ásia o Japão em 2017 alterou significativamente a *Act on the Protection of Personal Information* (APPI), refletindo a tendência global de aumentar a privacidade de dados, enquanto Singapura assinou em fevereiro de 2018 a *Cybersecurity Bill into law* (cfr. https://blogs.arubanetworks.com/solutions/data-privacy-laws-in-apac-what-you-need-to-know/, consultado a 29/09/2019). No que concerne à África, os membros da União Africana (UA) em 2014 aprovaram a Convenção da União Africana sobre Cibersegurança e Proteção de Dados (disponível em: https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_201809June_Final_Portuguese.pdf, consultado a 20/09/2019). Apesar da multiplicidade de diplomas internacionais no que concerne à proteção de dados pessoais para uma melhor sistematização decidimos abordar neste trabalho apenas o Regulamento Geral de Proteção de Dados.

2.4.2 No contexto europeu

A Carta dos Direitos Fundamentais da União Europeia[21], que institui os princípios, direitos e liberdades da União Europeia, consagrou a proteção das pessoas singulares relativamente ao tratamento dos dados pessoais como um direito fundamental. A Carta foi formalmente adotada em Nice[22] em dezembro de 2000, pelo Parlamento Europeu, pelo Conselho e pela Comissão, tendo-se tornado juridicamente vinculativa para a União Europeia e para os Estados-Membros aquando da aplicação da legislação da União Europeia, com a entrada em vigor do Tratado de Lisboa, em dezembro de 2009, tendo o mesmo valor jurídico do que um tratado da União Europeia.

Por sua vez, o Tratado Sobre o Funcionamento da União Europeia no seu artigo 7.º[23] e no número 1 do artigo 16.º[24], em conjugação com o artigo 8.º[25] da Carta dos Direitos Fundamentais da União Europeia estabelecem que todos as pessoas singulares têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.

Em 1990, inspirando-se na Convenção n.º 108 e na progressiva relevância do tratamento dos dados pessoais, bem como a necessidade de harmonizar o mercado único e as legislações dos Estados-Membros - dado que se confirmava uma acentuada divergência a nível da legislação nacional aplicável na matéria nos diversos Estados-

---

[21] Jornal Oficial n.º C 364 de 18/12/2000 p. 0001 – 0022. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000X1218(01):PT:HTML

[22] Tratado de Nice, Jornal Oficial nº C 080 de 10/03/2001 p. 0001 – 0087. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12001C/TXT

[23] Artigo 7.º do Tratado sobre o Funcionamento da União Europeia: *"Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações."*

[24] Artigo 16.º do Tratado sobre o Funcionamento da União Europeia: "*1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.º do Tratado da União Europeia.*"

[25] Artigo 8.º da Carta dos Direitos Fundamentais da União Europeia: *"1. Todas as pessoas têm direito proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."*

Membros - é proposta a Directiva 95/46/CE[26], relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, tendo a mesma sido adotada em 1995 pelo Parlamento Europeu e o Conselho da União Europeia, sido complementada pela Decisão-Quadro 2008/977/JAI[27], enquanto instrumento geral na União Europeia para a proteção de dados pessoais no âmbito da cooperação policial e judiciária em matéria penal.

A Diretiva 95/46/CE foi adotada como precavo do direito fundamental à proteção de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros, sendo que nos termos do considerando n.º 11 da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, as suas primordiais finalidades consistiam em clarificar e ampliar os princípios da Convenção n.º 108, salientando a necessidade de assegurar que a circulação transfronteiras de dados pessoais no âmbito da integração económica e social do funcionamento do mercado interno seja, realizada de forma regulada de modo a não impedir a livre circulação de dados pessoais entre Estados-Membros.

Deste modo, a Diretiva 95/46/CE do Parlamento Europeu e do Conselho constituiu a base do desenvolvimento das legislações nacionais de cada Estado-Membro no que respeita à proteção de dados em 1995.

Conquanto que as diretivas vinculam os "Estado(s)-Membro(s) destinatário(s) quando ao resultado a alcançar, deixando no entanto, às instâncias nacionais a competência quanto à forma e aos meios"[28], a Diretiva *in casu* atribuiu aos Estados-Membros a faculdade de precisar nas suas legislações ou normas de execução as condições gerais em que o tratamento de dados pessoais é lícito, o que consequentemente

[26] Jornal Oficial nº L 281 de 23/11/1995 p. 0031 – 0050.
[27] Jornal Oficial n.º L 350 de 30/12/2008 p. 60-71
[28] Artigo 288.º do Tratado Sobre o Funcionamento da União Europeia.

originou a carência de uniformização[29] dos direitos dos sujeitos nos diversos Estados-Membros e desiguais níveis de proteção dos indíviduos na proteção dos seus dados, analogamente verificou-se que a Diretiva não proporcionava proteção jurídica contra violações de dados pessoais sobrevindas de países terceiros.

Já o considerando n.º 9 da Diretiva determinava que " é deixada aos Estados-Membros uma margem de manobra que, no contexto de aplicação da diretiva, poderá ser utilizada pelos parceiros económicos e sociais; que os Estados-Membros poderão, pois, especificar na sua legislação nacional as condições gerais de licitude do tratamento de dados; (…) que, nos limites dessa margem de manobra e em conformidade com o direito comunitário, poderão verificar-se disparidades na aplicação da diretiva".

A par da fragmentação supramencionada, a Diretiva encontrava-se desatualizada do contexto tecnológico e digital, uma vez que aquando da sua redação a internet não detinha o avanço e importância na economia que se verifica no contexto atual.

Neste sentido, o Regulamento (UE) 2016/679 surge da necessidade de uniformizar a legislação em matéria de proteção de dados em todos os Estados-Membros, apesar de os objetivos e princípios contidos na Diretiva 95/46/CE permanecessem válidos, verificou-se que as diferenças no nível de proteção dos dados pessoais nos Estados-Membros, resultantes das disparidades na execução e aplicação da Diretiva, poderiam originar entraves à livre circulação de dados pessoais na União Europeia, bem como "insegurança jurídica ou o sentimento generalizado da opinião pública de que susbistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito

[29] Adiante se abordará a temática da uniformização resultante de um Regulamento e a harmonização decorrente de uma Diretiva.

às atividades por via eletrónica"[30], dado que se verificava uma fragmentação da aplicação da proteção de dados nos vários Estados-Membros da União Europeia.

Nos termos do artigo 288.º do Tratado Sobre o Funcionamento da União Europeia, um regulamento "tem carácter geral, é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros". Assim, o regulamento, enquanto ato legislativo vinculativo é aplicável a todos os Estados-Membros da União Europeia em todos os seus elementos, não dependendo de um diploma nacional de adaptação, ainda que o legislador comunitário tenha optado por remeter para o legislador nacional a densificação de diversas matérias[31], verificando-se uma maior harmonização da legislação aplicável na matéria, na medida em que pretende garantir uma aplicação homogénea e coerente dos direitos e liberdades fundamentais das pessoas singulares no que toca ao tratamento dos dados pessoais.

Deste modo, em abril de 2016 a União Europeia procedeu à reforma do seu quadro legislativo relativo a proteção de dados pessoais, adotando uma das mais importantes mudanças na legislação sobre proteção de dados, com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016[32], que consagra novos normativos relativos à proteção das pessoas singulares, vivas, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, tendo como principais objetivos proceder à harmonização

[30] Considerando 9 do RGPD.
[31] O RGPD atribui aos Estados-Membros margem de manobra para estipular as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais (neste sentido considerando 10 do RGPD).
[32] Alterado pela Retificação do 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), *Jornal Oficial da União Europeia N.º L 127/2, 23/5/2018.*

da legislação em todos os Estados-Membros, bem como permitir que os cidadãos e estruturas empresarias beneficiem da economia digital e do comércio eletrónico, alterando o modo como as organizações tratam os dados pessoais, e principalmente, proteger os dados pessoais dos cidadãos europeus, em contrapartida o Regulamento Geral de Proteção de Dados, doravante designado por RGPD, gera novas incumbências para o sector empresarial.

Na realidade, a reforma legislativa em matéria de proteção de dados pessoais sobrevém das comunicações da Comissão Europeia intituladas "Uma abordagem global da proteção de dados pessoais na União Europeia", "Proteção da privacidade num mundo interligado – Um quadro europeu de proteção de dados para o século XXI" e "Proposta de regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados".

A) Uma abordagem global da proteção de dados pessoais na União Europeia;

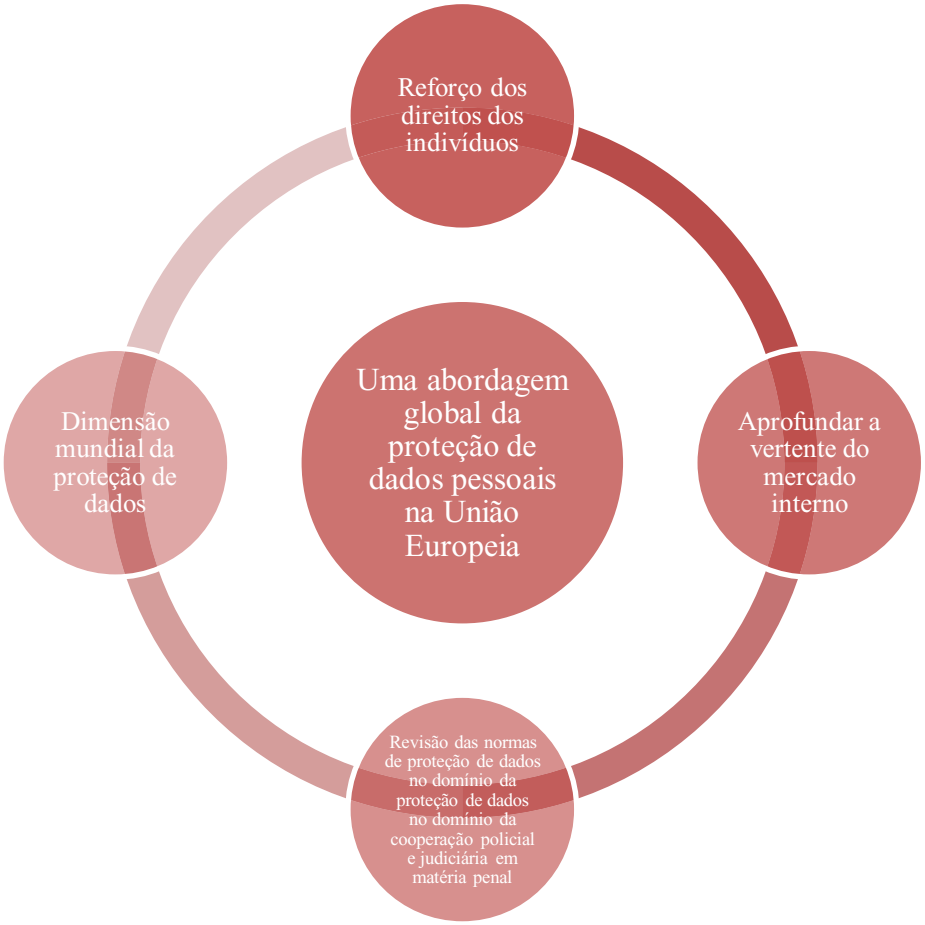
A COM(2010) 609 final aborda a necessidade de se proceder à revisão do quadro legislativo vigente à data, no caso a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, na medida em que "a rapidez dos avanços tecnológicos e da globalização vieram alterar profundamente o mundo que nos rodeia e trazer novos desafios para a proteção dos dados pessoais" (Comissão Europeia, 2010).

A Comissão Europeia promoveu uma conferência de alto nível em maio de 2009, a que se seguiu uma consulta pública até ao final de 2009, que concluiu que os princípios nucleares da diretiva mantinham-se válidos e que deveria ser preservado o seu carácter tecnologicamente neutro, no entanto foram assinaladas questões problemáticas, nomeadamente, a necessidade de se equacionar o impacto das novas tecnologias, de se reforçar a vertente da proteção de dados do mercado interno,

equacionar a globalização e melhorar as transferências de dados internacionais, conseguir um quadro institucional mais firme para a aplicação efetiva das normas da proteção de dados, assim como a necessidade de aumentar a coerência do quadro normativo que rege a proteção de dados. Tais questões "exigem que a UE desenvolva uma abordagem global e coerente qua garanta que o direito fundamental das pessoas singulares à proteção dos dados é plenamente respeitado na UE e fora dela", sendo que os principais objetivos dessa abordagem passavam por reforçar os direitos dos indivíduos, designadamente através do garante da proteção adequada das pessoas em todas as circunstâncias, aumento da transparência, aumento do controlo sobre os próprios dados, aumento da sensibilização do público, garante do consentimento livre e informado, proteção dos dados sensíveis, tornar as soluções e as sanções mais eficazes; aprofundar a vertente do mercado interno, mediante o aumento da segurança jurídica e assegurar a igualdade de condições para os responsáveis pelo tratamento de dados, reduzir a carga administrativa, clarificar as normas sobre a lei aplicável e a responsabilidade dos Estados-Membros, aumentar as responsabilidades dos responsáveis pelo tratamento de dados, incentivar as iniciativas autorreguladoras e explorar os regimes de certificação da UE; rever as normas de proteção de dados no domínio da proteção de dados no domínio da cooperação policial e judiciária em matéria penal; a dimensão mundial da proteção de dados, mediante a clarificação e simplificação das normas aplicáveis às transferências internacionais de dados, promoção de princípios universais; quadro institucional mais forte para uma melhor aplicação das normas de proteção de dados.

Concluindo ainda que a Comissão que a União Europeia carecia de uma política relativa ao direito fundamental à proteção de dados pessoais mais ampla e coerente.

Figura 1 - Principais objetivos da abordagem global e coerente qua garanta que o direito fundamental das pessoas singulares à proteção dos dados[33]



B) Proteção da privacidade num mundo interligado – Um quadro europeu de proteção de dados para o século XXI;

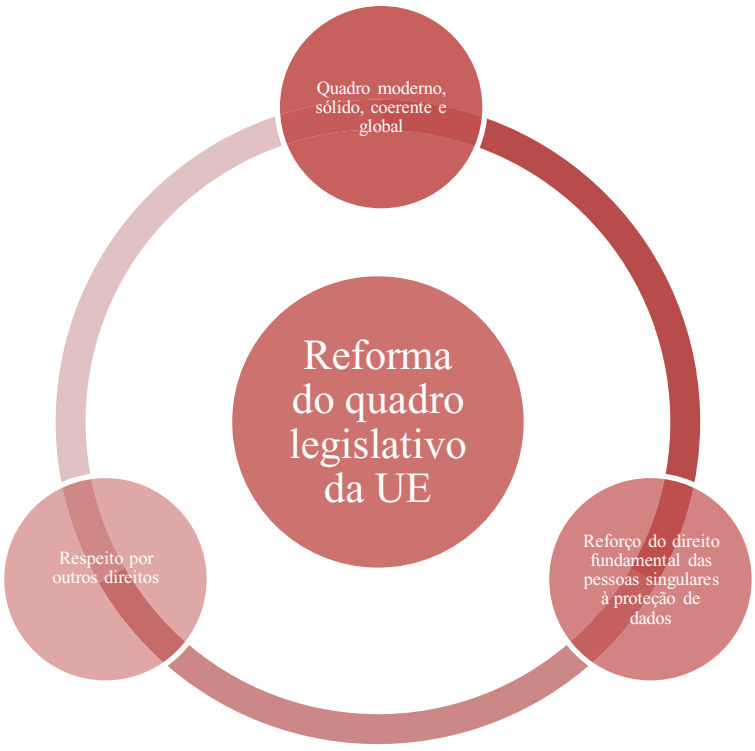
À semelhança da COM (2010) 609 final, a COM (2012) 9 final aborda o modo como a evolução tecnológica e da globalização transformou o modo como os dados

[33] Todas as figuras apresentadas na tese foram elaboradas pela mestranda, com exceção do *template* disponibilizado pela CNPD na figura 17.

pessoais são recolhidos, acedidos, utilizados e transferidos, apresentando os "elementos principais da reforma do quadro legislativo da UE relativo à proteção de dados" (Comissão Europeia, 2010).

Estabelece ainda que a reforma do quadro legislativo da UE deverá ter por objetivo instituir "um quadro moderno, sólido, coerente e global em matéria de proteção de dados para a União Europeia", reforçando o direito fundamental das pessoas singulares à proteção de dados, respeitando-se outros direitos, como "a liberdade de expressão e de informação, o direito das crianças, o direito de liberdade de empresa, o direito a um processo equitativo e ao sigilo profissional, bem como o estatuto das igrejas tal como definido nas legislações dos Estados-Membros".

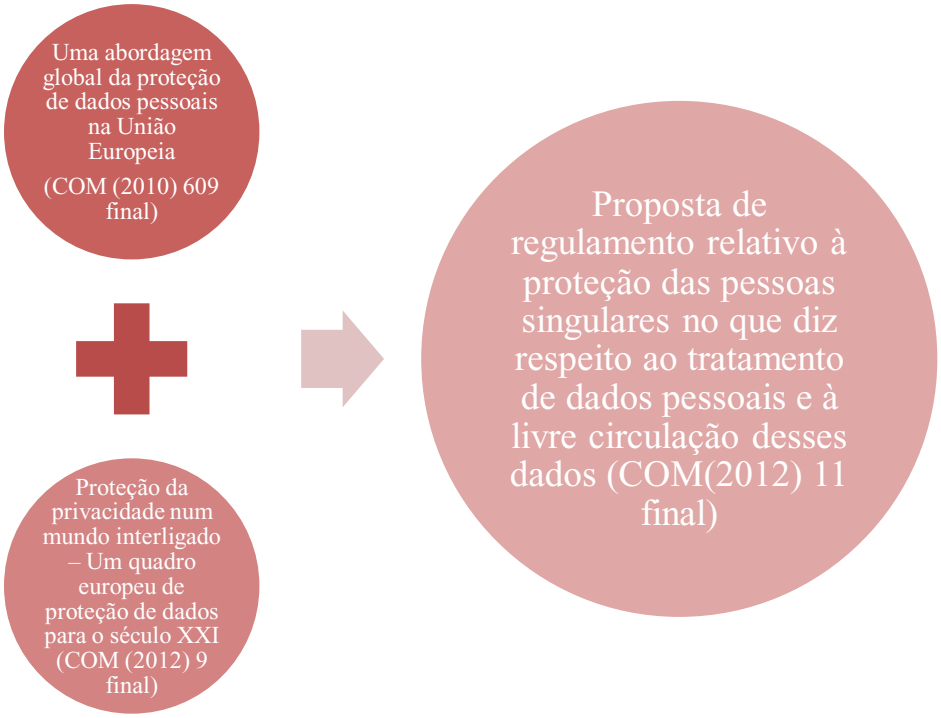
Figura 2 - Principais objetivos da reforma do quadro legislativo da UE em matéria de proteção de dados



C) Proposta de regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;

Baseando-se nos fundamentos da COM (2010) 609 e COM (2012) 9 final, como o próprio título refere, a COM(2012) 11 final constitui uma primeira proposta de regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Figura 3 - COM(2012) 11 final



Nas comunicações supramencionadas são levantadas questões pertinentes e de extrema importância no que concerne ao impacto da evolução tecnológica nos dados pessoais e sobre a necessidade de um novo quadro legislativo que acautele as evoluções e a necessidade de adequar os processos de transferências de dados pessoais.

A reforma do quadro legislativo da proteção de dados constitui um instrumento essencial à implementação e desenvolvimento do Mercado Único Digital no território europeu, dado que reforça a confiança dos titulares de dados nas novas tecnologias de informação, certificando que o tratamento de dados pessoais se encontra sujeito a regras uniformes e atualizadas ao novo paradigma tecnológico e digital em todos os Estados-Membros (Comissão Europeia, 2018).

Nesta medida, a Estratégia para o Mercado Único Digital foi adotada pela Comissão Europeia, em Bruxelas, a 6 de maio de 2015, visando criar o Mercado Único Digital, tratando-se de "um mercado em que é assegurada a livre circulação de mercadorias, pessoas, serviços e capitais e em que os cidadãos e as empresas podem beneficiar de um acesso sem descontinuidades a atividades em linha e desenvolver essas atividades em condições de concorrência leal e com um elevado nível de proteção dos consumidores e dos seus dados pessoais, independentemente da sua nacionalidade ou local de residência. A realização de um Mercado Único Digital permitirá à Europa manter a sua posição como líder mundial na economia digital, ajudando as empresas europeias a crescer a nível global" (Comissão Europeia, 2015).

O RGPD passou a ser diretamente aplicável em todos os Estados-Membros a partir de 25 de maio de 2018, dois anos após a sua adoção e entrada em vigor[34], aplicando-se a todas as entidades que tratem dados pessoais de pessoas singulares, devendo todas as entidades que efetuem tratamentos de dados pessoais observar, sem exceção, as normas nele previstas, todavia, e contrariamente ao estigma social que se criou com o RGPD, não se trata de um diploma europeu cujo paradigma subjacente é de correção e punição das grandes empresas que tratam dados pessoais à escala mundial, dado que "o RGPD toma

[34] Embora o RGPD tenha sido aprovado em 2016, o seu artigo 99.º estabelece que o mesmo apenas passaria a ser aplicável em todos os Estados-Membros a 25 de maio de 2019, de modo a permitir que os Estados-Membros adotassem medidas necessárias à correta vigência do RGPD.

como paradigma a tecnologia hoje disponível para a realização de tratamentos de dados pessoais e, portanto, visa conciliar a utilização de soluções tecnológicas no seu estado atual e futuro de desenvolvimento, e os riscos que comportam, com a defesa dos direitos e liberdades das pessoas cujos dados são objeto de tratamento" (Comissão Nacional de Proteção de Dados, 2018).

2.4.3 No contexto nacional

Analogamente à legislação europeia, a proteção dos dados pessoais em Portugal encontra-se consagrada como um direito fundamental na Constituição da República Portuguesa e demais legislação nacional, sendo a violação dos dados pessoais punida como crime ou contraordenação no ordenamento jurídico português.

Em Portugal, a proteção de dados enquanto direito fundamental encontra-se consagrado como tal desde o texto originário da Constituição da República Portuguesa de 1976 no seu artigo 35.º[35], com a epígrafe "Utilização da informática", tendo o legislador constitucional nacional adotado uma postura vanguardista na consagração constitucional de direitos que acautelem os dados pessoais das pessoas singulares no que alude ao uso de meios informáticos para o tratamento automático dos dados pessoais, elucidando-se o legislador constitucional nos estudos do Comité sobre a Proteção da Vida Privada sobre os potenciais perigos da utilização dos dados pessoais eletrónicos e nas

[35] Artigo 35º da Constituição da República de 1976 (redação originária): *"1. Todos os cidadãos tem o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização. 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos. 3. É proibida a atribuição de um número nacional único aos cidadãos."*
Artigo 35º da Constituição da República de 1976 (revista pelas Leis Constitucionais n.ºs 1/82, de 30 de setembro, 1/89, de 8 de julho, 1/92, de 25 de novembro, 1/97, de 20 de setembro e 1/2001, de 12 de dezembro,1/2004, de 24 de julho e 1/2005, de 12 de agosto): "1. *Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei."*

resoluções[36] aprovadas pelo Conselho da Europa na sequência da ação do referido Comité, que antecederam a Convenção n.º 180.

A redação originária do artigo 35.º da Constituição era composta apenas por três números, o número 1 consagrava o direito à informação e acesso do titular aos seus dados pessoais, o número 2 versava sobre a proibição de tratamento de dados pessoais sensíveis, por sua vez o número 3 proibia a criação de um número único nacional que identificasse cada indivíduo.

O artigo 35.º da Constituição da República Portuguesa consagra direitos fundamentais de proteção contra o tratamento informático de dados pessoais, sendo que na aceção de Canotilho & Moreira (1984) essa proteção concretiza-se em três direitos, designadamente, "o direito de acesso aos registos informáticos para conhecimento dos seus dados pessoas deles constantes, direito ao sigilo em relação a terceiros dos dados pessoais informatizados e direito à sua não interconexão, direito à proibição de tratamento informático de certos tipo de dados pessoais", sendo que "a proibição do número nacional único funciona como garantia daqueles direitos, dificultando o tratamento informático de dados pessoais e a sua interconexão, que seria facilitada com um identificador comum".

No ordenamento jurídico português vigorava a Lei n.º 67/98, de 26 de outubro, Lei da Proteção de Dados, que trânspus para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho, todavia e conforme supramencionado, o legislador europeu no RGPD permitiu que os Estados-Membros especificassem a nível interno determinados aspectos de execução do RGPD, sendo que pelo Despacho n.º 7456/2017 da Presidência do Conselho de Ministros foi criado um grupo de trabalho com

[36] As resoluções do Conselho de Europa não constituem documentos juridicamente vinculativos, tratando-se de documentos que exprimem posições do Conselho de Europa relacionadas com as áreas de atividade da União Europeia.

o objetivo de preparar e elaborar uma proposta de lei de execução do RGPD, tendo nesta sequência surgido a Proposta de Lei 120/XIII.

Ora, apesar de aprovada em Conselho de Ministros e reencaminhada à Assembleia da República, a Proposta de Lei 120/XIII não foi aprovada, tendo sido alvo do Parecer n.º 20/2018, de 2 de maio de 2018, da Comissão Nacional de Proteção de Dados[37], que teceu duras e acérrimas críticas, apontando imprecisões, reprodução de normas do RGPD e normas que se contradizem[38].

[37] Disponível em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e4554456376524739 6a6457316c626e527663306c7561574e7059585270646d464462323170633334e686279396a5a57593359544d794f4330325a44526c4c54526c4e546b74596a41304e4331694e54426d4f5449314d6a64684d7a45756347526d&fich=cef7a328-6d4e-4e59-b044-b50f92527a31.pdf&Inline=true, consultado a 5/06/2019.

[38] No parecer n.º 20/2018 a CNPD invoca, entre outros, o desrespeito pelo direito da União Europeia na medida em que "a presente Proposta pretende reproduzir em alguns artigos parte do articulado do RGPD. É esse, designadamente, o caso do artigo 2.º (âmbito de aplicação), do artigo 11.º (funções do encarregado de proteção de dados) ou do artigo 13.º (encarregados de proteção de dados em entidades privadas). E não se trata aqui sequer de legislar sobre aspetos específicos que o Regulamento remeta para o campo de ação do Estado-Membro, mas apenas de uma tentativa de replicar disposições, com a agravante de, em alguns casos concretos, desvirtuar por completo o teor do RGPD, contrariando-o grosseiramente. Em segundo lugar, a Proposta pretende introduzir no direito nacional norma que difere a aplicação do RGPD para momento posterior à data prescrita no artigo 99.º do próprio Regulamento. Assim, apesar do RGPD ser aplicável a partir de 25 de maio de 2018, seria possível, nos termos do proposto no artigo 61.º (renovação do consentimento) da Proposta, demorar seis meses desde a entrada em vigor da lei nacional para obter um consentimento que constituiria o fundamento de legitimidade para certos tratamentos de dados, admitindo-se portanto a contrario a existência de tratamentos ilícitos durante esse período de tempo. (…) O esforço de repetição de normas do Regulamento na lei nacional assume ainda maior gravidade quando o texto da Proposta entra em clara contradição com o conteúdo dos preceitos do RGPD", salientando ainda que "o artigo 2.º da Proposta sobre o âmbito de aplicação da lei nacional. O n.º 1 deste artigo prescreve: «[A] presente lei aplica-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante (…), aplicando-se todas as exclusões previstas no artigo 2.º do RGPD». A alínea a) do n.º 2 determina que: «[A] presente lei aplica-se aos tratamentos de dados pessoais realizados fora do território nacional quando sejam efetuados no âmbito da atividade de um estabelecimento situado no território nacional». Com efeito, estas normas traduzem-se numa manifesta violação do artigo 3.º, n.º 1, do RGPD, pondo em causa o mecanismo de balcão único que constitui uma das características mais emblemáticas deste regulamento". Invocando ainda a existência de desconformidades com o direito da união no que concerne às normas relativas à autoridade de controlo em matéria de proteção de dados, assim como o facto de a proposta de lei no seu artigo 11.º estabelecer "funções adicionais aos encarregados de proteção de dados, quando tal não é permitido pelo RGPD", acrescentando que os n.º 3 e 4 do artigo 12.º não cumprem com o preceituado no RGPD, devendo para o efeito ser suprimidos, na medida que dispõe sobre matérias que não se encontram na disponibilidade dos Estados-Membros. O mesmo acontece com o artigo 18.º, que dispõe sobre a portabilidade e interoperabilidade dos dados, e o artigo 22.º sobre a transferência de dados, onde pretende-se legislar sobre matéria não permitida pelo RGPD, ao mesmo tempo que se altera o alcance das disposições do RGPD. Outra crítica suscitada foi a relacionada com o dever de sigilo, sendo que "o artigo 20.º da Proposta suscita uma crítica veemente da CNPD pela violação flagrante da nossa Constituição e da Carta dos Direitos Fundamentais da União Europeia, além do incumprimento manifesto do RGPD, ao impedir liminarmente o exercício do direito de acesso". Outro dos pontos criticados prendeu-se com a consagração nos artigos 23.º (admite que os dados pessoais sejam tratados por entidades públicas para finalidades diferentes das que justificaram a recolha, desde que esteja em causa a prossecução do interesse público), 44.º e 54.º (preveem a isenção de coimas para as entidades públicas) da proposta de um regime diferenciado para os tratamentos de dados em que os responsáveis ou subcontratantes são entidades públicas. O modo como o legislador nacional optou por legislar em matérias de regulação obrigatória para o legislador nacional, nomeadamente, acreditação e certificação, idade para o consentimento de menores, tratamento de dados para efeitos de liberdade de expressão e de informação, para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, audiência dos interessados e os mecanismos de cooperação e coerência, também foi alvo de crítica. A CNPD também se pronunciou sobre consagração de limites máximos inferiores aos definidos no RGPD no que concerne ao regime sancionatório, concluindo que "o RGPD deixou às autoridades de controlo o poder de aplicar em concreto coimas nos montantes máximos aí previstos, naturalmente com a ponderação dos critérios orientadores do cálculo da coima a que se refere o artigo 83.º. Donde, a fixação em abstrato, em lei nacional, de limites máximos inferiores aos previstos nos n.ºs 4 e 5 do artigo 83.º do RGPD constituir uma violação dos mesmos. O mesmo raciocínio tem de valer para a fixação de limites mínimos, uma vez que o RGPD não deixa espaço ao legislador nacional para definir quadro sancionatório diferente do que está estabelecido nos n.ºs 4 e 5 do artigo 83.º do RGPD".

Por sua vez, a 14 de julho de 2019 foi aprovada na Assembleia da República a proposta de Lei n.º 120/XIII/3.ª[39], que assegura a execução, na ordem jurídica nacional, do RGPD, tendo a mesma sido promulgada pelo Presidente da República a 26 de julho e publicada a 8 de agosto, sob a Lei n.º 58/2019, de 8 de agosto, passados um ano e três meses da produção de efeitos do RGPD.

Todavia, a 20 de setembro de 2019 a CNPD publicou na sua página oficial a Deliberação 2019/494[40], que aplica um rude golpe sobre a Lei n.º 58/2019, deliberando desaplicar 15 disposições da referida lei de modo a "assegurar o primado do direito da União Europeia e a plena efetividade do RGPD", na medida que "decorre do princípio do primado que, além dos tribunais nacionas, também as entidades administrativas estão obrigadas a desaplicar as normas nacionais que contrariam o direito da União Europeia, como determinou expressamente o TJUE, no acórdão Fratelli Contanzo[41], 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".

A deliberação *in casu* surge na sequência de no Parecer n.º 20/2018, de 2 de maio de 2018, que a CNPD emitiu sobre a Proposta de Lei n.º 120/XIII/3.ª, terem sido elencados normas que a CNPD considerava suscetíveis de violar o direito da União Europeia e, em especial, do RGPD, sendo que a Lei n.º 58/2019, de 8 de agosto, manteve algumas das normas assinaladas como violadoras do direito da União.

---

[39] Diário da República, II série A, N. º89/XIII/3 de 26/03/2018 p. 30-48.
[40] Disponível em: https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_494.pdf?fbclid=IwAR1IQijM3fnl4JfN9jInj8C0uqW4ypczSQexMMTtE1Xa5KxkbG4DV_7J8Ds, consultado a 20/09/2019.
[41] Acórdão do TJUE de 22 de junho de 1989, processo 103/88, disponível em: http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30d52b26c65a76604e50811a96dd39ff0903.e34KaxiLc3qMb40Rch0SaxuNbxr0?text=&docid=96045&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=19496

Neste sentido, a CNPD deliberou desaplicar o número 1 e 2 do artigo 2.º, o número 1 do artigo 20.º, artigo 23.º, alínea a) do número 3 do artigo 28.º, o número 2 do artigo 37.º e o número 2 do artigo 38.º, os números 1 e 3 do artigo 39.º, número 2 do artigo 61.º e número 2 do artigo 62.º. Segundo a CNPD, a não aplicação, em futuros casos concretos, destas disposições legais, implicando tal a aplicação direta das normas do RGPD, que estavam a ser por aquelas "manifestamente restringidas, contrariadas ou comprometidas no seu efeito útil".

2.5 O RGPD: fundamentais progressos

O RGPD veio desenvolver, alargar e aplicar as normas, princípios e direitos estabelecidos na Diretiva 95/46/CE, nomeadamente, fortalecendo os princípios da transparência, minimização dos dados e limitação da finalidade consagrados na diretiva, assim como as regras relativas ao consentimento e à notificação da violação dos direitos dos titulares de dados pessoais, aperfeiçoando a sua aplicação nos Estados-membros.

No presente capítulo pretende-se abordar as principais alterações e evoluções introduzidas pelo RGPD, nomeadamente, no que concerne à definição de dados pessoais, tratamento de dados pessoais, princípios relativos ao tratamento de dados pessoais, consentimento, direitos do titular dos dados, âmbito de aplicação territorial, transferência de dados pessoais para países terceiros, a figura do encarregado de proteção de dados, regime de autorregulação em oposição ao regime heteroregulatório, avaliação de impacto sobre a proteção de dados, consulta prévia, segurança dos dados, assim como o novo quadro sancionatório.

2.5.1 Dados pessoais

Uma das mais importantes definições para a compreensão do RGPD é a de dados pessoais, na medida em que o Regulamento protege os dados pessoais de pessoas singulares[42], vivas, não abrangendo o tratamento de dados pessoais relativos a pessoas coletivas.[43]

Tanto a Diretiva como o Regulamento estabelecem que os princípios da proteção de dados aplicam-se "a todo e qualquer tratamento de dados pessoais sempre que as atividades do responsável pelo tratamanto sejam regidas pelo direito comunitário", excluindo-se do escopo de aplicação o tratamento de dados pessoais efetuados por pessoa singular no exercício de atividades exclusivamente pessoais ou doméstica[44].

Considerando que desde 1995 os meios técnologicos e digitais sofreram uma evolução significativa, uma das mais importantes evoluções do RGPD é o conceito de dados pessoais, sendo que o RGPD consagrou um conceito de dados pessoais lato, embora o conceito se mantenha idêntico ao anteriormente consagrado, por força da evolução da tecnológia da informação e considerando a infinitude de informações que possibilitam a identificação dos titulares de dados, o RGPD consagra este novo panorama no seu conceito.

Neste sentido, na aceção do artigo 2.º da Diretiva 95/46/CE entendia-se por dados pessoais "qualquer informação relativa a uma pessoa singular, identificada[45] ou identificável [46](«pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente, por referência a um número

[42] Artigo 1.º da Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro e artigo 1.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril.
[43] Em oposição ao estipulado no RGPD, a lei nacional de execução do RGPD, a Lei n.º 58/2019, de 8 de agosto, no seu artigo 17.º refere a proteção dos dados pessoais das pessoas falecidas que integrem na categoria de dados especiais.
[44] Artigo 3.º da Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro e artigo 2.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril.
[45] Uma pessoa singular é identificada quando a informação permite de forma direta e individual conhecer a sua identidade, por exemplo, através do seu nome, número de identificação civil ou fiscal, entre outras.
[46] Uma pessoa singular é identificável quando mediante agregação de informações ou de forma indireta é possível alcançar a identidade da mesma, por exemplo, características físicas agregadas, localização, *et cetera*.

de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

Do mesmo modo, a alínea a) do artigo 3.º da Lei n.º 76/98, de 26 de outubro[47], que transpôs a Diretiva 95/46/CE para o ordenamento jurídico português, definiu dados pessoais 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".

Por sua vez, o artigo 4.º do RGPD define dados pessoais 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 ou a um dos mais elementos específicos da identidade física, fisiologica, genética, mental, económica, cultural ou social dessa pessoa singular".

Ora, na definição da Diretiva não é feita alusão à identificação do titular de dados pessoais através de um identificador, sendo que na aceção do RGPD o titular de dados pessoais poderá ser direta ou indiretamente identificada, verificando-se nestes termos um alargamento do conceito de dados pessoais, que passa a abranger, dados biométricos, dados de geolocalização e identificadores por via eletrónica, nomeadamente, *Internet Protocol* (IP), testemunhos de conexão (*cookies*), identificação por radiofrequência, entre

[47] Revogada pela Lei n.º 58/2019, de 8 de agosto, Diário da República n.º 151/2019, Série I de 2019-08-08, p. 3-40.

outros, sendo que nos termos do considerando 3º do referido regulamento "esses identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares".

Na aceção de Francisco, D., & Francisco, S. (2019) "o teste decisivo para decidir se são dados pessoais para o RGPD ou não, consiste em avaliar se esses dados podem ser usados direta ou indiretamente para identificar uma pessoa. Enquanto o nome de uma pessoa identifica obviamente a mesma, a verdade é que algumas combinações de identificadores indiretos também permitem essa identificação" (p.29).

Pinheiro (2016) esclareceu que "o conceito de dados pessoais abrange uma pluralidade de informação pessoal que pode variar do nome à informação genética" (p.374).

Por sua vez, a Comissão Europeia definiu o conceito de dados pessoais como a "informação relativa a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identidicação de uma determinada pessoa. Dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados, mas que possam ser utilizados para reindentificar uma pessoa, continuam a ser dados pessoais e são abrangidos pelo âmbito de aplicação do RGPD"[48], exemplicando o que integra o conceito de dados pessoais, nomeadamente, "o nome e apelido, o endereço de uma residência, um endereço de correio eletrónico como nome.apelido@empresa.com, o número de um cartão de identificação, dados de localização (por exemplo, a função de dados de localização num telemóvel), um endereço IP (protocolo de internet), testemunhos de conexão *(cookies*), o identificador de

[48] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt, consultado a 4/03/2019.

publicidade do seu telefone, os dados detidos por um hospital ou médico, que permitam identificar uma pessoa de forma inequívoca", exemplificando dados considerados não pessoais, designadamente, o número de registo de empresa, um endereço de correio eletrónico como info@empresa.com, dados anonimizados".

Castro (2013) ilustrou o que são dados pessoais, estabelecendo que "são dados pessoais, para além do nome ou da morada, outros dados de identificação como o número de identificação civil, de passaporte, da segurança social, de constribuinte, ou de cliente de um estabelecimento comercial, assim como o número de telefone, o e-mail, o IP do nosso computador, uma chapa de matrícula, o valor de uma retribuição, o som da voz registada para permitir o acesso a uma conta bancária, as classificações escolares e *curriculum*, a história clínica, as dívidas e créditos, as compras que alguém efetua, o registo dos meios pagamento que utiliza, desde que, por estarem associados a uma pessoa, permitam identificá-la. É também o caso de uma impressão digital, de uma imagem biométrica do rosto, de uma imagem recolhida através do uso de uma câmara, como nos casos da videovigilância, ou de um conjunto de fotografias divulgadas na internet" (p.122).

Importa salientar que dados pessoais que tenham sido pseudonomizados[49] e encriptados, mas que possam ser utilizados para identificar um cidadão continuam a ser tratados como dados pessoais e encontram-se dentro do escopo do RGPD.

[49] Nos termos do número 5 do artigo 4.º do RGPD entende-se por pseudonimização "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".

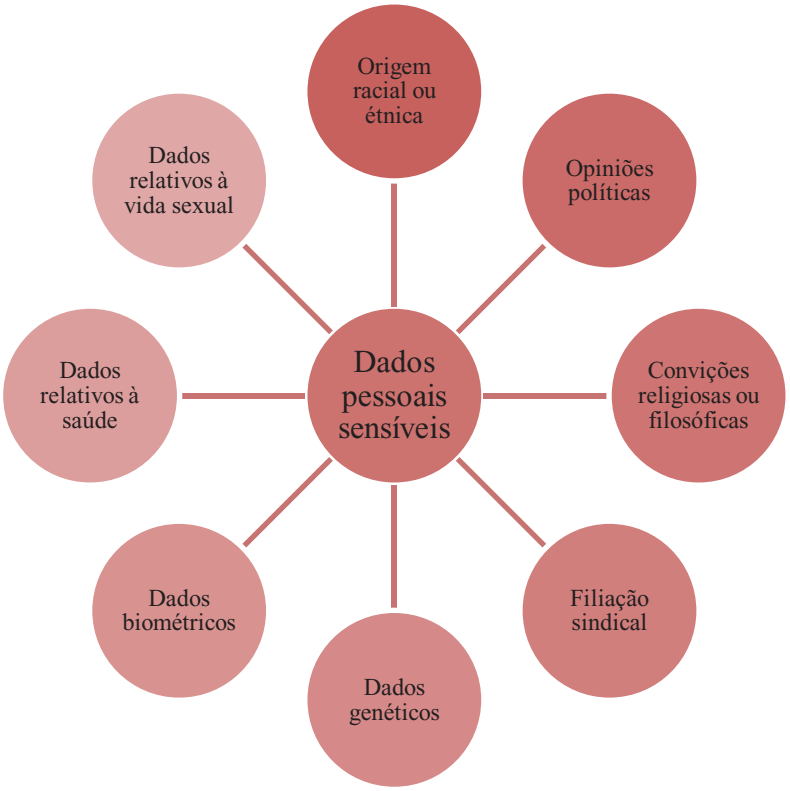
Na realidade, o tratamento de dados pessoais só deixam de estar sobre a alçada do RGPD quando os dados tenham sido anonimizados[50] e o processo de anonimização seja irreversível[51].

De igual modo, o RGPD procedeu ao alargamento das categorias especiais de dados pessoais, sendo que o artigo 9.º do RGPD estabelece como tal dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convições religiosas ou filosóficas,

[50] De acordo com o considerando 26 da Diretiva 95/46/CE a anonimização consiste num procedimento mediante o qual são retirados elementos suficientes de modo a que deixe de ser possível identificar o titular dos dados pessoais.
[51] A própria Comissão Europeia efetuou esse esclarecimento, clarificando que "dados pessoais que tenham sido tornados anónimos de modo a que a pessoa não seja ou deixe de ser identificável deixam de ser considerados dados pessoais. Para que os dados sejam verdadeiramente anonimizados, a anonimização tem de ser irreversível". Disponível em: ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt, consultado a 20/09/2019.

filiação sindical, dados genéticos[52], dados biométricos[53], dados relativos à saúde[54], dados relativos à vida sexual ou orientação singular de uma pessoa.

Figura 4 - Categorias especiais de dados pessoais



Por sua vez, a diretiva incluía no escopo das categorias específicas de dados[55] apenas os dados associados à origem racial ou étnica, opiniões políticas, convições religiosas ou filosóficas, filiação sindical, dados relativos à saúde e à vida sexual.

O Memorando da Comissão de Ética sobre "Orientações éticas para a investigação com sujeitos humanos em contextos letivos" define dados pessoais sensíveis como dados

[52] O número 14 do artigo 4.º do RGPD define dados genéticos como os dados relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma mostra biológica proveniente de uma pessoa singular em causa.
[53] O artigo 4.º número 14 do RGPD define dados biométricos como dados que resultam de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente, imagens faciais ou dados dactiloscópicos. Por sua vez o considerando 51 esclarece que o tratamento de fotografias de cidadãos não deverá ser considerado como um tratamento de dados sensíveis, uma vez que apenas são abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular.
[54] O artigo 4.º do RGPD no seu número 15 define dados relativos à saúde como os dados relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde que revelem informação sobre o estado de saúde.
[55] Artigo 8.º da Diretiva 95/46/CE.

que "enquadram-se num conjunto específico de dados pessoais que devem ser tratados com particular cuidado, pelo pontencial discriminatório que encerram e pela condição de vulnerabilidade que podem impor ao próprio indíviduo a quem os dados pertencem ou a outros indíviduos com ele relacionados" (Universidade dos Açores, 2018)[56].

O considerando 51 do RGPD alicerça a proteção específica dos dados pessoais especialmente sensíveis no facto de tratamento potencialmente poder "implicar riscos significativos para os direitos e liberdades fundamentais".

2.5.2 Tratamento de dados pessoais

O RGPD adotou um conceito de tratamento de dados pessoais análogo ao consagrado na Diretiva 95/46/CE, tratando-se de definição extremamente ampla, no entanto não é exaustiva. Na prática, o tratamento de dados inclui qualquer interação com os dados pessoais, independentemente da forma que tal interação aconteça.

Assim, nos termos do número 2 do artigo 4.º do RGPD entende-se por tratamento de dados pessoais quaisquer operações efetuadas sobre os dados pessoais, por meios automatizados ou não automatizados, "tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição".

Em Portugal, a alínea b) do artigo 3.º da Lei n.º 67/98, de 26 de outubro, designada por LPDP[57] definia o tratamento como qualquer operação sobre dados pessoais, "efetuada

---

[56] AA.VV. *Memorando da Comissão de Ética sobre Orientações Éticas para investigação com sujeitos humanos em contextos letivos*. Universidade dos Açores, 2018

[57] Revogada pela Lei n.º 58/2019, de 8 de agosto, Diário da República n.º 151/2019, Série I de 2019-08-08, p. 3-40.

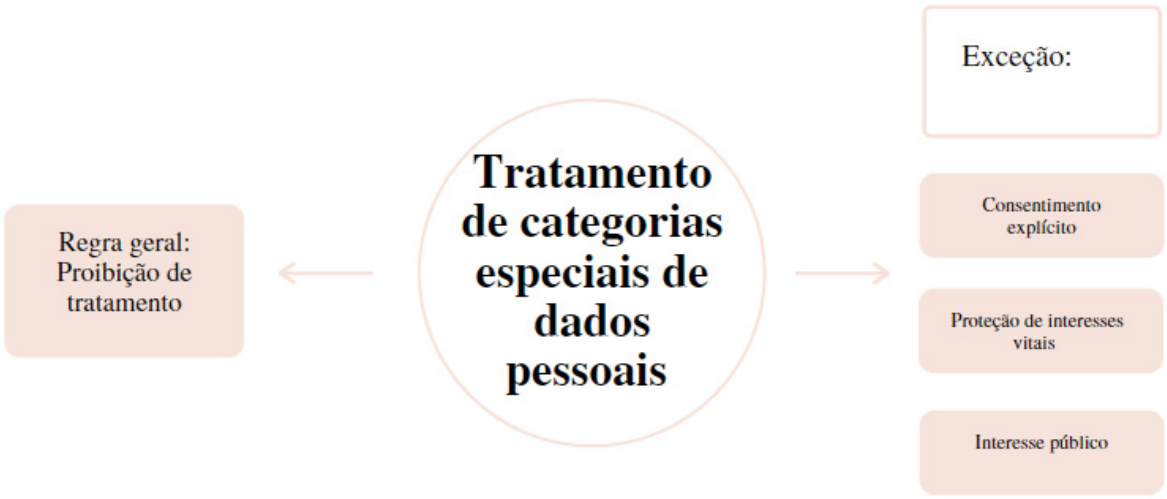
com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição".

O tratamento automatizado de dados pessoais, isto é, operações de tratamento que se concretizam com o apoio de meios tecnológicos, permite a definição de perfis dos titulares de dados pessoais, o que posteriormente permite o direcionamento de ofertas de bens e serviços especificos.

Saliente-se que o regulamento proíbe o tratamento de categorias especiais de dados pessoais, contudo o número 2 do artigo 9.º do RGPD estabelece situações em que a proibição não se aplica, nomeadamente, quando o titular dos dados tiver dado o seu consentimento explícito para o efeito[58], assim como quando o tratamento for necessário para proteger interesses vitais do titular dos dados ou de outra pessoa singular ou por motivos de interesse público importantes.

[58] Neste sentido *vide,* a título de exemplo, o Memorando da Comissão de Ética sobre "Orientações éticas para a investigação com sujeitos humanos em contextos letivos", que estabelece condições e requisitos do consentimento informado.

Figura 5 - Tratamento de categorias especiais de dados pessoais



Considerando que o tratamento de dados pessoais desencadeia novos e atraentes modelos de negócios para as empresas, principalmente no que concerne às técnicas de *big data* que permitem processar grandes quantidades de dados, assume particular relevância o conceito de atividades de tratamento de dados pessoais, na medida em que tais atividades podem afetar gravemente a privacidade dos dados pessoais e muitas vezes constituem tratamentos de dados pessoais de alto risco. Estabelecer os tratamentos de dados efetuados pela organização é uma parte signficativa de cumprimento do RGPD.

2.5.3 Princípios relativos ao tratamento de dados pessoais

O RGPD acautela a proteção de dados pessoais dos titulares dos dados pessoais através de princípios orientadores que norteiam e enquadram os normativos relativos à proteção de dados pessoais, assim como as situações específicas de tratamentos ~~a~~ de dados pessoais.

No RGPD verificou-se um reforço dos princípios já consagrados na Diretiva 95/46/CE, assim como a consagração de novos princípios orientadores da conduta dos

responsáveis pelo tratamento, subcontratantes e terceiros, elencando-os de forma estruturada no seu artigo 5.º.

Os princípios contemplados do RGPD impõem ao responsável pelo tratamento um comportamento transparente e leal para com o titular dos dados pessoais, de modo a que

este veja os seus direitos acautelados.

Nesta medida, o RGPD assume como axiais os princípios da licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade, confidencialidade e responsabilidade[59].

Figura 6 - Hierarquia de princípios relativos ao tratamento de dados pessoais

Por sua vez, o princípio da licitude, ao estar instrinsecamente relacionado com o princípio da transparência e da lealdade, implica que para um tratamento seja lícito os dados pessoais devem ser tratados com base no consentimento do titular dos dados ou em

[59] Artigo 5.º do RGPD.

outro fundamento previsto na lei, quer no RGPD quer em outro ato de direito da União ou de um Estado-Membro[60].

O artigo 6.º do regulamento, que corresponde ao artigo 7.º da Diretiva 95/46/CE, elenca os fundamentos de licitude do tratamento, estabelecento que este só é lícito quando o titular dos dados tiver dado o seu consentimento para uma ou mais finalidades especifícas, quando for necessário para a execução de um contrato do qual a pessoa singular seja ou vá em breve ser parte, para o cumprimento de uma obrigação jurídica[61], para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular, para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, para efeito dos interesses legítimos[62] prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto quando prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais.

Neste sentido, D. Francisco & S. Francisco (2019) esclarecem que "na existência de uma missão de interesse público ou levada a cabo no interesse de uma autoridade pública, as Entidades Públicas, desde que devidamente legitimadas por lei (da UE ou de Portugal), possuem licitude para efetuar tratamento de dados pessoais sem necessidade de consentimento do titular dos dados (a pessoa singular)" (p.34).

---

[60] Considerando 40 do RGPD.

[61] O fundamento jurídico do tratamento realizado ao abrigo de uma obrigação jurídica ou quando o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento é definido pelo direito da União ou do Estado-Membro ao qual o responsável pelo tratamento está sujeito.

[62] Considerando 47 do RGPD "… a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta".

Por sua vez. o princípio da lealdade relaciona-se diretamente com a transparência do tratamento, devendo o responsável pelo tratamento dar a conhecer ao titular dos dados os riscos associados ao tratamento efetuado, os seus diretos e as regras que regulam o tratamento, implicando que o tratamento dos dados seja realizado de acordo com a finalidade para os quais foram recolhidos.

A LPDP no seu artigo 2.º consagrava o princípio da transparência como o princípio geral[63], sendo que o princípio da transparência surge como pedra basilar no novo paradigma de proteção de dados, concretizando-se através do exercício dos direitos de informação e de acesso, traduzindo-se no direito do titular dos dados a deter pleno conhecimentos do tratamento efetuado aos dados, da identidade do responsável pelo tratamento, das finalidades de tratamento, dos seus direitos e dos meios que dispõem para exercer os seus direitos.

Nestes termos, o considerando 39 do RGPD estabelece que o tratamento deverá ser realizado de forma transparente de modo a que os titulares dos dados tenham pleno conhecimento dos dados pessoais que são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento, assim como a medida em que os dados são ou virão a ser tratados, implicando que as informações e comunicações transmitidas ao titular dos dados seja feita numa linguagem clara e simples, permitindo o seu fácil acesso e compreensão.

O GT29 (2017) esclareceu que "a transparência é uma obrigação abrangente nos termos do RGPD aplicável a três domínio centrais: 1) o fornecimento de informações aos titulares dos dados relacionado com o tratamento leal; 2) de que forma os responsáveis

[63] "O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais".

pelo tratamento comunicam com os titulares dos dados em relação aos direitos destes ao abrigo do RGPD; e 3) de que forma os responáveis pelo tratamento facilitam o exercício dos direitos dos titulares dos dados" (p.4).

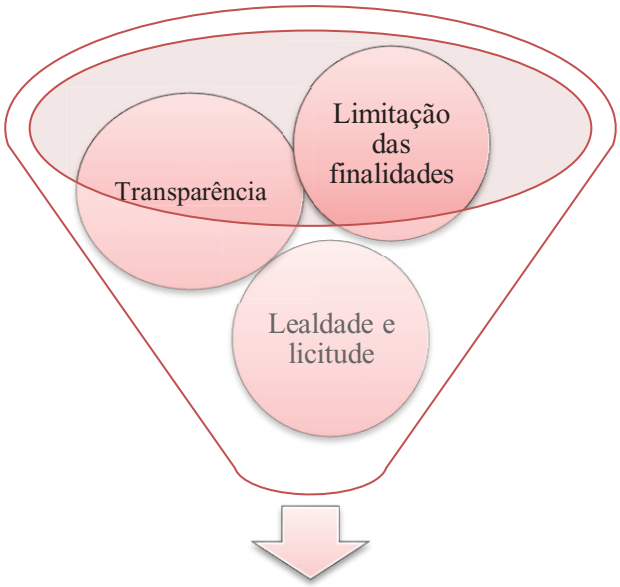
Nati (2018) considera que "oferecer transparência no modo como os dados pessoais são usados (…) resulta nos seguintes benefícios para o ecosistema de dados pessoais: Para os indíviduos (ao partilhar dados pessoais com organizações), (…) forneceder aos utilizadores uma melhor compreensão do que eles estão a deixar as organizações fazerem como os seus dados pessoais, sem ter que ler longos documentos escritos por advogados e para advogados, e não por utilizadores de serviços digitais. Como resultado do aumento da transparência e controlo de que os dados pessoais não vão acabar nas mãos erradas, a confiança do utilizador aumentará. Consequentemente, os utilizadores estarão mais dispostos a partilhar informações pessoais, sabendo exatamente para que serão usados e quanto controlo eles têm sobre os seus dados. Para as organizações (ao fornecer serviços digitais, recolhendo e usando dados pessoais): aumentar a transparência e criar confiança com os clientes/utilizadores implica que as organizações esclareçam como utilizam e processam os dados pessoais, fornecendo declarações de privacidade simplificadas. Ao fazer isso as organizações tornam-se exemplos de atitude centrada nos utilizadores em relação aos dados pessoais e, assim, abrem novos canais de comunicação com os clientes/utilizadores, evitando rotatividade e aumentando o acesso a dados de qualidade dos consumidores" (p.4).

O princípio da limitação das finalidades, assume particular importância na medida em que permite que o titular dos dados ao fornecer os seus dados tenha pleno conhecimento das finalidades para as quais os seus dados serão tratados, limitando tratamentos para finalidades diversas das quais os dados pessoais tenham sido inicialmente recolhidos, estabelecendo a alínea b) do número 1 do artigo 5.º do RGPD que os dados pessoais

devem ser recolhidos para "finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de modo incompatível com essas finalidades"[64].

Nesta medida, há uma correlação direta entre o princípio da limitação das finalidades com o princípio da transparência, lealdade e lícitude, na medida em que estes três últimos impõem ao responsável pelo tratamento a obrigação de informar o titular dos dados sobre as finalidades de tratamentos dos dados recolhidos.

Figura 7 - Informação sobre as finalidades de tratamento



O considerando 50 do RGPD esclarece como deverá ser aferida a compatibilidade de uma nova finalidade com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, esclarecendo que o responsável pelo tratamento deverá atentar à existência de uma ligação entre a finalidade primordial e a nova finalidade a que se destina a operação de tratamento que pretende levar a cabo, o contexto em que os dados pessoais foram recolhidas, "em especial as expetativas razoáveis do titular dos dados quanto à sua

[64] Nos termos do número 1 do artigo 89.º do RGPD os tratamentos posteriores para finalidades de arquivo de interesse público, investigação científica ou histórica ou para efeitos estatísticos deverão ser considerados tratamentos compatíveis com as finalidades que legitimaram a recolha de dados e lícitos.

posterior utilização, baseadas na sua relação com o responsável pelo tratamento, a natureza dos dados pessoais, as consequências que o posterior tratamento dos dados pode ter para o seu titular e a existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas"[65].

Acrescenta ainda o considerando 50 que nas situações em que o titular dos dados tenha prestado consentimento ou o tratamento se baseie em disposições do direito da União ou de um Estado-Membro que constituam medidas necessárias e proporcionais, com vista à salvaguarda do interesse público geral, o responsável pelo tratamento poderá proceder ao tratamento posterior de dados pessoais, independentemente da compatibilidade ou não das finalidades de tratamento, devendo, todavia, o titular dos dados ser informado sobre as finalidades que surgiram *a posteriori*, assim como dos seus direitos enquanto titular de dados pessoais.

Alguns autores consideram que o princípio da limitação das finalidades terá um grande impacto nos modelos de *big data*. Neste sentido, Ghani, Hamid & Udzir (2016) consideram que o "*big data* desafia o princípio da limitação das finalidades, e o princípio é uma barreira ao desenvolvimento da análise de *big data (*…) tendo um impacto negativo na eficiência do modelo "aviso e consentimento", uma vez que *"*as análises de *big data* permitem uma análise de dados usando algoritmos diferentes, o que revela correlações inesperadas que podem ser usadas para novos propósitos. O princípio da limitação das finalidades restringe a liberdade de uma organização fazer essas descobertas e inovações" (p. 116–121).

Por outro lado, o princípio da minimização dos dados prevê que os dados pessoais devem ser adequados, pertinentes e limitados ao que é necessário relativamente às

[65] Artigo 6.º número 4 do RGPD.

finalidades para as quais são tratados[66], proibindo a recolha de mais dados pessoais do que aqueles que são necessários e suficientes para a finalidade de tratamento.

Também o princípio da minimização é apontado como um desafio aos modelos de *big data*, na medida que "as organizações são obrigadas a limitar a recolha de dados pessoais ao necessário para atingir os seus objetivos legítimos e a eliminar os que não estão de acordo com esses objetivos. O modelo de negócio big data é antiético a estes princípios. Em vez disso, incentiva a recolha e retenção indireta e direta de quaisquer dados, por qualquer meio técnico" (Sloot, Broeders & Schrijvers, 2016, p.210).

O princípio da exatidão estabelece que os dados devem ser exatos e atualizados, devendo os dados inexatos, considerando as finalidades para as quais são tratados, sejam apagados ou retificados[67].

Por sua vez o princípio da limitação da conservação delimita a conservação dos dados pessoais, vedando conservações por tempo indeterminado, estipulando a alínea e) do número 1 do artigo 5.º do RGPD as regras itinientes à conservação, determinando que os dados pessoais devem ser conservados de forma que "permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os 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 (…), 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". Para o efeito, o

[66] Alínea c) do número 1 do artigo 5.º do RGPD.
[67] Alínea d) do número 1 do artigo 5.º do RGPD.

responsável pelo tratamento deverá estabelecer prazos de conservação, sendo que findo o prazo os dados devem ser apagados, devendo realizar revisões periódicas.

O princípio da integridade e confidencialidade, definido na alínea f) do número 1 do artigo 5.º do RGPD, consagra 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 danificação acidental, adotando as medidas técnicas ou organizativas adequadas". Este princípio assume particular importância na medida em que as organizações deverão adotar medidas que não permitam o acesso aos dados pessoais, danos, destruição ou a utilização dos mesmos por indíviduos não autorizados, devendo ser empregues engenhos de reforço deste princípio tais como a anonimização[68] e a pseudonimização.

O princípio da responsabilidade, por sua vez, imputa ao responsável pelo tratamento a obediência de todos os princípios supra enunciados, assim como o dever de demonstrar *compliance* e comprovar o cumprimento dos princípios relativos ao tratamento de dados pessoais.

Os princípios supramencionados assumem especial relevância no âmbito do novo paradigma de proteção de dados, devendo as entidades orientar os tratamentos de dados que efetuam por estes, verificando-se, todavia, um grande desconhecimento dos princípios a observar quando se efetuam tratamento, dando-se azo a tratamentos de dados ilícitos, seja por desconhecimento do fundamento de licitude de tratamento de dados, pedidos de consentimentos desnecessários, desconhecimento da origem dos dados, recolha de dados sem uma finalidade específica ou até recolha de dados para finalidades

[68] A anonimização consiste em técnicas que dividem a informação, de modo a que não seja possível a identificação do titular dos dados, tratando-se de uma operação irreversível, diversamente, a pseudonimização consiste em técnicas de separação de dados de modo a impossibilitar a identificação do titular dos dados, contudo é possível agregar os dados de modo a que seja identificado o titular dos dados, utilizando-se em situações em que seja necessário identificar o titular dos dados.

ilegítimas, assim como conservação de dados para além do tempo necessário e ausência de medidas de segurança efetivas para proteção dos dados pessoais.

2.5.4 Consentimento

De acordo com o RGPD, o consentimento do titular dos dados constitui um dos fundamentos legítimos para o tratamento de dados pessoais. No entanto, muitas organizações consideram que, na prática, o consentimento é o único fundamento de licitude para tratamento de dados na maioria dos casos. Exemplo disso é o facto de nos meses que antecederam a produção de efeitos do RGPD verificou-se uma lamentável enchente de pedidos de consentimentos por parte das entidades, totalmente equivocadas no que concerne à figura do consentimento e sobre os fundamentos de tratamento de dados, lançando mão de pedidos de consentimentos absolutamente inúteis[69], conforme infra se abordará, sendo que na maior parte existia outro fundamento do tratamento, por exemplo, como o cumprimento de um contrato.

Neste sentido, o consentimento já na Diretiva 95/46/CE constituia fundamento de legitimidade do tratamento de dados, previsto no artigo 7.º alínea a). Contudo, no RGPD a figura do consentimento é aprimorada, sendo impostas condições mais exigentes para que o mesmo seja lícito e legítimo.

Assim, a Diretiva definia consentimento como a "manifestação de vontade, livre e específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe digam respeito sejam objeto de tratamento"[70].

---

[69] Cfr. Nunes, F., Dantas, A., R., e Amaral, Hugo: "*O RGPD foi mal aplicado por muitas empresas. Pecaram por excesso",* Sapo, 25 de maio de 2019, in https://eco.sapo.pt/entrevista/o-rgpd-foi-mal-aplicado-por-muitas-empresas-pecaram-por-excesso/, consultado a 27/09/2019.

[70] Artigo 2.º alínea h) da Diretiva 95/46/CE.

Por sua vez, o consentimento é definido pelo RGPD como uma "manifestação de vontade, livre, específica, informada e explicíta, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco[71], que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"[72], ou seja, o titular dos dados deverá estar consciente do consentimento que está a prestar e do seu alcance, devendo prestar consentimento para cada uma das finalidades de tratamento.

O RGPD no seu artigo 7.º estabelece as condições aplicáveis ao consentimento. Neste sentido, quando o tratamento de dados pessoais é realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais, assim, deverão ser adotados modelos de consentimento que permitam demonstrar que o mesmo foi prestado licitamente pelo responsável pelo tratamento, nomeadamente, mediante declaração escrita ou oral[73/74].

---

[71] O consentimento deve ser inequívoco na medida em que não devem subsistir dúvidas sobre a vontade do titular dos dados pessoais.
[72] Artigo 4.º número 11 do RGPD.
[73] O considerando 32 do RGPD estabelece que o consentimento pode ser dado "validando uma opção ao visitar um sítio web na Internet (…), sendo que o silêncio, as opções pré-validades ou a omissão não deverão, por conseguinte, constituir um consentimento".
[74] Alguns exemplos de minutas de consentimento para tratamento de dados pessoais disponibilizados *online: Eu, , entidade gestora/titular do nome de domínio , pelo presente declaro, para efeitos do previsto no artigo 13.º do Regulamento Geral de Proteção de Dados (EU)2016/ 679/2016, de 27 de abril, de ora em diante abreviadamente designado por "RGPD", prestar, por este meio, consentimento para tratamento e divulgação, via protocolo WHOIS, em whois.dns.pt e via web, designadamente em www.dns.pt, dos meus dados pessoais, devidamente identificados na alínea f), à …, associação privada sem fins lucrativos, pessoa coletiva número …, na qualidade de presidente do conselho diretivo. Mais declaro, para efeitos designadamente do disposto nos artigos 13.º a 22.º do RGPD, ter tomado conhecimento e compreender que no âmbito do registo do domínio ora identificado: a) O … assume a qualidade de responsável pelo tratamento dos meus dados pessoais; b) A política … e o tratamento de dados pessoais no …obedece ao disposto na legislação relativa à proteção de dados pessoais, bem como na demais legislação aplicável; c) A finalidade do tratamento dos meus dados pessoais consiste na sua divulgação no diretório …., permitindo uma correta associação dos mesmos ao nome de domínio ;d) Os meus dados pessoais não poderão ser tratados para outra finalidade que não seja a indicada na alínea anterior;e) Caso não dê consentimento, os meus dados pessoais não serão publicados sendo, antes, apresentada, na versão web do WHOIS, uma opção de contacto anonimizada, destinado a contacto geral ou a eventuais infrações ou abusos; f) Os dados pessoais que serão divulgados limitam-se ao: nome, morada e email (quando titular do domínio). g) O … designou um Encarregado da Proteção de Dados Pessoais, pelo que poderei contactar diretamente o mesmo, utilizando os meios disponibilizados abaixo, sobre todas questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos meus direitos: Contactos do Encarregado da Proteção de Dados:Email: … h) Que no âmbito dos direitos que a lei me confere se inclui: • Aceder aos meus dados pessoais através da minha área reservada em www….pt, utilizando as respetivas credenciais; • Retificar os meus dados pessoais que se encontrem inexatos ou incompletos através da minha área reservada em www…..pt, contactando o meu Registrar, ou contactando diretamente o DNS.PT através do endereço email request@dns.pt; • Retirar o consentimento, a qualquer momento, à divulgação dos meus dados pessoais no serviço WHOIS, através da minha área reservada em www…..pt, utilizando as respetivas credenciais; • Reclamação à Comissão Nacional de Proteção de Dados Pessoais (www.cnpd.pt), caso considere estar a ser violado algum dos direitos elencados. i) Os meus dados pessoais, ainda que não tornados públicos, poderão ser comunicados ou transferidos, na medida do necessário, às autoridades judiciais, ao ARBITRARE - Centro de Arbitragem de Propriedade Industrial, Nomes de Domínios, Firmas e Denominações, às entidades a quem a lei atribua competências ao nível da investigação criminal, ou que tenham por missão a fiscalização ou prevenção do cumprimento da legislação no âmbito, designadamente da proteção dos direitos dos consumidores, propriedade intelectual, comunicações, segurança, saúde pública e práticas comerciais em geral; j) Os meus dados pessoais serão tratados com recurso a meios automatizados,contudo, enquanto titular dos mesmos, não serei sujeito a decisões automatizadas; k) Os meus dados pessoais*

Acrescenta ainda o artigo 7.º que nas situações em que o consentimento é prestado mediante declaração escrita não exclusiva para o efeito, deverá o pedido de consentimento ser apresentado diferencialmente dos restantes assuntos, de modo compreensível e de fácil acesso, através de numa linguagem clara e simples.

Como Reynolds (1979) elucidou "para ser informado, o consentimento deve ser dado por pessoas que sejam competentes para consentir, tenham consentido voluntariamente, estejam plenamente informadas sobre a pesquisa e tenham compreendido o que lhes foi dito" (p.261).

Uma das questões do RGPD que mais contorvérsia gerou, devido ao seu impacto no modo como as organizações tratam os dados pessoais, assim como pelo seu impacto na análise de *big data*, é o facto de o titular dos dados pessoais poder a qualquer momento retirar o seu consentimento, sendo que tal facto não compromete a licitude do tratamento que foi efectuado com base no consentimento outrora concedido, sendo que o titular dos dados deverá ser informado que poderá retirar o consentimento no momento em que o presta[75].

Neste sentido Politou, Alepis & Patsakis (2018), explicaram que o "*big data* extingue o pouco de esperança que permanece para o regime de notificação e escolha, uma vez que o aviso prévio não é possível caso o valor das informações pessoais não seja aparente no momento da recolha, quando o consentimento é normalmente concedido. Muito menos o facto de as novas classes de bens e serviços geralmente residem em usos futuros e imprevistos. Isso motivou muitas vozes radicais a argumentar contra a necessidade de

apenas serão disponibilizados no serviço… durante o período de vigência do nome de domínio , ou enquanto o consentimento não for retirado. Mais declaro, e considerando o ora enunciado, nomeadamente a identificação dos meus dados pessoais que serão objeto de divulgação, assim como a finalidade específica da mesma, constituir o presente documento uma declaração de consentimento, para os termos e efeitos do RGPD. DATA" Disponível em: https://www.dns.pt/fotos/editor2/declaracao_consentimento.pdf, consultado a 27/09/2019.

[75] Artigo 7.º número 3 do RGPD.

consentimento, que pode comprometer a inovação e os avanços sociais benéficos e, portanto, o seu papel deverá ser circunscrito ao uso prospetivo dos dados e, em casos específicos, o consentimento não deve ser necessário para legitimar o uso de dados pessoais. Ainda assim, para outros estudiosos, os requisitos do consentimento são a última defesa dos indivíduos contra a perda de controlo no processamento de informações pessoais e, assim, eliminar ou reduzir a necessidade de consentimento informado não pode ser aceite acriticamente e sem debate público, particularmente se os ideais democráticos são valorizados" (p.5).

O considerando 42 do RGPD clarifica que de modo a que o consentimento seja prestado de forma informada e esclarecida, o titular dos dados deverá conhecer a identidade do responsável pelo tratamento, assim como as finalidades de tratamento.

Por sua vez, o número 4 do artigo 7.º do RGPD estabelece que para avaliar se o consentimento é prestado de forma livre há que verificar se a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato. Nestes termos quando o titular dos dados não dispuser de uma opção verdadeiramente livre, que não o lese se não for concedido, não se deverá considerar que o consentimento foi prestado de livre vontade.

Com efeito, o considerando 43 do RGPD estipula que para que o consentimento constituía uma verdadeira manifestação de livre vontade "este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que onde exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade

pública pelo que torna-se improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa".

Por sua vez, o artigo 8.º do RGPD define as condições aplicáveis ao consentimento relativo ao tratamento de dados de menores em relação aos serviços da sociedade de informação, estabelecendo que o consentimento só é lícito se o menor tiver, pelo menos, 16 anos de idade, sendo que nas situação em que o menor tenha menos de 16 anos, "o tratamento só é lícito se e na medida em que o consentimento seja dados ou autorizado pelos titulares das responsabilidades parentais da criança".

A segunda parte do número 1 do artigo 8.º do RGPD atribui aos Estados-Membros o poder de definir uma idade inferior para a capacidade do menor *per si* consentir licitamente o tratamento dos seus dados pessoais, desde que a idade não seja inferior a 13 anos. Em Portugal, a Lei n.º 58/2019 no seu artigo 16.º sagrou a idade mínima de 13 anos, estabelecendo que quando a criança tenha idade inferior a 13 anos, o tratamento só é lícito se o consentimento for dado pelos representantes legais desta.

Figura 8 - Idade para o consentimento de menores na União Europeia

Fonte: https://www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751

Neste sentido, o considerando 38 do RGPD consagra a necessidade de estabelecer condições especiais para a licitude do consentimento para o tratamento de dados pessoais de menores no facto de "as crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus diretos relacionados com o tratamento dos dados pessoais", acrescentando ainda que a proteção específica deverá aplicar-se "à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças", isentando o consentimento do titular das responsabilidades parentais nas situações

relacionadas com "serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança".

Nas situações de consentimento para tratamento de dados pessoais de menores, o RGPD define que o responsável pelo tratamento deverá garantir com recurso a "todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível"[76].

As novas condições impostas pelo RGPD para que o consentimento seja válido constituem uma importante proteção do titular dos dados, tendo a sua natureza e uso sido intensamente debatidos pelo recurso ao consentimento em ambientes *on-line*, onde a maioria dos consentimentos são implícitos. Com o RGPD deve cada responsável pelo tratamento adotar as medidas necessárias a demonstrar que o titular dos dados prestou o seu consentimento de forma informada, livre, específica e explícita.

2.5.5 Novos direitos do titular dos dados

Considerando o novo paradigma associada à crescente importância dos dados pessoais, em que o titular dos dados é o dono dos dados e não o responsável pelo tratamento, tornou-se imperioso com o RGPD reforçar os direitos dos titulares dos dados, assim como atribuir novos direitos para além dos reconhecidos pela Diretiva 95/46/CE.

Assim, o RGPD confere ao titular de dados novos direitos individuais, como garantia de maior proteção jurídica, tais como, uma nova vertente do direito ao apagamento dos dados, que se traduz no direito a ser esquecido, o direito à portabilidade dos dados[77] e o

[76] Número 2 do artigo 8.º do RGPD.
[77] A Resolução do Parlamento Europeu, de 6 de julho de 2011, sobre uma abordagem global da proteção de dados pessoais na União Europeia, no seu ponto 16 sublinhava a importância de possibilitar o direito à portabilidade e clarificava o direito do titular de dados de ser esquecido.

direito à limitação do tratamento, reforçando o âmbito dos direitos consagrados na referida Diretiva, nomeadamente, o direito à informação, ao acesso, à oposição ao tratamento, oposição a decisões individuais automatizadas, retificação dos seus dados e eliminação.

Figura 9 - Direitos do titular de dados pessoais.

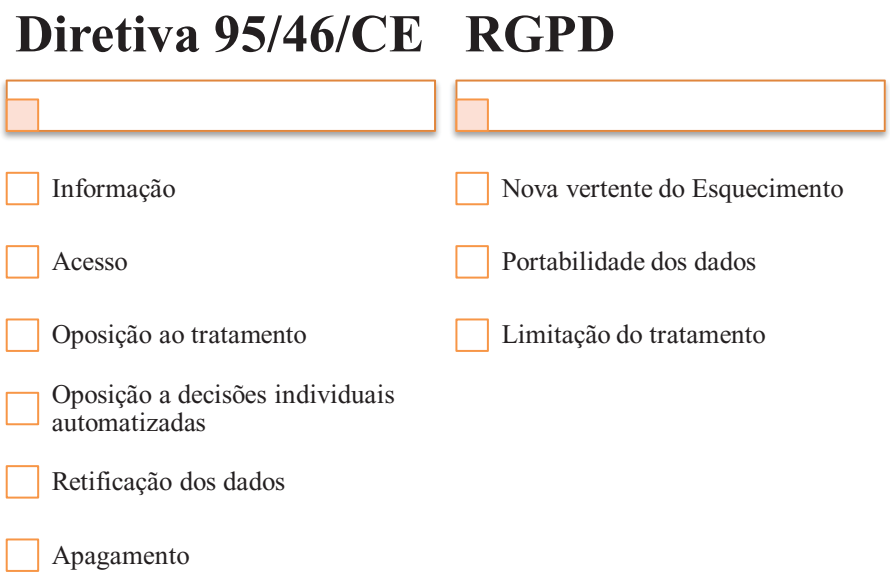
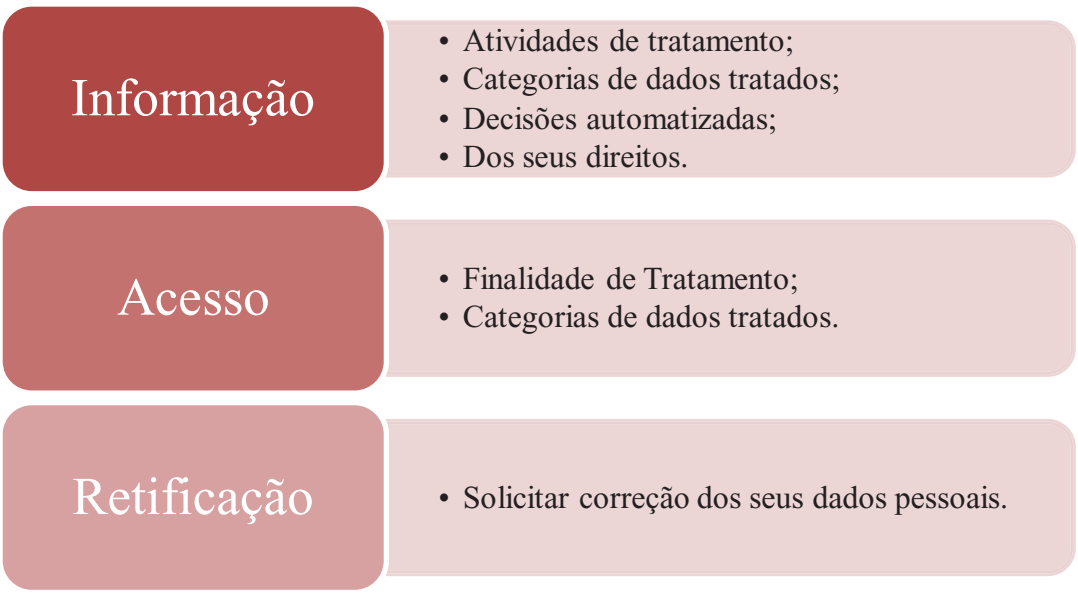
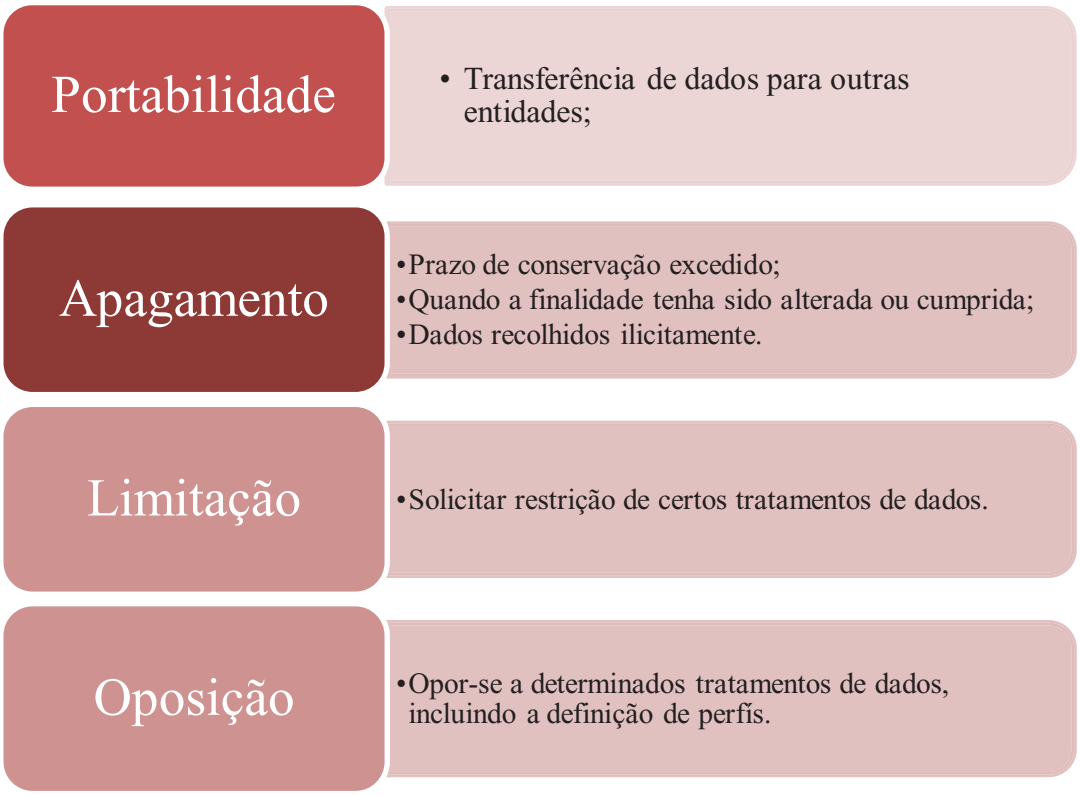


Figura 10 – Esquema dos direitos dos titulares dos dados pessoais





Neste sentido, o direito de portabilidade dos dados encontra-se previsto no artigo 20.º do RGPD, consistindo no direito do titular dos dados de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento em um formato de uso corrente e de leitura automática, e de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram *ab initio* fornecidos o possa impedir.

Conforme o considerando 68 do RGPD "os responsáveis pelo tratamento de dados deverão ser encorajados a desenvolver formatos interoperáveis que permitam a portabilidade dos dados", na medida em que o novo direito de portabilidade ao coadjuvar a transferência mais célere e eficaz de dados pessoais entre responsáveis pelo tratamanento promove o livre fluxo de dados pessoais assim como a realização do Mercado Único Digital.

Todavia, o direito de portabilidade dos dados apenas será aplicável quando o tratamento se basear no consentimento prestado pelo titular nos termos do referido regulamento ou num contrato, tendo o tratamento de ser realizado por meios automatizados[78], assim, não deverá ser aplicável quando o tratamento se basear num fundamento jurídico que não seja a execução de um contrato ou o consentimento.

Sobre o direito à portabilidade Hert *et al.* (2018) consideram que "constitui (…) um caso valioso de desenvolvimento e difusão de tecnologias efetivas de melhoramento da privacidade centrada no utilizador, tecnologias e uma primeira ferramenta a permitir os indívuidos a aproveitar a riqueza imaterial dos seus dados pessoais na economia dos dados. De facto, uma portabilidade gratuita dos dados pessoais de um responsável pelo tratamento para outro pode ser uma forte ferramenta para os titulares dos dados de modo a promover concorrência dos serviços digitais e a interoperabilidade de plataformas e promover o controlo dos indíviduos sobre os seus própios dados" (p.1).

Por sua vez, importa salientar que o exercício do direito à portabilidade dos dados "não desencadeia automaticamente o apagamento dos dados provenientes dos sistemas do responsável pelo tratamento e não afeta o período de conservação inicialmente aplicável aos dados que tiverem sido transmitidos" (GT20, 2017).

O considerando 65 do regulamento refere o direito dos titulares dos dados a serem esquecidos, salientando a particular importância deste direito nas situações em que o consentimento para o tratamento de dados pessoais é prestado quando o titular dos dados era criança e em adulto deseje eliminar esses dados, acrescentando o considerando 66 que de modo a reforçar o direito a ser esquecido no ambiente por via eletrónica, ao responsável pelo tratamento que tenha tornado públicos os dados pessoais deverão ser

[78] Alínea a) e b) do n.º 1 do artigo 20.º do RGPD.

impostos a adoção de “medidas razoáveis, incluindo a aplicação de medidas técnicas, para informar os responsáveis que estejam a tratar esses dados pessoais de que os titulares dos dados solicitaram a supressão de quaisquer ligações para esses dados pessoais ou de cópias ou reproduções dos mesmos”.

Como Politou, Alepis & Patsakis (2018), explicam “esquecer os dados anteriormente recolhidos, obtidos porque o utilizador os submeteu uma vez ou porque um serviço online sorrateiramente os recolheu, foi durante muito tempo um assunto controverso que o Comissão Europeia tentou desembaraçar com legislação. Dada a inviabilidade de os utilizadores manterem o controlo dos seus dados, a sua difusão e o subsequente uso assim que forem recolhidos, este direito pretende contrabalançar a falta de transparência no processamento de dados pessoais” (p.9).

Nesse sentido, o direito ao apagamento dos dados ou o direito a ser esquecido, encontra-se previsto no artigo 17.º do RGPD, traduzindo-se no direito do titular dos dados a que o responsável pelo tratamento proceda ao apagamento dos seus dados pessoais, sem demora injustificada, quando se verifique algum dos motivos do referido artigo 17.º, nomeadamente, quando os dados pessoais não forem mais necessários para a finalidade que motivou o seu recolha, quando o titular retire o seu consentimento e não existir outro fundamento jurídico para o tratamento, o titular opuser-se ao tratamento e não existam interesses legítimos que fundamentem o tratamento, o tratamento seja ilícito, o apagamento dos dados pessoais seja necessário para o cumprimento de uma obrigação jurídica decorrente do direito da União Europeia ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito, ou ainda quando os dados tenham sido recolhidos no contexto da oferta de serviços da sociedade da informação.

O novo direito ao esquecimento, *right to be forgotten,* em inglês, causou grande controvérsia[79] devido ao seu impacto nos modelos de negócio e no modo como os dados pessoais serão tratados ao abrigo do RGPD, assim como aos novos requisitos que impõe ao responsável pelo tratamento.

Todavia, o direito ao esquecimento não constitui um direito absoluto, devendo outros direitos ser salvaguardados, nomeadamente a liberdade de expressão e a investigação científica.[80]

Nestes termos, o número 3 do referido artigo estabelece que o titular dos dados pessoais não poderá lançar mão do direito ao esquecimento quando o tratamento dos dados pessoais se revele indispensável ao exercício da liberdade de expressão e de informação, ao cumprimento de uma obrigação legal decorrente do direito da União ou de um Estado-Membro, ao exercício de função de interesse público ou de autoridade pública de que esteja investido o responsável pelo tratamento, por motivos de interesse público no domínio da saúde pública, para fins de arquivo de interesse público, para fins de investigação científica ou histórica, assim como para fins estatísticos, sendo afastado o direito ao apagamento nas situações de efeitos de declaração, exercício ou defesa de um direito em um processo judicial.

O direito ao esquecimento concretiza um dos principais objetivos do RGPD, designadamente, assegurar um alto nível de proteção dos dados, dotando os titulares de dados pessoais de um poder efetivo sobre os seus próprios dados, reconhecendo o direito

[79] Neste sentido *vide* Santín (2017). The problem of the right to be forgotten from the perspective of self-regulation in journalism. *El Profesional De La Información*, 26(2), 303. doi: 10.3145/epi.2017.mar.17 e Bloomberg, "*The dangers and problem with the right to be forgotten on the internet*", *YoungPost,* 4 de outubro de 2018, *in* https://yp.scmp.com/over-to-you/op-ed/article/110660/dangers-and-problem-right-be-forgotten-internet, consultado a 28/09/2019.

[80]Comissão Europeia (2019). "Posso pedir a uma empresa que apague os meus dados pessoais?" Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-askcompany-delete-my-personal-data_pt, consultado a 3/04/2019.

ao controlo dos dados pessoais, à eliminação dos dados pessoais caso o titular assim o pretenda quando as finalidades pelas quais foram os dados recolhidos tenham sido atingidas.

O referido direito foi chamado à colação no acórdão do Tribunal de Justiça da União Europeia C-131/12, de 13 de maio de 2014[81], onde Mario Costeja González requeria que os seus dados fossem eliminados de páginas da La Vanguardia, assim como que a Google Spain ou Google Inc. eliminasse ou ocultasse os seus dados pessoais de modo a que os mesmos deixassem de constar nos resultados de pesquisa e nas ligações da La Vanguardia.

Por sua vez o TJUE considerou que "os artigos 12.°, alínea b), e 14.°, primeiro parágrafo, alínea a), da Diretiva 95/46 devem ser interpretados no sentido de que, no âmbito da apreciação das condições de aplicação destas disposições, importa designadamente examinar se a pessoa em causa tem o direito de a informação em questão sobre a sua pessoa deixe de ser associada ao seu nome através de uma lista de resultados exibida na sequência de uma pesquisa efetuada a partir do seu nome, sem que, todavia, a constatação desse direito pressuponha que a inclusão dessa informação nessa lista causa prejuízo a essa pessoa. Na medida em que esta pode, tendo em conta os seus direitos fundamentais nos termos dos artigos 7.° e 8.° da Carta dos Direitos Fundamentais da União Europeia, requerer que a informação em questão deixe de estar à disposição do grande público devido à sua inclusão nessa lista de resultados, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em aceder à referida informação numa pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso se se afigurar que, por razões

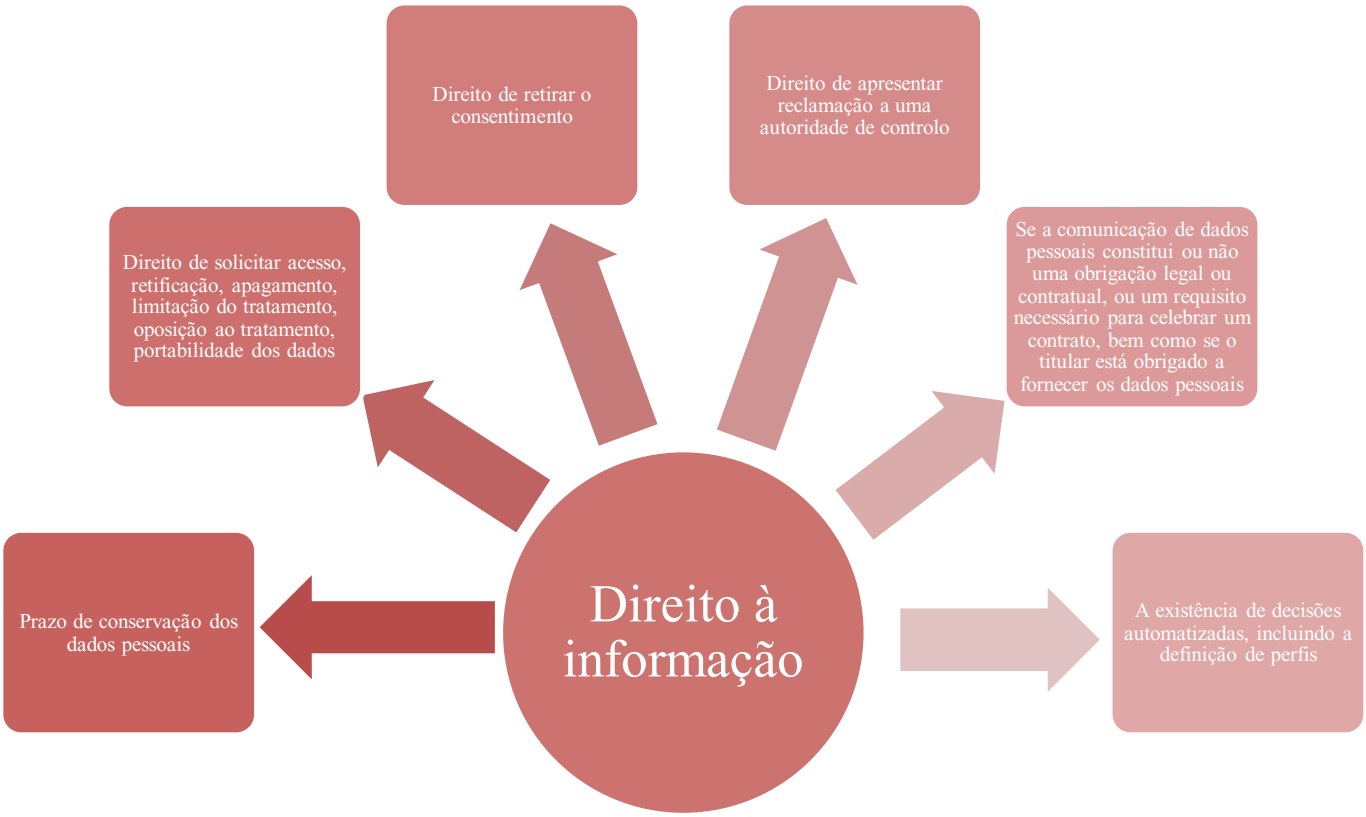
[81] Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT, consultado a 3/06/2019.

especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais ~~é~~ for justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão".

2.5.6 Direitos tradicionais

Um dos principais direitos do titular dos dados é o direito à informação, previsto nos artigos 10.º e 11.º da Diretiva 95/46/CE, encontrando-se consagrado nos artigos 13.º e 14.º do RGPD.

Figura 11 - Informações obrigatórias que decorrem do direito à informação



O considerando 61 do RGPD esclarece que "as informações sobre o tratamento de dados pessoais relativos ao titular dos dados deverão ser a este fornecidas no momento

da sua recolha junto do titular dos dados ou, se os dados pessoais tiverem sido obtidos a partir de outra fonte, dentro de um prazo ravoável".

Por sua vez, o artigo 13.º do RGPD refere as informações que o responsável pelo tratamento tem de facultar ao titular dos dados quando esses dados pessoais são recolhidos junto do titular, sendo que o tratamento transparente e equitativo dita que o titular dos dados seja informado de todos os tratamentos dos seus dados e das suas finalidades, assim como, a identidade do responsável pelo tratamento e os seus contacto, os contatos do encarregado de proteção de dados, a identidade dos destinatários dos dados e da existência ou não de uma decisão de adequadação adotada pela Comissão ou a referência às garantias adequadas e os meios de obter cópia das mesmas quando o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional[82].

O titular dos dados deve de igual modo ser informado de informações adcionais, nomeadamente, prazo de conservação, o direito a solicitar o acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, limitação do tratamento ou o direito de se opor ao tratamento, assim como o direito de apresentar reclamação a uma autoridade de controlo, se a comunicação dos dados constitui ou não uma obrigação legal ou contratual, a existência de decisões automatizadas, incluindo a definição de perfis.

Quando os dados pessoais não são recolhidos junto do titular, o responsável pelo tratamento deve comunicar ao titular dos dados as informações elencadas no artigo 14.º do RGPD, nomeadamente a identidade e os contactos do responsável pelo tratamento, os contactos do encarregado de proteção de dados, as finalidades do tratamento a que os

[82] Número 1 do artigo 13.º do RGPD.

dados pessoais se destinam, bem como o fundamento jurídico para o tratamento, as categorias dos dados pessoais em questão, os destinatários ou categorias de destinatários dos dados, assim como, a intenção de transferência de dados pessoais para um país terceiro ou uma organização internacional e a existência ou não de uma decisão de adequação adotada pela Comissão.

O direito do titular de dados pessoais de aceder aos seus dados pessoais tratados pelo responsável pelo tratamento encontrava-se previsto no artigo 12.º da Diretiva 95/46/CE, tendo sofrido diversas inovações aquando da sua transposição para o RGPD, tendo como corolário o "direito (do titular dos dados) a aceder aos dados pessoais recolhidos que lhe digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de conhecer e verficar a tomar conhecimento do tratamento e verificar a sua licitude"[83].

Nestes termos o artigo 15.º do RGPD prevê o direito do titular de dados de aceder aos seus dados pessoais e a ser informado das finalidades de tratamento dos seus dados, das categorias dos dados pessoais, da identidade dos destinatários dos dados pessoais, do prazo de conservação dos dados pessoais ou os critérios utilizados para fixar esse prazo, do seu direito a solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação e oposição ao tratamento de dados pessoais, o direito a ter acesso às informações disponíveis sobre a origem dos dados quando os mesmos não tenham sido recolhidos junto do titular, assim como, da lógica subjacente ao tratamento automático dos dados pessoais.

De igual modo, o titular dos dados tem o direito a ser informado das garantias adequadas relativas à transferência de dados pessoais para países terceiros[84].

[83] Considerando 63 do RGPD.
[84] Número 2 do artigo 15.º do RGPD.

Nestes termos, o titular dos dados tem o direito de aceder aos dados pessoais registados sobre si sem restrições, sem demoras ou custos excessivos, devendo exercer esse direito junto do responsável pelo tratamento dos dados.

Do direito ao acesso decorrem outros direitos do titular dos dados pessoais, nomeadamente, o direito de retificação, direito ao apagamento dos dados, assim como o direito à limitação do tratamento[85].

O direito de retificação[86] consiste na possibilidade do titular dos dados ordenar que os seus dados pessoais sejam atuais e exatos, e consequentemente, o direito de solicitar a retificação dos dados incorretos.

Por sua vez, o direito à limitação do tratamento apenas aplica-se quando o titular dos dados contestar a exatidão dos dados pessoais, o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e instar pela limitação da sua utilização, quando o responsável pelo tratamento já não necessitar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercío ou defesa de um direito em processo judiciaal ou quando o titular se tiver oposto ao tratamento e encontram-se em averiguação se os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

Nos termos do artigo 19.º do RGPD o responsável pelo tratamento deverá notificar os destinatários a quem os dados pessoais tenham sido transmitidos as retificações, o apagamento, as limitações de tratamento, excepto nas situações em que essa comunicação se demonstre inexequível ou acarrete um esforço desproporcionado.

---

[85] Artigo 18.º do RGPD.

[86] Artigo 16.º do RGPD: "O titular 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 pessoais tem o direito a que os seus dados pessoais incompletos sejam contemplados, incluindo por meio de uma declaração adicional".

O direito à oposição encontrava-se previsto no artigo 14.º da Diretiva 95/46/CE, sendo que o regulamento no seu artigo 22.º não introduziu grandes inovações, estabelecendo que o "titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.º n.º 1 alínea e), referente ao exercício de funções de interesse público ou de autoridade pública como fundamento de licitude do tratamento e alínea f), alusiva aos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros enquanto fundamento de licitude do tratamento, ou no artigo 6.º n.º 4[87], incluindo a definição de perfis com base nessas disposições", sendo que o tratamento deve ser findo, salvo quando o responsável pelo tratamento manifeste "razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para fins de declaração, exercício ou defesa de um direito num processo judicial".

O número 2 do artigo 21.º acrescenta que sempre que os dados sejam tratados para efeitos de comercialização direta, abrangendo a definição de perfis, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados que lhe digam respeito, acrescentando o n.º 3 que nessas situações os dados pessoais deixam de ser tratados para esse fim.

O titular dos dados deverá ser informado da hipótese de exercer o seu direito à oposição, devendo este direito ser apresentado de modo "claro e distinto de quaisquer

[87] Artigo 6.º número 4 do RGPD – "4 - Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º n.º 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:
a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º;
d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;
e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização."

outras informações"[88]. Assim, este direito deverá ser explicitamente levado à atenção do titular e apresentado de modo claro e distinto de quaisquer outras informações.

No que concerne ao direito de oposição a decisões individuais automatizadas[89], incluindo a definição de perfis[90], o artigo 22.º do RGPD convenciona que o "titular dos dados tem direito a 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", ou seja, o RGPD estabelece a repressão de tomadas de decisão, que produzam efeitos jurídicos ou originem danos, baseadas exclusivamente em sistemas automáticos, sem que exista qualquer intervenção humana, proibindo, também, a definição de perfis. Contudo, existem prerrogativas onde é permitida a tomada de decisões automatizadas, designadamente, quando o titular dos dados tenha dado o seu consentimento, seja necessário para a execução de um contrato ou nas situações em que as decisões automatizadas são autorizadas pelo direito da União Europeia ou do Estrado-Membro a que o responsável pelo tratamento está sujeito, e na qual estejam previstas de igual modo medidas adequadas a proteger os direitos, liberdades e garantias dos titulares dos dados.

No entanto o direito do titular dos dados a não ficar sujeito a decisões individuais automatizadas não se aplica às situações previstas no número 2 do artigo 22.º do referido regulamento, designadamente quando for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, o tratamento for

---

[88] Considerando 70 do RGPD.

[89] A Orientação sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679 do Grupo de Trabalho do artigo 29.º para a Proteção de Dados estabelece que "as decisões exclusivamente automatizadas correspondem à capacidade de tomar decisões através de meios tecnológicos e sem intervenção humana. As decisões automatizadas podem basear-se em qualquer tipo de dados, como, por exemplo: dados fornecidos diretamente pelas pessoas em causa (tais como respostas a um questionário); dados observados acerca das pessoas (tais como dados de localização recolhidos por meio de uma aplicação); dados obtidos ou inferidos, tais como um perfil da pessoa que já tenha sido criado (p. ex., uma pontuação de crédito)". Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp251rev01_pt.pdf, consultado a 20/07/2019.

[90] O artigo 4.º número 4 do RGPD define como definição de perfis tratamentos automatizados de dados pessoais que consistam em empregar esses dados pessoais para estimar determinados aspetos pessoais de uma pessoa singular, "nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações".

baseado no consentimento explícito do titular dos dados ou ainda quando a decisão tiver sido autorizada pelo direito da União Europeia ou do Estado-Membro a que o responsável pelo tratamento se encontra sujeito e na qual estejam previstas medidas adequadas para salvaguardar os direitos, liberdades e legítimos interesses do titular dos dados pessoais, sendo que no âmbito deste direito verifica-se que o RGPD manteve a mesma linha de pensamento do que a Diretiva, não introduzindo alterações significativas.

Em suma, de modo a reforçar efetivamente a proteção dos dados pessoais dos titulares dos dados pessoais o RGPD consagrou novos direitos, sendo que o legislador não se limitou a reforçar as obrigações de informação a que o responsável pelo tratamento se encontra adstrito, consagrando novos direitos e alargando o âmbito de direitos anteriormente consagrados na Diretiva, como o direito à portabilidade dos dados e o direito ao esquecimento.

Assim, de modo a que os direitos do titular dos dados sejam acautelados os responsáveis pelos dados devem identificar e analisar as suas novas obrigações e implentar procedimentos internos eficazes para responder às solicitações dos titulares dos dados no que concerne ao exercícios de direitos, sendo que a ausência de resposta às solicitações do titular dos dados poderá levar à aplicação de coimas nos termos do RGPD.

2.5.7 Âmbito de aplicação territorial

No que concerne ao âmbito de aplicação territorial, enquanto a Diretiva atribuia enfâse no local onde os dados pessoais eram tratados, para o RGPD releva o local onde o titular dos dados pessoais se encontra. Assim, com o RGPD verificou-se um aumento do escopo de aplicação tanto a nível material como geograficamente, afetando diversas entidades estebelecidas dentro e fora do território da União Europeia.

A Diretiva 95/46/EU consagrava no seu artigo 4.º o âmbito de aplicação territorial, estipulando a aplicabilidade da diretiva a operadores comerciais sediados em países terceiros em determinadas situações, estabelecendo que "cada Estado-Membro aplicará as suas disposições nacionais adotadas por força da presente diretiva ao tratamento de dados pessoais quando: a) o tratamento for efetuado no contexto das atividade de um estabelecimento do responsável pelo tratamento situado no território desse Estado-Membro", acrescentado na sua alínea b) aplicação da diretiva a responsáveis pelo tratamento não estabelecidos no território da União Europeia por força do direito internacional público e nas situações em que o responsável pelo tratamento não estiver estabelecido no território da União e recorrer a meios, automatizados ou não, situados no território desse Estado-Membro, exceto se esses meios somente forem empregues para trânsito no território da União Europeia.

Não obstante, anteriormente à entrada em vigor do RGPD, as questões relacionadas com a aplicação territorial do regime da proteção de dados instituído pela União Europeia foram debatidas e abordadas no acórdão do Tribunal de Justiça da União Europeia, de 13 de maio de 2014, usualmente designada pela decisão *Google Spain*[91], onde foi definido que a Diretiva 95/46/CE aplicava-se a uma empresa sediada nos Estados Unidos da América, nomeadamente, à *Google Inc.*.

Por sua vez, o RGPD adotou uma posição acertiva no que concerne à definição do âmbito de aplicação territorial, acabando com as eventuais dificuldades interpretativas de aplicação do quadro normativo da União Europeia no que concerne aos dados pessoais, consagrando a sua aplicação "ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um

[91] Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT, consultado a 20/06/2019.

subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União"[92], sendo que o RGPD aplica-se de igual modo ao "tratamento efetuado por um responsável pelo tratamento ou subcontratante não estabelecido no território da União Europeia, quando as atividades de tratamento estejam relacionadas com: a) oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;[93] b) o controlo do seu comportamento[94], desde que esse comportamento tenha lugar na União"[95], aplicando de igual modo a tratamentos de dados pessoais por um responsável pelo tratamento não estabelecido na União Europeia, mas num lugar em que se aplique o direito de um Estado-Membro.

Por outros palavras, qualquer organização, independemente de onde esteja sediada, poderá estar sujeita ao RGPD se fornecer serviços a titulares de dados que se encontram na União Europeia. Assim, de forma prática é possível afirmar que o focos do âmbito de aplicação territorial do RGPD encontra-se na localização do titular dos dados e não do responsável pelo tratamento ou do subcontratante.

Por sua vez, a redação originária do Regulamento, nomeadamente, do número 2 do artigo 3.º gerou algumas divergências linguísticas, sendo que *ab initio* estabelecia que o regulamento aplicava-se ao tratamento de dados pessoais de titulares residentes no território da União Europeia. Todavia, o Conselho de Europa publicou uma retificação[96] do RGPD que resolveu a questão, passando a estabelecer que o regulamento "aplica-se

[92] Número 1 do artigo 3.º do Regulamento Geral de Proteção de Dados.
[93] Nos termos do considerando 23 do RGPD há que determinar em que medida é evidente a intenção do responsável pelo tratamento ou subcontratante de oferecer serviços a titulares de dados em um ou mais Estados-Membros para se apurar se os mesmos oferecem serviços aos titulares de dados que se encontrem na União Europeia.
[94] O considerando 23 do RGPD define o controlo do comportamento como seguir na internet determinadas pessoas 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".
[95] Número 2 do artigo 3.º do Regulamento Geral de Proteção de Dados.
[96] Disponível em: http://www.sg.pcm.gov.pt/media/33583/01pdf_dados.pdf, consultado a 2/03/2019.

ao tratamento de dados pessoais de titulares que se encontrem no território da União", dissipando eventuais dúvidas sobre a pertinência do local de residência do titular dos dados para a aplicação do RGPD.

O novo âmbito de aplicação territorial constitui uma das mais importantes inovações do RGPD, permitindo que se alcance um tratamento de dados, a nível internacional, mais harmoniozo por parte dos responsáveis pelo tratamento sediados fora ou dentro da União Europeia, permitindo-se assim o mesmo nível de segurança dos dados pessoais no que concerne à utilização de sites, nomeadamente, Google, Facebook, Amazon e aplicações geridas por grandes multinacionais que operam no território europeu. Assim, o RGPD compõe uma autêntica arma ao dispor dos cidadãos europeus na defesa dos seus direitos, protegendo-se cada vez mais o cidadão europeu contra tratamentos ilegítimos dos seus dados pessoais.

2.5.8 Transferência de dados pessoais para países terceiros

Considerando que as transferências de dados pessoais constitui um elemento essencial das relações transatlânticas, em que cada vez mais as transferências de dados constituem parte integrante das trocas comerciais, o RGPD veio reforçar as regras relativas à transferência de dados pessoais para países terceiros (Comissão Europeia, 2015, p.2).

Segundo a própria Comissão Europeia "no mundo globalizado de hoje, existem grandes quantidades de transferências transfronteiriças de dados pessoais, que, por vezes, são armazenados em servidores situados em vários países diferentes. A proteção concedido pelo RGPD viaja com os dados, o que significa que as regras que protegem os dados pessoais continuam a aplicar-se independentemente da localização dos dados. Tal

aplica-se também quando os dados são transferidos para um país que não seja membro da UE (país terceiro)"[97].

No que concerne à transferência de dados para países terceiros, a Diretiva reconhecia no seu considerando 56 que os fluxos transfronteiras de dados pessoais são necessários ao desenvolvimento do comércio internacional, contudo, estebelecia no seu artigo 25.º que tais transferências de dados pessoais para países terceiros só podiam ocorrer se esses países assegurassem um nível de proteção adequado. Por sua vez, o considerando 57 da referida diretiva determinava que as transferências de dados pessoais para países que não ofereçam um nível de proteção adequado devia ser proíbida, acrescentando o considerando 60 que as transferências só podiam ser realizadas no pleno respeito das disposições adotadas pelos Estados-Membros nos termos da diretiva.

Resulta do artigo 25.º da referida diretiva que a adequação do nível de proteção era avaliado em função das circunstâncias em torno da transferência dos dados pessoais, sendo que o artigo 25.º imponha um conjunto de obrigações aos Estados-membros e à Comissão, nomeadamente no que concerne à confirmação se um país terceiros assegura um nível de proteção adequado.

Conquanto o regulamento consagra a proibição geral de enviar dados pessoais para países fora do Espaço Económico Europeu[98] que não garanta a proteção adequada, estabelecendo no seu artigo 44.º que qualquer transferência de dados pessoais para um país terceiro ou organização internacional só é realizada se as condições estabelecidas no capítulo V do RGPD forem cumpridas pelo responsável pelo tratamento e pelo

[97] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pt, consultado a 20/09/2019.
[98] O Espaço Económico Europeu é constituído pelos 28 Estados-Membros da União Europeia, Islândia, Noruega e Liechtenstein.

subcontratante, devendo ser assegurado que "não é comprometido o nível de proteção das pessoas singulares" assegurado na União Europeia pelo RGPD.

De igual modo ao estabelecido na Diretiva, o artigo 45.º do RGPD institui que podem ser realizadas transferências de dados pessoais para países terceiros ou organizações internacionais se a Comissão tiver decidido que é assegurado um nível de proteção adequado de proteção dos direitos fundamentais dos titulares de dados pessoais por parte do país terceiro ou da organização internacional.

Os países que a Comissão Europeia considera, até ao presente, que garantem proteção adequada são "empresas norte-americanas que se enquadrem no autocertificação do Escudo de Privacidade UE-EUA, Andorra, Argentina, Canadá (limitado ao PIPEDA – Lei de Proteção de Informações Pessoais e Documentos Eletrónicos do Canadá), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça, Uruguai e Japão" (Francisco, D., & Francisco, S., 2019, p.35).

Segundo Martins (2019) "o critério de adequação, subjacente a uma decisão, não exige que o sistema de proteção de dados do país terceiro seja idêntico ao da União Europeia. O objetivo não é imitar ponto por ponto a legislação europeia, mas sim estabelecer um «standard de equivalência essencial», o que pressupõe uma prévia avaliação global do sistema de proteção de dados pessoais do país terceiro, em particular ao nível das garantias de proteção aplicáveis e mecanismos de supervisão e reparações disponíveis" (p.1).

A Comissão pode determinar que um país terceiro, um território ou um sector determinado de um país terceiro, ou uma organização internacional garante um nível de proteção adequado, acautelando a segurança jurídica e a uniformidade ao nível da União Europeia relativamente a essas entidades que sejam consideradas adequadas a assegurar

tal nível de proteção, acrescenta o considerando 104 do RGPD que "em conformidade com os valores fundamentais em que a União assenta, particularmente que a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou sector específico de um país terceiro, ter me consideração em que medida esse país respeita o primado do Estado de direito, o acesso à justiça e as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. A adoção de uma decisão de adequação relativamente a um território ou um sector específico num país terceiro deverá ter em conta critérios claros e objetivos, pais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro. Este deverá dar garantias para assegurar um nível adequado de proteção essencialmente equivalente ao assegurado na União, nomeadamente quando os dados pessoais são tratatados num ou mais sectores específicos. Em especial, o país terceiro deverá garantir o controlo efetivo e independentente da proteção dos dados, assim como estabelecer regras de cooperação com as autoridades de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial".

Não obstante, a Comissão pode considerar que um país terceiro ou organização internacional deixou de assegurar um nível adequado de proteção de dados, devendo nesses casos ser vedada a transferência de dados pessoais, excpeto quando forem acautelados os requisitos do RGPD para transferências sujeitas a garantias adequadas ao titular de dados nos termos do artigo 46.º[99] do referido regulamento, sendo que tal situação

[99] Artigo 46.º do RGPD: "Transferências sujeitas a garantias adequadas. 1 - Não tendo sido tomada qualquer decisão nos termos do artigo 45.º, n.º 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes. 2. Podem ser previstas as garantias adequadas referidas no n.º 1, sem requerer

deverá igualmente ser extensível perante uma falta de decisão sobre o nível de proteção adequado num país terceiro.

Por outro lado, nos termos do artigo 49.º do RGPD, mesmo na ausência de uma decisão de adequação ou de garantias adequadas a transferência de dados pessoais para países terceiros ou organizações internacionais é permitida, nomeadamente, quando o titular dos dados tiver prestado o seu consentimento, a tranferência for necessária à execução de um contrato, por razões de interesse público, necessária à declaração, ao exercício ou à defesa de um direito em processo judicial, para proteção de interesses vitais do titular dos dados ou de terceiros, se estes estiverem física ou legalmente incapazes de dar o seu consentimento, ou quando a transferência é realizada a partir de um registo que se destine a informar o público ou qualquer pessoa que possa provar nela ter um interesse legítimo, desde que as condições de consulta instituídas no direito da União Europeia se encontrem preenchidas no caso concreto.

Nestes termos, deverão as entidades que realizam transferências de dados pessoais atentar aos seus protocolos de transferências de dados com entidades em países que não garantam uma proteção adequada, na medida em que a transferência de dados para países que não garantam a proteção adequada constitui uma violação do RGPD, assim deverão

---

nenhuma autorização específica de uma autoridade de controlo, por meio de: a) Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos; b) Regras vinculativas aplicáveis às empresas em conformidade com o artigo 47.º; c) Cláusulas-tipo de proteção de dados adotadas pela Comissão pelo procedimento de exame referido no artigo 93.º, n.º 2; d) Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão pelo procedimento de exame referido no artigo 93.º, n.º 2; e) Um código de conduta, aprovado nos termos do artigo 40.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados; ou f) Um procedimento de certificação, aprovado nos termos do artigo 42.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados. 3. Sob reserva de autorização da autoridade de controlo competente, podem também ser previstas as garantias adequadas referidas no n.º 1, nomeadamente por meio de: a) Cláusulas contratuais entre os responsáveis pelo tratamento ou subcontratantes e os responsáveis pelo tratamento, subcontratantes ou destinatários dos dados pessoais no país terceiro ou organização internacional; ou b) Disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados. 4. A autoridade de controlo aplica o procedimento de controlo da coerência a que se refere o artigo 63.º nos casos enunciados no n.º 3 do presente artigo. 5. As autorizações concedidas por um Estado-Membro ou uma autoridade de controlo com base no artigo 26.º, n.º 2, da Diretiva 95/46/CE continuam válidas até que a mesma autoridade de controlo as altere, substitua ou revogue, caso seja necessário. As decisões adotadas pela Comissão com base no artigo 26.º, n.º 4, da Diretiva 95/46/CE permanecem em vigor até que sejam alteradas, substituídas ou revogadas, caso seja necessário, por uma decisão da Comissão adotada em conformidade com o n.º 2 do presente artigo."

as organizações identificar, avaliar e dissecar os fluxos transfronteiriços de dados que levam a cabo e na ausência de uma falta de decisão de adequação, tomar as medidas necessárias para colmatar a falta da proteção de dados no país terceiro, de modo a caucionar garantias adequadas aos titulares dos dados.

2.5.9 Encarregado de proteção de dados

O encarregado de proteção de dados surge no RGPD como uma figura essencial, todavia diversas dúvidas surgiram em torno desta figura, nomeadamente em que situações deverá ser nomeado, quais as suas funções, qual o perfil do EPD, assim como a obrigatoriedade ou não de certifiação destes profissionais[100].

A Diretiva 95/46/CE nos seus considerando 49 e 54, assim como no seu artigo 18.º, previa a figura do encarregado de proteção de dados, associado ao controlo prévio ao tratamento de dados e à obrigação de notificação à autoridade de controlo anterior ao tratamento, total ou parcialmente automatizado, destinado à prossecução de uma ou mais finalidades interligadas, dispondo o n.º 2 do referido artigo que os Estados-Membros encontravam-se isentos da notificação ou que poderiam estabelecer a simplificação da referida notificação quando o responsável pelo tratamento nomear, nos termos do direito nacional a que está sujeito, um encarregado de proteção de dados.

Embora a Diretiva não obrigasse a nomeação de um EPD, a nomeação de um EPD começou a desenvolver-se em diversos Estados-Membros[101].

Em Portugal, a LPDP não consagrava a figura do encarregado de proteção de dados.

---

[100] Neste sentido, Green, A.: "*GDPR: Do You Have to Hire a DPO?", Varonis*, 22 de março de 2018, in https://www.varonis.com/blog/eu-gdpr-spotlight-do-you-have-to-hire-a-dpo/, consultado a 29/09/2010; Nowak, J. "*Top 10 Questions About Data Protection Officer", SGS, GPDR Online,* 9 de abril de 2019, in https://gdpr.sgs.com/s/article/TOP-10-QUESTIONS-ABOUT-DATA-PROTECTION-OFFICER?language=en_US, consultado a 29/09/2019.

[101] É o exemplo da Alemanha (Cfr. Kirkby, J.: "*A intrigante figura do encarregado de proteção de dados", Bas, disponível em:* https://www.bas.pt/comunicacao/noticias/a-intrigante-figura-do-encarregado-de-protecao-de-dados/, consultado a 27/09/2019).

Tendo tudo isto presente e incidindo sobre o atual quadro legal, o RGPD consagra que o responsável pelo tratamento obrigatoriamente deverá designar um encarregado de proteção de dados, em inglês *Data Processor Officer* (DPO), sempre que o tratamento de dados pessoais for efetuado por um autoridade pública, excetuando os tribunais ou autoridades judiciais independentes no exercício da sua função jurisdicional, sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que exijam um controlo regular e sistemático dos titulares dos dados em grande escala ou sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados pessoais ou de dados pessoais relacionados com condenações penais e infrações[102], sendo os responsável pelo tratamento, subcontratantes e as associações que não se encontrem obrigados a designar um DPO poderão optar por nomear um.

Considerando que o RGPD consagrou as situações em que a designação de um encarregado de proteção de dados mas não densificou os conceitos que utilizou, o GT29 emitiu orientações sobre a interpretação dos conceitos do RGPD. Assim, o GT29 estabeleceu que para determinar se um tratamento de dados é efetuado em grande escala deverá atentar-se ao "número de titulares de dados afetados – como número concreto ou em percentagem da população em causa; o volume de dados e/ou o alcance dos diferentes elementos de dados objeto de tratamento; a duração, ou permanência, da atividade de tratamento de dados; o âmbito geográfico da atividade de tratamento" (GT29, 2016, p.24).

De igual modo, o GT29 (2016) estabeleceu o significado de atividades principais como "as operações essenciais para alcançar os objetivos do responsável pelo tratamento

[102] Artigo 37.º e considerando 97 do RGPD.

ou do subcontratante, as quais incluem também todas as atividades em que o tratamento de dados constitui parte indissociável das atividades do responsável pelo tratamento ou do subcontratnte" (p.23).

Por sua vez, o GT29 (2016) definiu o controlo regular e sistemático como "contínuo ou que ocorre em intervalos específicos num determinado período, recorrente ou repetido em horários estipulados, constante ou periódico", que "ocorre de acordo com um sistema, predefinido, organizado ou metódico, realizado no âmbito de um plano geral de recolha de dados, efetuado no âmbito de uma estratégia" (p.10).

Sempre se refira que poderá ser designado um único EPD para um grupo empresarial ou quando o responsável pelo tratamento ou o subcontratante for um organismo público, abordando-se no capítulo seguinte tal opção.

Por sua vez, o EPD deverá ser designado "com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no dominío do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39.º"[103], podendo o EPD ser um elemento do responsável pelo tratamento ou exercer as suas funções mediante um contrato de prestação de serviços[104].

O GT29 (2016) esclareceu o âmbito das qualidades profissionais que o EPD deverá ter, estabelecendo que "as competências e conhecimentos especializados pertinentes incluem: competências no domínio das normas e práticas de proteção de dados nacionais e europeias, incluindo um conhecimento profundo do RGPD; conhecimento das operações de tratamento efetuadas; conhecimento das tecnologias da informação e da segurança dos dados; conhecimento do setor empresarial e da organização; capacidade

[103] Número 5 do artigo 37.º do RGPD.
[104] Número 6 do artigo 37.º do RGPD.

para promover uma cultura de proteção de dados no seio da organização" (p.26). Assim, aquando da nomeação de um EPD deverá ser escolhido um candidato que possua as competências acima elencadas.

O desempenho das funções do EPD deverá ser pautada por total indepedência, sendo que nos termos do número 3 do artigo 38.º o responsável pelo tratamento e o subcontratante asseguram que o EPD "não recebe instruções relativamente ao exercício das suas funções", não podendo "ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções", informando "diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante", sempre se refira que a responsabilidade pelo tratamento é do responsável pelo tratamento, não se confundindo como responsabilidade do EPD.

O EPD deverá ser envolvido, de forma adequada e em tempo útil em todas as questões relacionadas com a proteção de dados pessoais, sendo que os titulares dos dados podem contatar o EPD sobre todas as questões relacionadas com o tratamento dos seus dados pessoais e exercício dos seus direitos.

O EPD têm a função de informar e aconselhar o responsável pelo tratamento ou o subcontratante das obrigações decorrentes do RGPD e demais disposições do direito da União ou dos Estados-Membros na matéria, controlar a conformidade com o RGPD "incluíndo a repartição de responsablidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes"[105], controlar e prestar aconselhamento no que concerne à avaliação de impacto sobre a

[105] Alínea b) do número 1 do artigo 39.º do RGPD.

proteção de dados, cooperar com a autoridade de controlo, assim como servir de ponto de contato com a autoridade de controlo e o responsável pelo tratamento.

Figura 12 - Funções do Encarregado de Proteção de dados

Os dados do EPD deverão ser publicados pelo responável pelo tratamento, de modo a facilitar a comunicação dos titulares dos dados com este. De igual modo, o responsável pelo tratamento deverá comunicar os dados do EPD à autoridade de controlo[106].

No que concerne à certificação dos EPD, embora seja possível averiguar a promoção de cursos de certificação de EPD, a realidade é que o RGPD no seu número 5 do artigo 37.º não exige a certificação para o exercício das funções inerentes ao EPD, sendo que o número 1 do artigo 9.º da Lei n.º 58/2019, de 8 de agosto dispõe no mesmo sentido.

Neste sentido, o artigo 43.º do RGPD, com a epigráfe "Organismos de certificação", estipula que os organismos de certificação "que tenham um nível adequado de

[106] *Cfr.* Número 7 do artigo 37.º do RGPD.

competência em matéria de proteção de dados" têm poderes para emitir e renovar a certificação, sendo que estes organismos de certificação deverão ser acreditados pela autoridade de controlo e pelo organismo nacional de acreditação, no contexto nacional, pelo Instituto Português de Acreditação (IPAC)[107], sendo que até à data não foi acreditado nenhum organismo de certificação.

Considerando que o RGPD exige que o EPD tenha um conhecimento especializados no domínio do direito e das boas práticas de proteção de dados, a certificação poderá ser uma forma de garantir a qualificação profissional do EPD para o exercicio das funções que lhe cometidas pelo artigo 39.º do RGPD, assim como forma de garantir um nível de competência miníma dos profissionais. Neste sentido, Lachaud (2018) esclareceu que "a certificação do EPD oferece duas notáveis contribuições teóricas (…). Por um lado, a certificação do EPD teoricamente contribui para a precisão e consistência da implementação do RGPD. A certificação contribui para simplificar, para padronizar, o perfil do EPD na medida em que aplica requisitos e processos semelhantes aos candidatos. A certificação teoricamente oferece um nível mais elevado de padronização, na medida em que regularmente verifica a aplicação completa e precisa dos requisitos sem os quais a certificação poderia ser retirada. Portanto, a certificação do EPD oferece a longo prazo um instrumento de otimização do perfil do EPD e, consequentemente, deve contribuir para a otimização da proteção de dados a longo prazo. Por outro lado, o padrão usado no processo de certificação operacionaliza a lei. Traduz as disposições legais em leis aplicáveis e requisitos verificáveis" (pp.12-13).

[107] O artigo 14.º da Lei n.º 58/2019, de 8 de agosto estipula no seu número 1 que "a autoridade competente para a acreditação dos organismos de certificação em matéria de proteção de dados é o IPAC, I.P.", acrescentando no seu número 3 que "a certificação, bem como a emissão de selos e marcas de proteção de dados, é efetuada por organismos de certificação acreditados nos termos do n.º 1, destinando-se a atestar que os procedimentos implementados cumprem o disposto no RGPD e na presente lei".

Embora o RGPD seja bem claro quanto ao facto de os EPD não serem pessoalmente responsáveis em caso de incumprimento do RGPD, estabelecendo que essa responsabilidade é imputada ao responsável pelo tratamento e subcontratantes, considerando que o RGPD estabelece um quadro de autoregulação e de crescente responsabilidade dos responsáveis pelo tratamento e respetivos subcontratantes pelo cumprimento da legislação de proteção de dados, os encarregados de proteção de dados assumem um papel central no cumprimento das disposições do RGPD, sendo que a nomeação de um EPD, conhecedor do RGPD, facilitará o cumprimento das disposições do RGPD, assim como, facilita a comunicação entre as partes interessadas, designadamente, autoridade de controlo e os titulares de dados.

O EPD deverá ser envolvido desde o início no processo de implementação do RGPD no seio da organização e em todos os assuntos relacionados com a proteção de dados. O próprio RGPD prevê explicitamente o envolvimento do EPD no que concerne às avaliações de impacto, estabelecendo que o responsável pelo tratamento deverá aconselhar-se com o EPD ao realização a referida avaliação[108].

2.5.10 *Accountability* – responsabilidade proativa e autorregulação

Com o RGPD verifica-se um diferente nível de responsabilização, na medida em que na aceção da Diretiva apenas aos responsáveis pelo tratamento[109] poderia ser imputado o incumprimento, neste sentido é de apontar o artigo 23.º da Diretiva. Por sua vez, o RGPD no seu capítulo IV, com a epígrafe "Responsável pelo tratamento e subcontratante", estabelece o regime obrigacional aplicável aos responsáveis pelo tratamento e aos

[108] *Cfr.* Número 2 do artigo 35.º do RGPD.
[109] Nos termos do número 7 do artigo 4.º do RGPD responsável pelo tratamento é 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; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro".

subcontratantes[110], sendo que o artigo 24.º do RGPD estabelece que o responsável pelo tratamento deverá adotar as medidas técnicas e organizativas adequadas de modo a assegurar e poder comprovar a conformidade do tratamento efetuado com o RGPD.

A Diretiva 95/46/CE estabelecia um regime de heterorregulação entre o responsável pelo tratamento e a entidade reguladora, consagrando uma obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo[111], assim como, controlo prévio dos tratamentos que pudessem representar um risco para os direitos e liberdades dos indíviduos, pareceres apresentados ou solicitados por parte do responsável pelo tratamento.

Nestes termos, ao abrigo do quadro legal anterior em matéria de proteção de dados, em Portugal, a Comissão Nacional de Proteção de Dados supervisionava o tratamento de dados, emitindo autorizações para o tratamento de dados sensíveis.

Por sua vez, o RGPD sustenta um modelo de autorregulação por parte dos responsáveis pelo tratamento, estabelecendo novos modelos de demonstração de responsabilidades, novas obrigações de avaliação de impacto, obrigações de notificações de violações, assim como um novo modelo sancionatório, sendo que ao abrigo deste novo regime autoregulatório a autoridade de controlo deixa de realizar os controlos prévio através de emissão de autorizações para o tratamento, sendo estas substituídas pelo dever de cada responsável pelo tratamento adota procedimentos internos que demonstrem que se encontra em conformidade com o regulamento, sendo o registo das atividades de tratamento uma obrigação suplementar.

---

[110] Na aceção do número 8 do artigo 4.º do RGPD 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", nesta medida, o subcontratante não determina as finalidades e os meios de tratamento dos dados pessoais, sendo que se o fizer é considerado responsável pelo tratamento no que respeita ao tratamento em questão.

[111] Artigo 18.º da Diretiva 95/46/CE.

Para Crabtree *et al.* (2018) a responsabilidade "exige que qualquer organização que controle o tratamento de dados implemente políticas, procedimentos e sistemas para demonstrar a si mesmo que as suas operações de tratamento estão em conformidade com os requisitos da regulamentação da proteção de dados. Esse foco interno é enfatizado pelas diretrizes de proteção de dados e pode ser fornecida através de ferramentas como as avaliações de impacto. Menos pronunciada à primeira vista, embora igualmente importante, é a dimensão externa da responsabilidade, que exige que a organização demonstre a outras pessoas, particularmente autoridades de controlo e indivíduos, que as suas operações de tratamento de dados estão em conformidade com o RGPD" (pp.39-45).

Assim, de modo a demonstrar o cumprimento das obrigações do responsável pelo tratamento, este poderá socorrer-se de códigos de conduta aprovados nos termos do artigo 40.º do RGPD ou de procedimentos de certificação aprovados nos termos do artigo 42.º do referido diploma, assim como do registo das atividades de tratamento.

Neste sentido o responsável pelo tratamento e os subcontratantes devem preservar um registo escrito, incluindo em formato eletrónico, das atividades de tratamento sob a sua responsabilidade, quando as suas organizações tiverem mais de 250 trabalhadores, quando o tratamento efetuado seja suscetível de causar riscos aos direitos e liberdades do titular dos dados, não seja ocasional ou abranja categorias especiais de dados ou dados relativos a condenações penais e infrações. Desse registo deve constar o nome e os contactos do responsável pelo tratamento e do encarregado de proteção de dados, as finalidades do tratamento dos dados pessoais, a descrição das categorias de titulares de dados e das categorias de dados pessoais, categorias de destinatários a quem os dados pessoais são divulgados, as transferências de dados para países terceiros ou organizações internacionais, os prazos de conservação, assim como as medidas técnicas e organizativas

no domínio da segurança[112]. O registo de atividades deverá ser disponibilizado à autoridade de controlo quando esta o solicitar.

Concomitantemente, o RGPD reforçou o conceito de proteção de dados desde a conceção e por defeito (*privacy by design and by default*), estipulando no seu artigo 25.º que as empresas devem adotar medidas técnicas e organizativas desde o momento tanto de definição dos meios de tratamento como no momento do próprio tratamento de modo a salvaguardar os princípios da proteção de dados desde o início (desde a conceção).

Cavoukian (2011) definiu a *privacy by design* como "caracterizada por medidas proativas e não reativas. Antecipa e previne eventos de invasão de privacidade antes que eles aconteçam. A PhB não espera que os riscos de privacidade se materializem, nem oferece soluções para a resolução de infrações de privacidade após ocorrerem. Em resumo, PbD vem antes de facto e não depois. (…) A PbD procura oferecer o maior grau de privacidade, garantindo que os dados pessoais são protegidos automaticamente em qualquer sistema de IT ou prática empresarial. Se o indíviduo nada fizer, a sua privacidade premanece intacta. Nenhuma ação é necessária por parte do indíviduo para proteger a sua privacidade" (p.2).

No que concerne à proteção por defeito, o responsável pelo tratamento deverá aplicar medidas técnicas e organizativas que certifiquem que só são tratados os dados pessoais necessários para cada finalidade de tratamento, devendo o tratamento ser limitado às finalidades estabelecidas e cumprido o prazo de conservação, assim como, a limitação da acessibilidade aos dados pessoais. Exemplo dessas medidas são especificar as finalidades de tratamento, ou seja, os objetos para os quais os dados pessoais são recolhidos, usados e conservados, comunicando ao titular dos dados tais finalidades, minimização dos dados,

[112] Artigo 30.º do RGPD.

devendo só ser recolhidos ser os dados pessoais estritamente necessários às finalidades de tratamento devidamente especificadas.

Esclarecendo o considerando 78 do RGPD "para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os procípios da proteção de dados desde a conceção e da proteção de dados por defeito. Tais medidas podem incluir a minimização do tratamento de dados pessoais, a pseudonomização de dados o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança".

2.5.11 Avaliação de impacto sobre a proteção de dados e consulta prévia

A avaliação de impacto sobre a proteção de dados[113] encontra-se consagrada no artigo 35.º do RGPD, assim como no artigo 27.º da Diretiva 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril, relativa à proteção de 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.

Bieker *et al.* (2016) definiram a AIPD como "um instrumento para identificar e analisar riscos para os indivíduos, que existem devido ao uso de uma determinada tecnologia ou sistema por uma organização nos seus vários papéis (como cidadãos, clientes, pacientes etc)" (pp.2 e 3).

[113] Doravante designada por AIPD.

O GT29 (2017) descreveu a AIPD como um processo que visa "estabelecer e demonstrar conformidade", constituindo "um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos" (p.4), acrescentando que compõem um instrumento de responsabilização, na medida em que permite ao responsável pelo tratamento demonstrar que foram tomadas as medidas adequadas para assegurar a conformidade com o RGPD.

Por sua vez, o considerando 84 do RGPD clarificou o seu sentido, estabelecendo que "nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento".

Na aceção de Houser & Voss (2018) com a avaliação de impacto "a ideia é que as salvaguardas apropriadas possam ser instituídas quando forem descobertas deficiências. Em vez de esperar que os individuos avaliem os riscos ao partilharem os seus dados pessoais, o fardo é colocado no responsável no tratamento" (p.55).

Por conseguinte, nos termos do número 1 do artigo 35.º do RGPD, a avaliação de impacto sobre a proteção de dados deverá ocorrer, antes de iniciar o tratamento, quando o responsável pelo tratamento efetue tratamentos que utilizem novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, forem suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares.

Nestes termos, não é obrigatório efectuar uma AIPD para todas as operações de tratamento, sendo que esta só é obrigatória quando o tratamento for susceptível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, perante situações de avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, que desencadeiam a adoção de decisões que produzam efeitos jurídicos relativamente à pessoa singular ou que a afetam significativamente de forma similar, de operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais referentes a condenações penais e infrações, assim como, em situações do controlo sistemático de zonas acessíveis ao público em grande escala[114].

Não obstante, o RGPD atribuiu à autoridade de controlo o poder de elaborar uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto sobre a proteção de dados[115], assim como estipulou que a AIPD fica exceptuada nas situações em que o tratamento é efetuado para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito ou for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, tendo "por fundamento jurídico o direito da União ou do Estado-Membro a que o responsável pelo tratamento está sujeito, e esse

[114] Número 3 do artigo 35.º do RGPD.
[115] Número 5 do artigo 35.º do RGPD.

direito regular a operação ou as operações de tratamento específicas em questão, e se já tiver sido realizada uma avaliação de impacto sobre a proteção de dados no âmbito de uma avaliação de impacto geral no contexto da adoção desse fundamento jurídico", excepto se os Estados-Membros considerarem imprescindível proceder a essa avaliação antes das atividades de tratamento.

O número 4 do artigo 35.º do RGPD estabelece que a autoridade de controlo deverá elaborar uma lista das operações de tratamento sujeitos à AIPD. Neste sentido, em Portugal a Comissão Nacional de Proteção de Dados publicou o Regulamento 1/2018, relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados, elencando 9 operações de tratamento que carecem de AIPD, nomeadamente, "tratamento de informação decorrente da utilização de dispositivos eletrónicos que transmitam, por redes de comunicação, dados pessoais relativos à saúde; interconexão de dados pessoais ou tratamento que relacione dados pessoais previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal; tratamento de dados previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal com base em recolha indireta dos mesmos, quando não seja possível ou exequível assegurar o direito de informação nos termos da alínea b) do n.º 5 do artigo 14.º do RGPD; tratamento de dados que implique ou consista na criação de perfis em grande escala; tratamento de dados pessoais que permita rastrear a localização ou os comportamentos dos respetivos titulares, que tenha como efeito a avaliação ou classificação destes, exceto quando o tratamento for indispensável para a prestação de serviços requeridos especificamente pelos mesmos; tratamento dos dados previstos no n.º 1 do artigo 9.º ou do artigo 19.º do RGPD ou ainda dos dados de natureza altamente pessoal para finalidade de arquivo de interesse público, investigação científica e histórica ou fins estatísticos, com exceção dos tratamentos previstos e regulados por lei que

apresente garantias adequadas dos direitos dos titulares; tratamento de dados biométricos para identificação inequívoca dos seus titulares, quando estes sejam pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados; tratamento de dados genéticos de pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados; tratamento de dados pessoais previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal com utilização de novas tecnologias ou nova utilização de tecnologias existentes".

Por força do número 1 do artigo 35.º, uma AIPD pode dizer respeito a um conjunto de operações de tratamento que apresenta riscos elevados semelhantes, explanando o considerando 92 que "em certas circunstâncias pode ser razoável e económico alargar a avaliação de impacto sobre a proteção de dados para além de um projeto único, por exemplo se as autoridades ou organismos públicos pretenderem criar uma aplicação ou uma plataforma de tratamento comum, ou se vários responsável pelo tratamento planearem criar uma aplicação ou um ambiente de tratamento comum em todo um setor ou segmento profissional, ou uma atividade horizontal amplamente utilizada".

A AIPD deverá compreender uma descrição organizada das operações de tratamento previstas e a finalidade do tratamento, a avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos, a avaliação dos riscos para os direitos e liberdades dos titulares dos direitos, as medidas previstas para fazer face aos riscos, assim como garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o RGPD[116], devendo ser

[116] Número 7 do artigo 35.º do RGPD.

solicitado parecer ao encarregado de proteção de dados, quando este tenha sido designado[117].

Por sua vez, sempre que da avaliação de impacto advier que do tratamento redundaria um risco elevado para os direitos e liberdade do titular dos dados na falta de garantias e de medidas tomadas pelo responsável pelo tratamento para atenuar o risco, o RGPD sagra a possibilidade do responsável pelo tratamento consultar a autoridade de controlo antes de proceder ao tratamento[118], clarificando o considerando 94 que nas situações em que o responsável pelo tratamento "considerar que o risco não poderá ser atenuado através de medidas razoáveis, atendendo à tecnologia disponível e aos custos de aplicação, a autoridade de controlo deverá ser consultada antes das atividades de tratamento terem início", acrescendo ainda que "a autoridade de controlo deverá responder ao pedido de consulta dentro de um determinado prazo. Contudo, a ausência de reação da autoridade de controlo no decorrer desse prazo não prejudicará qualquer intervenção que esta autoridade venha a fazer em conformidade com as suas funções e competências"[119].

O pedido de consulta prévia deverá ser acompanhado da indicação da repartição de responsabilidades entre o responsável pelo tratamento, os responsáveis conjuntos e os subcontratantes, quando aplicável, as finalidades e os meios de tratamento, as medidas e garantias previstas para defesa dos direitos e liberdades dos titulares dos dados, os

[117] Número 2 do artigo 35.º do RGPD.
[118] Artigo 36.º do RGPD.
[119] Número 2 do artigo 36.º do RGPD: "2. Sempre que considerar que o tratamento previsto referido no n.º 1 violaria o disposto no presente regulamento, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, a autoridade de controlo, no prazo máximo de oito semanas a contar da receção do pedido de consulta, dá orientações, por escrito, ao responsável pelo tratamento e, se o houver, ao subcontratante e pode recorrer a todos os seus poderes referidos no artigo 58.º. Esse prazo pode ser prorrogado até seis semanas, tendo em conta a complexidade do tratamento previsto. A autoridade de controlo informa da prorrogação o responsável pelo tratamento ou, se o houver, o subcontratante no prazo de um mês a contar da data de receção do pedido de consulta, juntamente com os motivos do atraso. Esses prazos podem ser suspensos até que a autoridade de controlo tenha obtido as informações que tenha solicitado para efeitos da consulta".

contactos do encarregado de proteção de dados, a avaliação de impacto sobre a proteção de dados, quaisquer outras informações solicitadas pela entidade de controlo[120].

A avaliação de impacto constitui uma excelente inovação do RGPD, podendo tornar-se uma ferramente extremamente útil às organizações na identificação de potenciais problemas com o tratamento de dados que efetuam, bem como demonstrar de *compliance* com o RGPD, contudo poderá trazer algumas dificuldades às organizações, nomeadamente "a incapacidade inerente de identificar riscos específicos quando o *machine learning*[121] estiver envolvido (…), por que a máquina pode estar a tomar decisões baseadas em factores que não são revelados fora da "caixa preta", não sendo possível antecipar um risco exato (embora certamente o potencial de discriminação em geral deva ser antecipado quando ocorrer criação de perfis)" (Houser & Voss, 2018 p. 55).

2.5.12 Segurança dos dados pessoais

Nos termos supra expostos, o princípio da integridade e confidencialidade impõe ao responsável pelo tratamento, e aos subcontratantes, a segurança dos dados pessoais das pessoas singulares, devendo os dados ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, devendo ser adotadas as medidas técnicas ou organizativas adequadas[122].

Considerando que a evolução da tecnologia, como a IoT[123], das redes sociais, computação em núvem e análise de dados permite uma recolha de dados em grande

[120] Número 3 do artigo 36.º do RGPD.
[121] O termo *machine learning* refere-se à "deteção automática de padrões significativos padrões em dados" (Shalev-Shwartz, & Ben-David, 2014, p. XV).
[122] Alínea f) do número 1 do artigo 5.º do RGPD.
[123] Por IoT entende-se internet das coisas, *Internt of things,* em inglês. "A Internet das Coisas (IoT) é um termo criado por Kevin Ashton, um pioneiro tecnológico britânico que concebeu um sistema de sensores onipresentes conectando o mundo físico à Internet,

quantidade, surgem diversos desafios relacionados com o aumento da preocupação com a privacidade em relação ao uso de grandes quantidades de dados e a necessidade de reconciliar o uso de dados pessoais e a privacidade, assim como, o uso de novos dispositivos de recolha e processamento de dados que aumentam o risco de ataque (Bertino & Ferrari, 2018, p. 425). Assim, no contexto da crescente evolução do cibercrime, o RGPD poderá apresentar uma oportunidade de acompanhar um cenário de segurança em mudança, na medida que obriga as organizações a adotar medidas técnicas e organizativas adqueadas aos tratamentos que realizam.

O RGPD introduziu inovações à noção de segurança do tratamento, assim, o artigo 32.º do RGPD obriga que o responsável pelo tratamento e os subcontratantes empreguem as medidas técnicas e organizativas apropriadas para asseverar um nível de segurança adequado ao risco, considerando as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades de tratamento, assim como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares. As medidas a adotar pelo responsável pelo tratamento e subcontratantes para assegurar a segurança do tratamento, são, nos termos do RGPD, a pseudonimização e a cifragem dos dados pessoais, medidas que assegurem a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, assim como, de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico, bem como, processos para atestar, apreciar e avaliar

enquanto trabalhava em identificação por rádio frequência (RFID). Embora as coisas, a Internet e a conectividade sejam os três componentes principais da Internet, o valor está no fechamento das lacunas entre os mundos físico e digital em sistemas com recursos de reforço e aprimoramento automáticos. A IoT cria esses sistemas ao conectar coisas, animadas ou inanimadas, à internet com identificadores exclusivos que oferecem contexto, o que proporciona visibilidade à rede, aos dispositivos e ao ambiente. Capacitada com conjuntos de dados completos e usando análise avançada, a IoT pode nos oferecer insights importantíssimos sobre o nosso mundo: ao medir as vibrações de pás de turbinas eólicas e executar análise em tempo real para determinar necessidades de manutenção antes que as pás apresentem defeitos. Ao reduzir o consumo de energia em edifícios controlando a iluminação em andares quando ninguém estiver presente. Ou ao criar veículos sem condutor que processam informações ambientais para tomar decisões imediatas para parar e evitar acidentes. O conhecimento coletivo sobre o mundo físico, obtido por meio da IoT, tornam-se ideias para aumentar a eficiência, novos modelos de negócios, diminuir a poluição e melhorar a saúde" (Cfr.https://aws.amazon.com/pt/iot/what-is-the-internet-of-things/, consultado 4/09/2019).

regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Acrescenta o considerando 74 do RGPD que as medidas a adotar deverão ter em consideração o seu âmbito, contexto e as finalidades de tratamento, bem como os riscos para os direitos e liberdades dos titulares dos dados pessoais.

A não adoção das medidas técnicas e organizativas que visem a segurança dos dados poderá desencadear violações dos dados pessoais que causem danos ao titular dos dados. Neste sentido, o número 12 do artigo 4.º do RGPD define a violação de dados pessoais como "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

O GT29 no seu parecer 03/2014 classificou as violações de dados pessoais de acordo com o princípio da segurança da informação, que abrange, conforme supramencionado, a confidencialidade, integridade e disponibilização, assim, uma violação da confidencialidade ocorre quando se verifica uma divulgação ou acesso acidental ou não autorizados aos dados pessoais, por sua vez uma violação da integridade dos dados ocorre quando existe uma alteração acidental ou não autorizada dos dados pessoais, a violação da disponibilidade ocorre quando existe uma perda de acesso ou a destruição acidental ou não autorizada de dados pessoais.

Perante uma possível violação de dados pessoais o RGPD exige que seja apurado se foram aplicadas todas as medidas tecnológicas de proteção e de organização de modo a

apurar a ocorrência de uma violação de dados pessoais e informar, sem demora injustificada, a autoridade de controlo, assim como o titular dos dados[124].

Assim que o responsável pelo tratamento confirme a ocorrência de uma violação dos dados pessoais, deverá notificá-la à autoridade de controlo, sem demora injustificada[125] e, sempre que possível, no prazo de 72 horas após o conhecimento, excepto nas situações em que consiga demonstrar, ao abrigo do princípio da responsabilidade, que a violação não é susceptível de implicar um risco para os direitos e liberdades das pessoas singulares[126].

Da notificação da violação dos dados pessoais à autoridade de controlo deverá constar a descrição da natureza da violação dos dados pessoais, referindo as categorias e o número aproximado de titulares de dados afetados, assim como as categorias e o número aproximado de registos de dados pessoais em causa, o nome e os contactos do encarregado da proteção de dados, a descrição das consequências prováveis da violação, assim como, as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive medidas para atenuar os seus eventuais efeitos negativos[127].

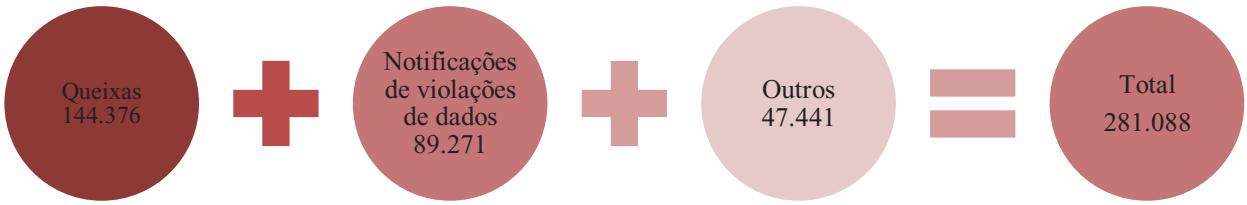
Quando a violação dos dados pessoais for passível de acarretar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento, mediante linguagem clara e simples, comunica a violação dos dados pessoais ao titular dos dados, sem demora injustificada, excepto quando o responsável pelo tratamento tiver aplicado as medidas de proteção adequadas aos dados pessoais afetados pela violação de dados

[124] Considerando 87 do RGPD.
[125] Nas situações em que não é possível ao responsável pelo tratamento notificar a violação de dados pessoais à autoridade de controlo no prazo de 72 horas, da notificação deverá constar os motivos que justificam o atraso.
[126] Artigo 33.º e considerando 85 do RGPD.
[127] Número 3 do artigo 33.º do RGPD.

pessoais, quando o responsável pelo tratamento tiver adotado medidas subsequentes à violação que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados não sejam suscetíveis de se concretizar, ou quando a comunicação implicar um esforço desproporcidonado, situação em que deverá ser feita uma comunicação pública.[128].

De acordo com o infográfico disponibilizado a 25 de maio de 2019 pela Comissão Europeia denominado "*GDPR in numbers*" [129] foram notificadas às autoridades de controlo na União Europeia 89.271[130] violações de dados pessoais entre 25 maio de 2018 e 25 de maio de 2019.

Figura 13 - Número de processos por tipo.

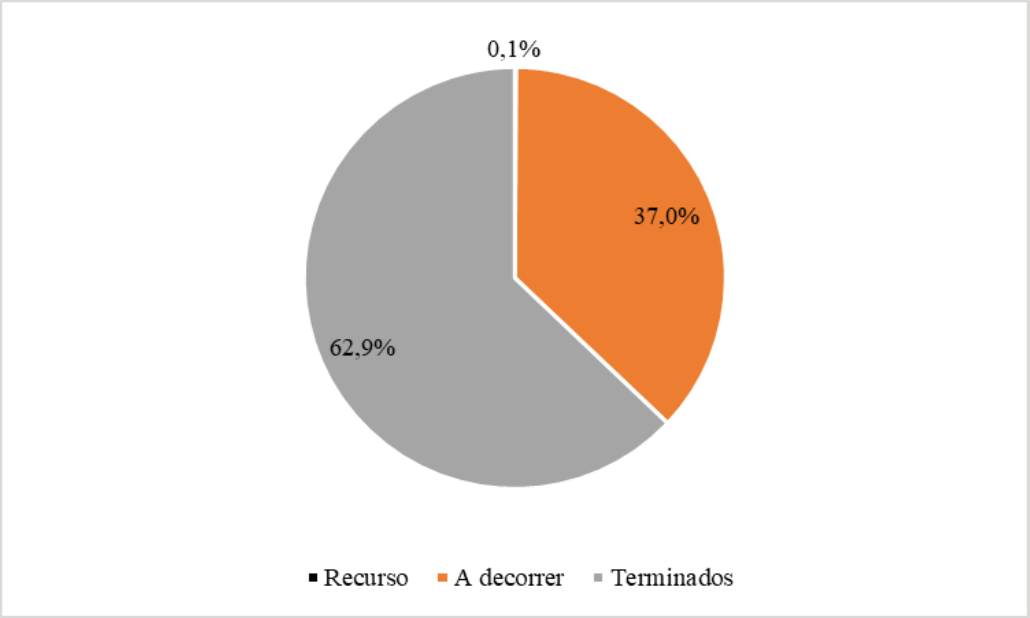


Fonte: "1 year GDPR – taking stock" European Data Protection Board

[128] Artigo 34.º do RGPD.
[129] Disponível no portal: https://ec.europa.eu/commission/sites/beta-political/files/infographicgdpr_in_numbers_0.pdf consultado a 30/07/2019.
[130] De acordo com o infográfico "GDPR in numbers", as atividades que geraram mais reclamações foram o telemarketing, e-mails promocionais e a utilização de sistemas de videovigilância.

Nos termos do publicação da European Data Protection Board (2019) intitulada "*1 year GDPR – taking stock*"[131] verificou-se um aumento das consultas e das reclamações rececionadas pelas autoridades de controlo, tendo-se verificando 144.376 consultas e reclamações e mais de 89.271 violações de dados pessoais, sendo que 62,9% das reclamações foram fechadas e 37% decorriam à data da publicação.

Figura 14 - Estado dos processos a nível Europeu. Fonte:"1 year GDPR – taking stock" European Data Protection Board



Deste modo, resulta do balanço realizado pela European Data Protection Board um aumento de consultas e reclamações por parte dos titulares de dados pessoais às autoridades de controlo, o que demonstra uma maior consciencialização dos titulares de dados pessoais dos seus direitos. Neste sentido, o Eurobârometro Especial 487a[132]/[133] de

[131] Disponível no portal: https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en, Consultado a 30/07/2019.

[132] Cfr. "Eurobârometro Especial 487ª", disponível em: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86886, consultado a 30/07/2019.

[133] "*MAIN FINDINGS: More than two thirds of Europeans have heard of GDPR. A clear majority have heard of most of the rights guaranteed by GDPR, and almost six in ten have heard of a national authority protecting their data: The majority (67%) of respondents have heard of GDPR: 36% have heard of it and know what it is, and 31% have heard of it but don't know exactly what it is; Overall almost three quarters (73%) have heard of at least one right guaranteed by GDPR. Three in ten respondents (31%) have heard of all the rights asked about in the survey, while just over one quarter (27%) have not heard of any of them. Almost two thirds (65%) have heard of the right to access their data, 61% have heard of the right to correct their data if it is wrong, 59% about the right to object to receiving direct marketing and 57% about the right to have their data deleted and forgotten. Half of the respondents have heard about the right to move their data from one provider to another and 41% have heard about the right to have a say when decisions are automated. The three most exercised rights are the right to object to receiving direct marketing (24%), the right to*

março de 2019 indicou que 67% dos cidadões europeus inquiridos já ouviram falar do RGPD, contudo apenas 36% dos cidadãos europeus inquiridos indicaram estar cientes do que o RGPD implica.

Mediante uma comparação dos resultados do Eurobârometro Especial 487a com os resultados obtidos no Eurobârometro Especial 431 de 2015[134], sobre a proteção de dados, é possível aferir um maior conhecimento das autoridades de controlo responsáveis pela proteção dos direitos de proteção de dados, sendo que no Eurobârometro 487a 57% dos inquiridos indicaram ter conhecimento da sua existência, enquanto que em 2015 apenas 37% dos inquiridos afirmaram ter conhecimento da existência de uma autoridade de controlo no seu país, verificando-se, assim, um aumento de 20% em comparação aos resultados do Eurobârometro 431.

Deste modo, os resultados do Eurobârometro 487a demonstram que a crescente preocupação com os dados pessoais aliada à ampla atenção que o RGPD trouxe para a temática dos dados pessoais, contribui para uma maior consciencialização do cidadão europeu para os seus direitos enquanto titular de dados pessoais, assim como do modo como os seus dados pessoais são tratados.

---

access personal data (18%), and the right to correct personal data if it is wrong (16%). A clear majority (57%) say they have heard about the existence of a public authority in their country responsible for protecting their rights regarding their personal data – an increase of 20 percentage points since 2015.A fifth of respondents know which public authority is responsible for protecting their data. The majority of respondents feel they have at least partial control over the information they provide online. Almost two thirds of respondents (65%) who provide personal information online feel they have at least some control over this information: 14% feel they have complete control and 51% that they have partial control. In all but one country, the majority of respondents who use the Internet feel they have at least some control over the information they provide online. 62% of respondents who feel they have partial or no control over the information they provide say they are concerned about this. This represents a decrease of five percentage points since 2015. Just over one in five say they are always informed about the conditions attached to the collection and use of their personal data online, and only a minority (13%) fully read privacy statements online. Amongst respondents who use the Internet, 57% say that they are at least sometimes informed about the conditions under which their data is collected and may be used further: 22% say they are always informed, while 35% say they are sometimes informed. Amongst respondents who use the Internet, the majority (60%) read privacy statements on the Internet – although they are more likely to do so partially (47%) than fully (13%). Respondents are less likely to read privacy statements than they were in 2015 (-7 percentage points). For respondents that only partially read privacy statement on the Internet, or who don't read them at all, by far the most common reason is that they are too long to read (66%). Almost one third (31%) say they find these statements unclear or difficult to understand, while 17% say it is enough for them to see the website has a privacy policy." (*Cfr* Comissão Europeia (2019). *Special Eurobarometer 487a, The General Data Protection Regulation*. P. 3-4. Disponível no portal: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222, consultado a 20/08/2019).

[134] *Cfr*. "Eurobârometro Especial 431 de 2015", disponível em: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/yearFrom/2013/yearTo/2015/s, consultado a 30/07/2019.

No contexto nacional, a CNPD abriu, até 31 de dezembro de 2018, 161 processos de violação de dados[135], salientando-se que o número de notificações de violações de dados pessoais foi bem superior ao número de processos abertos, nomeadamente, 439, contudo muitas das notificações correspondiam a denúncias ou reclamações dos titulares de dados que não justificaram a abertura de um processo de violações de dados. No mesmo período foram abertos 610 processos de natureza contraordenacional.

Desde a entrada em vigor do RGPD, na Região Autónoma dos Açores foram anunciadas três violações de dados por entidades públicas, nomeadamente, em abril de 2019 verificou-se a divulgação de dados de passageiros da Atlântico Line, incluindo a divulgação de dados de menores, onde "mais de 3600 ficheiros com dados de utilizadores da empresa de transporte marítimo Atlântico Line estiveram expostos na Internet durante tempo indeterminado. Segundo apurou a Exame Informática através de quem descobriu a fuga de informação cerca de 90% dos ficheiros dizem respeito a autorizações dadas por encarregados de menores no âmbito de viagens efetuadas através de ligações marítimas efetuadas por esta empresa pública entre as nove ilhas dos Açores. Entre os dados pessoais expostos na Internet, figuram múltiplos cartões do cidadão"[136].

Todavia, a violação de dados pessoais na Região Autónoma dos Açores mais mediática relaciona-se com a fuga de informação de 230 mil utentes do Serviço Regional de Saúde em que informação relativa a quase todos os habitantes dos Açores esteve exposta no site da ARS do Alentejo, "o ficheiro tinha o nome 'Exportação Utentes SRSA para Reembolsos'. Quem o descobria na Internet tinha uma surpresa: numa grelha Excel"

---

[135] Comissão Nacional de Proteção de Dados (2018). *Relatório de Atividades 2017-2018*. Disponível no portal: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201718.pdf, consultado a 7 de agosto de 2019.

[136] *Cfr*. SÉNECA, Hugo: *"Açores: dados de 3000 menores expostos na Internet por falha da Atlântico Line",* Exame Informática, 30 de abril de 2019, in http://exameinformatica.sapo.pt/noticias/internet/2019-04-30-Acores-dados-de-3000-menores-expostos-na-Internet-por-falha-da-Atlantico-Line.

estavam "os dados discriminados de mais de 230 mil habitantes dos Açores", incluindo "nomes completos, número fiscal, e de utente dos serviços de saúde regionais, moradas, datas de nascimento e números de telefone e/ou telemóveis"[137].

Por sua vez em março de 2017 foi divulgado que "endereços eletrónicos de alunos menores de idade de Angra do Heroísmo, na ilha Terceira, estavam acessíveis na Internet há vários anos, situação confirmada pela Direção Regional da Educação, que negou "má-fé" neste caso. Na página na Internet da escola básica integrada de Angra do Heroísmo, os endereços eletrónicos de diversos alunos surgiam acompanhados do nome completo, idade, turma e ano de escolaridade, em listagens do Departamento de Matemática do estabelecimento de ensino. Estas listagens, que, entretanto, deixaram de constar na Internet, eram relativas à resolução do "problema do mês", nas quais surgiam, igualmente, as notas que os alunos obtiveram neste ano letivo neste concurso, que visa "incentivar o gosto pela Matemática"[138].

Na decorrência de um pedido de colaboração no âmbito da presente dissertação, a CNPD informou que "todas as notificações de violações de dados realizadas ao abrigo do artigo 33.º do RGPD dão origem a processos. Foram recebidas na CNPD no período de 25 de maio (de 2018) a 31 de julho (2019) um total de 326 notificações" acrescentando ainda que "não foram ainda aplicadas coimas, mas sim outras medidas corretivas e algumas recomendações".

A nível contraordenacional verificou-se a aplicação da maior coima no contexto nacional, referente a três coimas, no valor global de 400.000,00€, aplicadas ao Centro

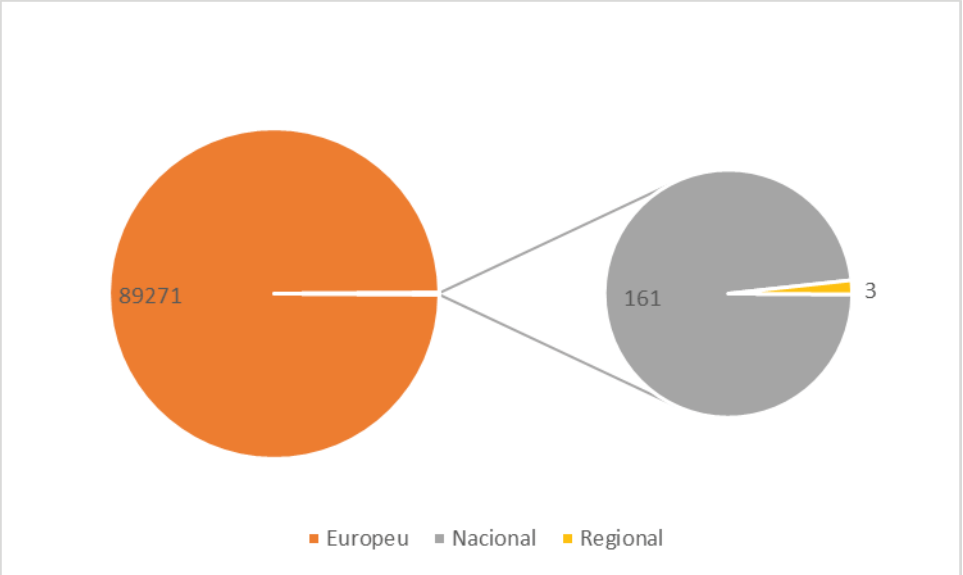
---

[137] *Cfr.* LUSA, BERENGUER, Márcio, SANCHES, Andreia: *"Açores: dados de 230 mil utentes do Serviço Regional de Saúde divulgados na Internet",* Público, 13 de março de 2017, in https://www.publico.pt/2017/03/13/sociedade/noticia/dados-de-230-mil-utentes-do-servico-regional-de-saude-divulgados-na-internet-1765047.

[138] *Cfr.* LUSA: *"PSD/Açores quer explicações sobre dados pessoais de alunos menores expostos na Internet",* Acoriano Oriental, 21 de março de 2017, in https://www.acorianooriental.pt/noticia/psd-acores-quer-explicacoes-sobre-dados-pessoais-de-alunos-menores-expostos-na-internet.

Hospitalar Barreiro-Montijo, por violação do princípio da minimização de dados, na medida em que era possível o acesso indiscriminado aos dados clínicos dos utentes, do princípio da integridade e confindencialidade[139/140].

Figura 15 – Violação de dados pessoais a nível europeu, nacional e regional.



Em suma, o gráfico supra retrata bem a questão da violação dos dados pessoais a nível da União Europeia, na nível nacional e regional.

2.5.13 Vias de recuro, responsabilidade e sanções

O RGPD confere a todos os titulares de dados pessoais o direito a apresentar reclamação a uma autoridade de controlo, quando considere que as operações de tratamento dos dados pessoais que lhe digam respeito viola o regulamento[141], assim como o direito à ação judicial contra as decisões juridicamente vinculativas das autoridades de controlo que lhes digam respeito[142] e o direito à ação judicial contra um responsável pelo tratamento ou

[139] *Cfr.* HIPPA Journal: "First Hospital GDPR Violation Penalty Issued: Portuguese Hospital to Pay €400,000 GDPR Fine", HIPPA Journal, 7 de dezembro de 2018, *in* https://www.hipaajournal.com/first-hospital-gdpr-violation-penalty-issued-portuguese-hospital-to-pay-e400000-gdpr-fine/, consultado a 07/08/2019.
[140] *Cfr.* Comissão Nacional de Proteção de dados, Deliberação n.º 984/2018, de 9 de outubro de 2018. Disponível em: https://www.cnpd.pt/bin/decisoes/Delib/20_984_2018.pdf, consultado a 22/09/2019.
[141] Artigo 77.º do RGPD.
[142] Artigo 78.º do RGPD.

subcontratante quando considerem ter havido violação dos direitos que lhes assistem nos termos do RGPD, na sequência do tratamento dos seus dados pessoais efetuado em violação do RGPD[143].

Parelalemente, o RGPD confere o direito do titular dos dados que tenha sofrido danos materiais ou imateriais devido a uma violação do RGPD à indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos[144]. Todavia, o responsável pelo tratamento ou o subcontratante fica isento de responsabilidade se provar que não é responsável pelo evento que originou os danos sofridos.

Uma das principais novidades introduzidas pelo RGPD é o quadro sancionatório. Nesta medida, de modo a reforçar o cumprimento das regras impostas pelo RGPD, o regulamento determina a aplicação de sanções por "violação do presente regulamento, para além, ou em substituição, das medidas adequadas que venham a ser impostas pela autoridade de controlo", sendo que em caso "infração menor, ou se o montante da coima (…) constituir um encargo desproporcionado para uma pessoa singular, pode ser feita uma repreensão em vez de ser aplicada uma coima", devendo ser considerado a seriedade da infração, o seu carácter doloso, a adoção de medidas atenuantes dos danos sofridos, o grau de responsabilidade, a via pela qual a infração chegou ao conhecimento da autoridade de controlo, o cumprimento das medidas ordenadas contra o responsável pelo tratamento ou subcontratante, ou quaisquer outros fatores agravantes ou atenuantes[145].

As coimas deverão ser em cada caso individuais, efetivas, proporcionadas e dissuasivas podendo ser fixadas até 10 000 000€ ou, no caso de uma empresa, até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro

[143] Artigo 79.º do RGPD.
[144] Artigo 82.º do RGPD.
[145] Considerando 148 e artigo 83.º do RGPD.

anterior[146] nas situação do número 4.º do artigo 83.º do RGPD ou até 20 000 000€ ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior[147]. Todavia, a Lei n.º 58/2018, de 8 de agosto veio atenuar o regime sancionatório europeu ao introduzir limites minímos nos artigos 37.º[148] e 38.º[149], ora, considerando que o principal objetivo do RGPD é a uniformização no espaço europeu, não se entende como o legislador português pretende afastar os limites máximos definidos nos números 4 e 5 do artigo 83.º do RGPD, sendo,

[146] Número 4 do artigo 83.º do RGPD: "A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.º 2, a coimas até 10 000 000 EUR ou, no caso de uma empresa, até 2 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado: a) As obrigações do responsável pelo tratamento e do subcontratante nos termos dos artigos 8, 11.º, 25.º a 39.º e 42.º e 43.º; b) As obrigações do organismo de certificação nos termos dos artigos 42.º e 43.º; c) As obrigações do organismo de supervisão nos termos do artigo 41.º, n.º4".

[147] Número 5 do artigo 83.º do RGPD: "A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.º 2, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado: a) Os princípios básicos do tratamento, incluindo as condições de consentimento, nos termos dos artigos 5, 6.º, 7.º e 9.º; b) Os direitos dos titulares dos dados nos termos dos artigos 12 a 22.º; c) As transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional nos termos dos artigos 44 a 49.º; d) As obrigações nos termos do direito do Estado-Membro adotado ao abrigo do capítulo IX; e) O incumprimento de uma ordem de limitação, temporária ou definitiva, relativa ao tratamento ou à suspensão de fluxos de dados, emitida pela autoridade de controlo nos termos do artigo 58.º, n.º 2, ou o facto de não facultar acesso, em violação do artigo 58.º, n.º 1."

[148] Artigo 37.º da Lei n.º 58/2019, de 8 de agosto "Contraordenações muito graves 1 - Constituem contraordenações muito graves: a) Os tratamentos de dados pessoais com inobservância dolosa dos princípios consagrados no artigo 5.º do RGDP; b) Os tratamentos de dados pessoais que não tenham por base o consentimento ou outra condição de legitimidade, nos termos do artigo 6.º do RGPD ou de norma nacional; c) O incumprimento das regras relativas à prestação do consentimento previstas no artigo 7.º do RGPD; d) Os tratamentos de dados pessoais previstos no n.º 1 do artigo 9.º do RGPD sem que se verifique uma das circunstâncias previstas no n.º 2 do mesmo artigo; e) Os tratamentos de dados pessoais previstos no artigo 10.º do RGPD que contrariem as regras aí previstas; f) A exigência do pagamento de uma quantia em dinheiro fora dos casos previstos no n.º 5 do artigo 12.º do RGPD; g) A exigência do pagamento de uma quantia em dinheiro, nos casos previstos no n.º 5 do artigo 12.º do RGPD, que exceda os custos necessários para satisfazer o direito do titular dos dados; h) A não prestação de informação relevante nos termos dos artigos 13.º e 14.º do RGPD, o que ocorre nas seguintes circunstâncias: i) Omissão de informação das finalidades a que se destina o tratamento; ii) Omissão de informação acerca dos destinatários ou categorias de destinatários dos dados pessoais; iii) Omissão de informação acerca do direito de retirar o consentimento nos casos previstos na alínea a) do n.º 1 do artigo 6.º e na alínea a) do n.º 2 do artigo 9.º do RGPD; i) Não permitir, não assegurar ou dificultar o exercício dos direitos previstos nos artigos 15.º a 22.º do RGPD; j) A transferência internacional de dados pessoais em violação do disposto nos artigos 44.º a 49.º do RGPD; k) O incumprimento das decisões da autoridade de controlo previstas no n.º 2 do artigo 58.º do RGPD, ou recusa da colaboração que lhe seja exigida pela CNPD, no exercício dos seus poderes; l) A violação das regras previstas no capítulo vi da presente lei. 2 - As contraordenações referidas no número anterior são punidas com coima: a) De 5000 (euro) a 20 000 000 (euro) ou 4 % do volume de negócios anual, a nível mundial, conforme o que for mais elevado, tratando-se de grande empresa; b) De 2000 (euro) a 2 000 000 (euro) ou 4 % do volume de negócios anual, a nível mundial, conforme o que for mais elevado, tratando-se de PME; c) De 1000 (euro) a 500 000 (euro), no caso de pessoas singulares."

[149] Artigo 38.º da Lei n.º 58/2019, de 8 de agosto "Contraordenações graves 1 - Constituem contraordenações graves: a) A violação do disposto no artigo 8.º do RGPD; b) A não prestação da restante informação prevista nos artigos 13.º e 14.º do RGPD; c) A violação do disposto nos artigos 24.º e 25.º do RGPD; d) A violação das obrigações previstas no artigo 26.º do RGPD; e) A violação do disposto no artigo 27.º do RGPD; f) A violação das obrigações previstas no artigo 28.º do RGPD; g) A violação do disposto no artigo 29.º do RGPD; h) A ausência de registo dos tratamentos de dados pessoais em violação do disposto no artigo 30.º do RGPD; i) A violação das regras de segurança previstas no artigo 32.º do RGPD; j) O incumprimento dos deveres previstos no artigo 33.º do RGPD; k) O incumprimento do dever de informar o titular dos dados pessoais nas situações previstas no artigo 34.º do RGPD; l) O incumprimento da obrigação de realizar avaliações de impacto nos casos previstos no artigo 35.º do RGPD; m) O incumprimento da obrigação de consultar a autoridade de controlo previamente à realização de operações de tratamento de dados nos casos previstos no artigo 36.º do RGPD; n) O incumprimento dos deveres previstos no artigo 37.º do RGPD; o) A violação do disposto no artigo 38.º do RGPD, nomeadamente no que respeita às garantias de independência do encarregado de proteção de dados; p) O incumprimento dos deveres previstos no artigo 39.º do RGPD; q) A prática de atos de supervisão de códigos de conduta por organismos não acreditados pela autoridade de controlo nos termos do artigo 41.º do RGPD; r) O incumprimento, por parte dos organismos de supervisão de códigos de conduta, do previsto no n.º 4 do artigo 41.º do RGPD; s) A utilização de selos ou marcas de proteção de dados que não tinham sido emitidos por organismos de certificação devidamente acreditados nos termos dos artigos 42.º e 43.º do RGPD; t) O incumprimento, por parte dos organismos de certificação, dos deveres previstos no artigo 43.º do RGPD; u) A violação do disposto no artigo 19.º da presente lei. 2 - As contraordenações referidas no número anterior são punidas com coima de: a) De 2500 (euro) a 10 000 000 (euro) ou 2 % do volume de negócios anual, a nível mundial, conforme o que for mais elevado, tratando-se de grande empresa; b) De 1000 (euro) a 1 000 000 (euro) ou 2 % do volume de negócios anual, a nível mundial, conforme o que for mais elevado, tratando-se de PME; c) De 500 (euro) a 250 000 (euro), no caso de pessoas singulares".

claramente, estabelecido no referido artigo que a competência para definição das coimas compete às autoridades de controlo e não ao legislador, neste sentido dispõem os considerandos 148 e 150 do RGPD, estabelecendo o considerando 150 que "o presente regulamento deverá definir as violações e o montante máximo e o critério de fixação do valor das coima daí decorrentes, que deverá ser determinado pela autoridade de controlo competente, em cada caso individual" [150].

Uma das grandes problemáticas que assomaram no contexto nacional português relacionadas à aplicação do RGPD surgiu com a proposta de Lei n.º 120/XIII que isentava as entidades públicas de aplicações de contraordenações. Por sua vez a Lei n.º 58/2019, de 8 de agosto, no seu artigo 44.º estipula que as coimas previstas no RGPD e na referida lei aplicam-se de igual modo às entidades públicas e privadas, no entando o seu número 2 consagra uma isenção de aplicação de contraordenações às entidades públicas que depende de determinados requisitos[151], estabelecendo 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"[152], todavia, a referida lei prevê sanções criminais nos seus artigos 46.º a 54.º não isentando as entidades públicas e os seus colaboradores das mesmas, sendo que tal circunstância surge como agravante da responsabilidade criminal na alínea a) do número 2 do artigo 51.º referente ao crime de violação do dever de sigilo.

---

[150] A Deliberação/2019/494 veio proceder à desaplicação dos artigos 37.º, 38.º e 39.º da Lei n.º 58/2019, estabelecendo que "o n.º 2 do artigo 37.º e o n.º 2 do artigo 38.º definem, para os ilícitos previstos nos n.ºs 4 e 5 do artigo 83.º do RGPD, molduras sancionatórias distintas em função da dimensão das empresas e da natureza coletiva ou singular dos sujeitos que realizem tratamentos de dados. Num quadro regulatório que se pretende uniforme no espaço europeu, os limites máximos definidos nos n.ºs 4 e 5 do artigo 83.º do RGPD não podem ser afastados pelos Estados-Membros da União.

[151] O artigo 59.º da Lei n.º 58/2019, de 8 de agosto, estipula que a possibilidade de não aplicabilidade de coimas às entidades públicas deverá ser objeto de reavaliação no prazo de três anos após a entrada em vigor da referida lei.

[152] Sobre está temática a CNPD veio através da Deliberação 2019/495 esclarecer que "interpreta o disposto no n.º2 do artigo 44.º da Lei n.º 58/2019 no sentido de este lhe conferir um poder discricionário de apreciar, apenas no caso concreto de verificação prática de um facto ilícito em violação do disposto no RGPD ou naquela lei, se se justifica afastar a regra legal de aplicação de uma sanção pecuniária (coima) a um determinado organismo público, enquanto responsável pelo tratamento (ou subcontratante), tendo em consta os diferentes interesses e direitos em presença), disponível em: https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_495.pdf)-, consultado em 24/09/2019.

A Comissão Europeia, questionada sobre as consequências do incumprimento das regras relativas à proteção de dados para as administrações públicas, esclareceu que "em caso de infração provável, pode ser emitida uma advertência. Em caso de infração, as possibilidades incluem: uma repreensão ou uma proibição temporária ou definitiva do tratamento. Em alguns países, os organismos públicos podem estar também sujeitos a coimas administrativas."[153]

Para que o novo quadro sancionatório seja eficaz as autoridades de controlo devem estar munidas de vários poderes de investigação e correção e condições para o efeito. Por sua vez, a CNPD por diversas vezes afirmou não dispor dos meios necessários para fiscalizar o cumprimento do RGPD[154/155], o que constitui um grande entrave à correta aplicação do RGPD no território português, sendo que Portugal é um dos países mais atrasado na aplicação do RGPD.

2.6 Considerações finais

Através da análise da evolução legislativa no âmbito dos dados pessoais e do RGPD, procurou-se desenvolver, ao longo do presente capítulo, um estudo onde fossem abordadas as alterações introduzidas pelo RGPD, que acarreta para os responsáveis pelo tratamento um quadro legal mais rígido, baseado na autorregulação, concluindo-se que muitas dos institutos consagrados pelo RGPD são uma evolução do que vinha sendo consagrado legalmente na matéria, não se tratando de novidades, conforme muitos responsáveis pelo tratamento consideram.

---

[153] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-if-public-administration-fails-comply-data-protection-rules_pt, consultado a 21/09/2019.

[154] *Cfr.* LUSA: *"Comissão Nacional de Proteção de Dados continua sem meios para fiscalizar",* Diário de Notícias, 22 de maio de 2019, *in* https://www.dn.pt/lusa/interior/comissao-nacional-de-protecao-de-dados-continua-sem-meios-para-fiscalizar-10927841.html, consultado a 15/07/2019.

[155] *Cfr.* REVISTA DE IMPRENSA JE: "*Portugal sem meios de proteção de dados pessoais, CNPD alerta o agravamento da situação*", Jornal Económico, 8 de novembro de 2018, *in* https://jornaleconomico.sapo.pt/noticias/portugal-sem-meios-de-protecao-de-dados-pessoais-cnpd-alerta-o-agravamento-da-situacao-375383, consultado a 15/09/2019.

As evoluções introduzidas pelo RGPD demonstram-se essenciais ao desenvolvimento do Mercado Único Digital, assim como à proteção dos dados das pessoas singulares, que até então viam os seus dados pessoais a ser constantemente violados, e com poucos mecanismos de defesa dos seus direitos, sendo que o RGPD representa uma oportunidade dos responsáveis de tratamento de refazerem os seus modelos de tratamento de dados, não devendo por este modo ser encarado como um sistema penalizador e obrigacional aos responsáveis pelo tratamento, mas sim um regime protecionista dos dados pessoais.

CAPÍTULO III – A ADMINISTRAÇÃO PÚBLICA E A PROTEÇÃO DE DADOS

3.1 Sumário

3.2. Resumo – **3.3.** Introdução; **3.4.** O RGPD e a Administração Pública. **3.5.** O encarregado de proteção de dados e a Administração Pública Regional **3.6.** O acesso a documentos administrativos e a proteção de dados pessoais; **3.6.1.** O acesso a documentos administrativos nominativos; **3.6.2**. O princípio da proporcionalidade; **3.7.** Considerações finais.

3.2 Resumo

Neste segundo capítulo incidiremos o nosso estudo sobre o papel da proteção de dados na Administração Pública, assim como os contornos da implementação nos organismos públicos. Finalmente, abordaremos o regime de acesso aos documentos administrativos, nomeadamente, documentos nominativos, procedendo à análise do seu âmbito e limites, assim como o modo como o regime de proteção de dados deverá relacionar-se com o regime de acesso aos documentos administrativos.

3.3 Introdução

Tanto o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 como a Constituição da República Portuguesa consagram, como regra geral, a proibição de acesso a dados pessoais de terceiros. No entanto os princípios orientadores da atividade administrativa no ordenamento jurídico português, nomeadamente, o princípio da informação, transparência administrativa e da administração aberta, consagram o direito do cidadão a ser informado e de ter acesso à atuação administrativa.

No presente capítulo abordar-se-á a correlação do novo paradigma da proteção de dados e do regime de acesso aos documentos administrativos, uma vez que o RGPD não

pretende desvirtuar os princípios orientadores da atividade administrativa ou proibir o acesso do cidadão aos documentos administrativos, ou conceber a Administração como uma organização secreta, prevendo, inclusive, o acesso a documentos administrativos nominativos.

3.4 O RGPD e a Administração Pública

Na aceção de Almeida (2015) "etimologicamente, administração consiste no manejo, na utilização de certos meios, com vista a alcançar um determinado fim. A palavra, é, no entanto, utilizada para designar a atividade de administrar, como, também, para designar o organismo ou entidade que desenvolve essa atividade. (…) A atividade da administração pública vai ser, assim, desenvolvida por um conjunto de entidades, pessoas coletivas de direito público, integradas por um vasto conjunto de serviços públicos, especificadamente instituídos para o efeito: ao conjunto desses serviços dá-se o nome de Administração Pública" (p.16).

Neste sentido, a Administração pública encontra-se sujeita às regras do RGPD na medida que no âmbito das suas competências e atribuições conferidas por lei aos serviços públicos, tem legitimidade para tratar dados pessoais dos administrandos, devendo esse tratamento ser pautado pelos princípios fundamentais de tratamento de dados pessoais consagrados no RGPD, nomeadamente, tratamento equitativo e lícito, limitação da finalidade, minimização dos dados e conservação dos dados, esclarecendo a Comissão Europeia que "a maior parte dos dados pessoais detidos pela administração pública são habitualmente tratados com base numa obrigação jurídica ou na medida do necessário

para realizar tarefas por motivos de interesse público ou no exercício de autoridade pública de que está investida"[156].

No entendimento de Francisco, D., & Francisco, S. (2019) "a AP por estar legitimada para efetuar tratamentos de dados pessoais, não pode deixar de aplicar os princípios de proteção de dados do artigo 5.º do RGPD (…) e de garantir que são para o cumprimento de finalidades determinadas, explícitas e legítimas. Em especial quando pretender efetuar tratamentos que estejam para além das suas competências, situação em que a AP deve verificar se necessita de invocar outros meios de licitude, designadamente o consentimento do titular" (p.34).

Por sua vez, o artigo 26.º da Lei n.º 58/2019, de 8 de agosto, permite que em casos excecionais e devidamente fundamentados, o tratamento de dados pessoais por entidades públicas para finalidades diferentes das determinadas pela recolha, devendo tal tratamento ser fundamentado na prossecução do interesse público que de outra forma não possa ser acautelado, permitindo ainda a transmissão de dados pessoais entre entidades públicas para finalidades diferentes das determinadas pela recolha, devendo tal tratamento constar de um protocolo que determine as responsabilidades de cada entidade interveniente.

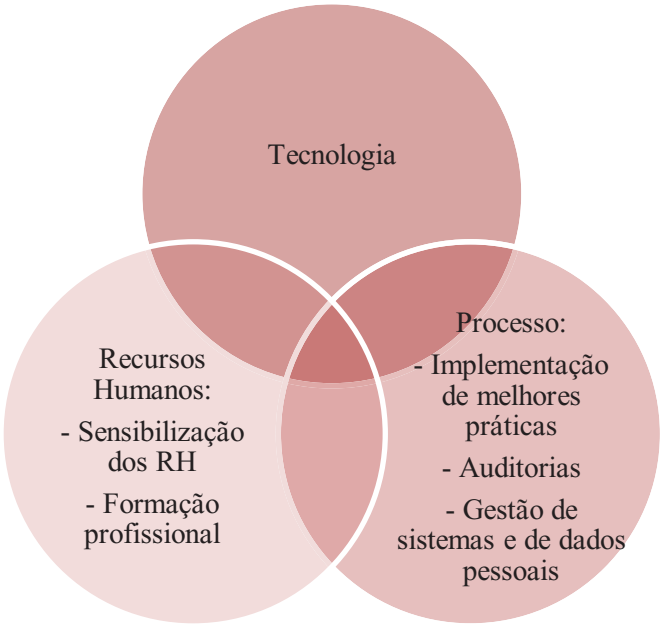
A implementação do RGPD no seio da administração pública demonstra-se ardilosa, obrigando o envolvimento de toda a organização e a implementação de mudanças, sendo que implica um conhecimento vasto da própria organização, devendo as entidades públicas identificar que dados pessoais tratam, em que processos sucede o tratamento e se estes tratamentos encontram-se conforme o estabelecido no RGPD, sendo certo que,

[156] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_pt, consultado a 2/09/2019.

embora o regime de proteção de dados não seja novidade, não consubstanciava uma preocupação de muitas das entidades.

A implementação deverá incluir três categorias de atividade, nomeadamente, recursos humanos, processos e tecnologia.

Figura 16 - Áreas de atividade a envolver na implementação do RGPD



Deste modo, cada organismo de direito público é responsável pela implementação do RGPD no seio da sua organização, implementando as medidas necessárias a demonstrar *compliance* da sua atividade com o RGPD. Nos termos do artigo 24.º do RGPD a implementação do referido regulamento nos serviços públicos constitui responsabilidade do dirigente máximo, na medida que este é o responsável pelo tratamento[157].

A Presidência do Conselho de Ministros publicou uma proposta de plano de ação[158] dividido em cinco fases, nomeadamente, "designar um encarregado de proteção de dados,

[157] Artigo 24.º do RGPD "Responsabilidade do responsável pelo tratamento. 1. 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."
[158] Disponível em: http://www.sg.pcm.gov.pt/media/33592/04.pdf, consultado a 10/09/2019.

mapear os dados pessoais objeto de tratamento, priorizar as ações a desenvolver, organizar os processos internos e documentar a conformidade com o RGPD".

Por sua vez Francisco, D., & Francisco, S. (2019) sistematizam um projeto de implementação em 7 passos, nomeadamente, "planear bem o trabalho, mapear todos os dados pessoais tratados na organização, caracterizar os tratamentos tal como são realizados à data, identificar as atividades que carecem de alteração e quais as que têm maior risco, implementar as alterações, verificar a conformidade e garantir a compatibilidade tecnológica, constituir um dossier com as evidências de implementação, avaliar o impacto do projeto, formar os colaboradores da organização e criar as condições para que a organização integre, no seu funcionamento, estruturas e cultura organizacional, a monitorização e a conformidade com o RGPD" (p.60).

De modo a que a implementação do RGPD seja possível torna-se necessário que a organização tenha um conhecimento amplo dos seus procedimentos de tratamento de dados, devendo para o efeito proceder ao levantamento dos dados pessoais tratados por si, mediante um registo de atividades de tratamento, obrigatório nos termos do artigo 30.º do RGPD[159], estabelecendo as finalidades de tratamento, fundamentos de licitude de

[159] Artigo 30.º do RGPD" Registos das atividades de tratamento 1. Cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade. Desse registo constam todas seguintes informações: a) O nome e os contactos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados; b) As finalidades do tratamento dos dados; c) A descrição das categorias de titulares de dados e das categorias de dados pessoais; d) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais; e) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.o, n.º 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas; f) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados; g) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1. 2. Cada subcontratante e, sendo caso disso, o representante deste, conserva um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento, do qual constará: a) O nome e contactos do subcontratante ou subcontratantes e de cada responsável pelo tratamento em nome do qual o subcontratante atua, bem como, sendo caso disso do representante do responsável pelo tratamento ou do subcontratante e do encarregado da proteção de dados; b) As categorias de tratamentos de dados pessoais efetuados em nome de cada responsável pelo tratamento; c) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.º, n.º 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas; d)Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1. 3. Os registos a que se referem os n.º 1 e 2 são efetuados por escrito, incluindo em formato eletrónico. 4. O responsável pelo tratamento e, sendo caso disso, o subcontratante, o representante do responsável pelo tratamento ou do subcontratante, disponibilizam, a pedido, o registo à autoridade de controlo. 5. As obrigações a que se referem os n.º 1 e 2 não se aplicam às empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou

tratamento, definindo categorias de dados pessoais e prazos de conservação dos mesmos, categorias de titulares de dados, categorias de destinatários de dados pessoais, assim como definir medidas técnicas e organizativas de segurança. Para o efeito a CNPD disponibilizou um *template* de registo de atividades de tratamento no seu site[160].

Figura 17 - Exemplo de *template* de registo de tratamento disponibilizado pela CNPD

# Tratamento							
Qual a finalidade							
ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade							
Categorias de Dados tratados							
dados de identificação		dados de contacto		dados de faturação		vida familiar	
Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação
ex: nome, fotografia, número de identificação civil	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: morada, e-mail, telefone*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: NIF, montante cobrado, data, IBAN*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: situação familiar, dados do agregado familiar, estado civil*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*

Fonte: Comissão Nacional de Proteção de Dados

Deverão ainda ser implementados processos e políticas que assegurem e demonstrem a conformidade com todas as obrigações impostas pelo RGPD, nomeadamente, criadas políticas de privacidade e de proteção de dados, devidamente publicadas de modo a que todos os titulares de dados pessoais possam ter acesso, em que os titulares dos dados pessoais sejam informados dos seus direitos e de como os poderão exercer, os dados pessoais dos mesmo que são tratados, prazos e por quem estão a ser tratados, bem como dos fins do tratamento, devendo de igual modo os contatos do EPD ser divulgado.

abranja as categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10º."

[160] *Cfr.* Comissão Nacional de Proteção de Dados, disponível em: https://www.cnpd.pt/bin/rgpd/rgpd.htm, consultado a 9/09/2019.

Por sua vez a documentação da organização deverá ser revista, nomeadamente, políticas internas da empresa e formulários, de modo a que sejam identificados quaisquer detalhes ausentes que constituam obrigação legal nos termos do RGPD. De igual modo, deverá a entidade desenvolver formulários próprios para o exercício de direitos, assim como uma política de resposta às solicitações do titular dos dados e de resposta a violações de dados pessoais, elaborando minutas de notificação.

Deve ainda ser criado um procedimento para a avaliação do impacto de proteção de dados (ex. aplicação da norma ISO 31000:2009), assim como devem ser avaliados os sistemas de tecnologia da informação e adotadas medidas de segurança no tratamento.

Considerando que as entidades públicas nos termos do número 1 do artigo 2.º do Código dos Contratos Públicos[161]/[162] encontram-se sujeitas às regras de contratação pública previstas no referido Código, torna-se imperioso que as mesmas consignem nos contratos públicos que celebram a sua conformidade com o RGPD, devendo dos seus contratos fazer constar uma cláusula relacionada com a proteção de dados, que responsabilize o adjudicatário - que assume o papel do subcontratante[163]/[164] - pelo respeito pelas normas respeitantes à proteção de dados pessoais, assim como regule os termos do tratamento a efetuar, sendo que o subcontratante assume diretamente responsabilidades, recaindo sobre ele um conjunto de obrigações. Por sua vez, os contratos vigentes devem

[161] Decreto-Lei n.º 18/2008, Diário da República n.º 20/2008, Série I de 2008-01-29, pp. 753 – 852.
[162] Nos termos do número 1 do artigo 2.º do Código dos Contratos Públicos as regras de contratação pública aplicam-se ao Estado, às Regiões Autónomas, Autarquias Locais, Institutos Públicos, entidades administrativas independentes, Banco de Portugal, as fundações públicas, as associações públicas, as associações de que façam parte uma ou várias pessoas coletivas referidas anteriormente, desde que sejam maioritariamente financiadas por estas, estejam sujeitas ao seu controle de gestão ou tenham um órgão de administração, de direção ou de fiscalização cuja maioria dos titulares seja, direta ou indiretamente, designadas pelas mesmas.
[163] A Comissão Europeia esclareceu que" o subcontratante só efetua o tratamento de dados pessoais em nome do responsável pelo tratamento. O subcontratante é geralmente um terceiro externo à empresa; contudo, no caso dos grupos de empresas, uma empresa pode atuar como subcontratante para outra empresa. Os deveres do subcontratante perante o responsável pelo tratamento devem ser especificadas num contrato ou noutro ato jurídico. Por exemplo o contrato deve indicar o que acontece aos dados pessoais uma vez terminado o contrato", disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_pt, consultado a 1/09/2019.
[164] O artigo 4.º n.º 8 define subcontratante como "uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes".

ser analisados e determinadas as alterações necessárias, em especial à luz dos novos requisitos para o tratamento dos dados.

A implementação do RGPD na Administração Pública demonstra-se uma tarefa árdua, obrigando a uma enorme análise e revisão de todos os procedimentos de tratamentos de dados pessoais, contudo, o RGPD deverá ser encarado como uma excelente oportunidade para os organismos públicos modernizarem e reverem os seus procedimentos de tratamento de dados, privacidade e segurança, assim como, os processos de gestão dos seus dados pessoais, reduzindo o número de dados que recolhem e armazenam, melhorando, assim, a eficiência dos entes públicos.

3.5 O Encarregado de proteção de dados e a Administração Pública Regional

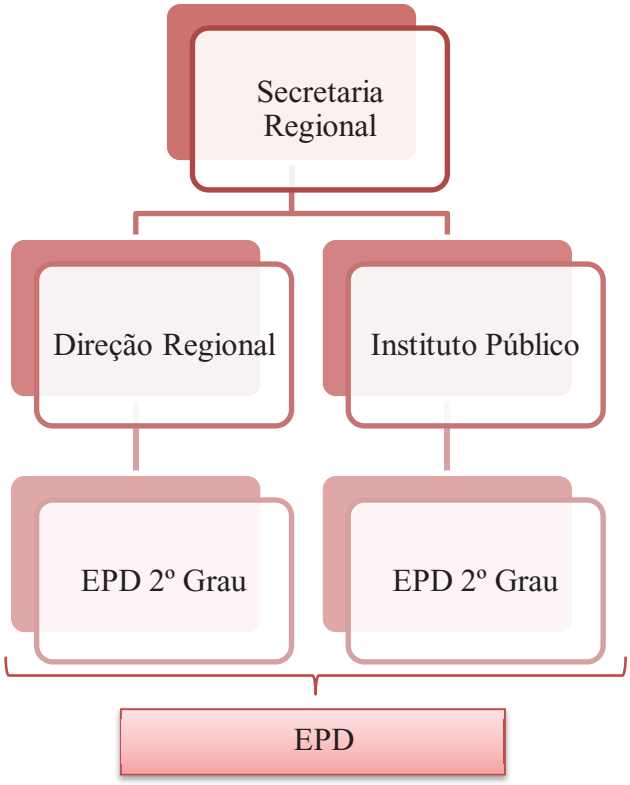
As administrações públicas "têm a obrigação de nomear um encarregado de proteção de dados, embora seja possível nomear um único encarregado da proteção de dados para vários organismos públicos, que poderão partilhar os seus serviços ou subcontratar esta tarefa a um EPD externo"[165], neste sentido dispõe a alínea a) do n.º 1 do artigo 37.º do RGPD e a Lei n.º 58/2019, de 8 de agosto no seu artigo 12.º[166].

[165] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_pt , consultado a 10/08/2019.

[166] Artigo 12.º da Lei n.º 58/2019, de 8 de agosto "Encarregados de proteção de dados em entidades públicas. 1 - Nos termos da alínea a) do n.º 1 do artigo 37.º do RGPD, é obrigatória a designação de encarregados de proteção de dados nas entidades públicas, de acordo com o disposto nos números seguintes. 2 - Para efeitos do número anterior, entende-se por entidades públicas: a) O Estado; b) As regiões autónomas; c) As autarquias locais e as entidades supranacionais previstas na lei; d) As entidades administrativas independentes e o Banco de Portugal; e) Os institutos públicos; f) As instituições de ensino superior públicas, independentemente da sua natureza; g) As empresas do setor empresarial do Estado e dos setores empresariais regionais e locais; h) As associações públicas. 3 - Independentemente de quem seja responsável pelo tratamento, existe pelo menos um encarregado de proteção de dados: a) 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; b) 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; c) Por cada município, sendo designado pela câmara municipal, com faculdade de delegação no presidente e subdelegação em qualquer vereador; d) 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; e) Por cada entidade, no caso das demais entidades referidas no número anterior, sendo designada pelo respetivo órgão executivo, de administração ou gestão, com faculdade de delegação no respetivo presidente. 4 - Nos termos do n.º 3 do artigo 37.º do RGPD, pode ser designado o mesmo encarregado de proteção de dados para vários ministérios ou áreas governativas, secretarias regionais, autarquias locais ou outras pessoas coletivas públicas. 5 - Cabe a cada entidade a designação do encarregado de proteção de dados, não sendo obrigatório o exercício de funções em regime de exclusividade.6 - O encarregado de proteção de dados

Na administração pública os Encarregados de Proteção de Dados poderão ser trabalhadores em funções públicas ou consultores externos que tem como função principal informar e aconselhar quando ao cumprimento das obrigações relevantes em matéria de proteção de dados.

Figura 18 – Encarregado de Proteção de Dados de 2.º grau



A Administração Regional Açoriana optou pela nomeação de um trabalhador em funções públicas por secretária regional para o exercício de funções de EPD, sendo nomeados por direção regional e institutos públicos regionais um interlocutor que trabalha diretamente com o EPD, assumindo este interlocutor a designação de EPD de segundo grau[167]. Ora, a nomeação de um EPD de segundo grau constitui uma verdadeira

de uma entidade pública que tenha atribuições de regulação ou controlo não pode exercer essas funções simultaneamente em entidade sujeita ao controlo, ou inserida no perímetro regulatório daquela entidade."

[167] A título exemplificativo, no exercício das minhas funções como técnica superior no Instituto de Alimentação e Mercados Agrícolas, fui nomeada por despacho do Grupo de Trabalhos de Implementação do RGPD no SRAF, via e-mail, datado de 1 de agosto de 2018, para integrar o referido grupo na qualidade de Encarregada de Proteção de Dados de 2.º grau.

inovação da Administração Regional, sendo que tal figura não se encontra prevista no RGPD, todavia, foi o modo encontrado para que dentro de cada organismo público exista um colaborador que auxilie o EPD no exercício das suas funções.

Na realidade, o EPD de 2.º grau funciona como um secretário do EPD. No nosso entendimento não deveria ser utilizada a designação de EPD de 2.º grau, mas sim de secretário, de modo a não confundir o público e descredibilizar ou desautorizar o próprio EPD.

Esta inovação regional vem por em causa o próprio RGPD, cujo objetivo primordial é uniformizar a matéria de proteção de dados no território dos Estados-Membros, criando assim uma brecha jurídica que pode por em causa o próprio RGPD, na medida em que o EPD é o único com competências atribuídas para o exercício das funções cometidas por lei.

A opção de nomeação de um trabalhador em funções públicas poderá gerar problemas laborais, uma vez que na maioria das situações as funções de EPD acumulam às funções originárias, sendo que o EPD "não recebe instruções relativamente ao exercício das suas funções (…) não podendo ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções"[168], sendo que quanto às suas funções originárias encontra-se subordinado jurídico, pelo que será necessário definir os limites e contornos dessa nomeação[169].

Embora o RGPD preveja a possibilidade de ser nomeado um único EPD por organismo público, a decisão de nomeação de um único EPD por área governativa poderá, em nossa opinião, originar problemas, dado que o EPD é responsável por uma variedade

[168] *Cfr.* Número 3 do artigo 38.º do RGPD.
[169] Neste sentido, o considerando 97 do RGPD estabelece que os "encarregados de proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência".

de tarefas, o responsável deverá garantir que um único EPD possa realizar o trabalho com eficiência, apesar de ser responsável por várias autoridades públicas.

O EPD deverá ser visto como um membro da organização com uma opinião crítica sobre as atividades de tratamento de dados e, portanto, faz parte dos grupos de trabalho da organização que lida com o tratamento de dados, devendo para o efeito ter um conhecimento bastante amplo da atividade do responsável pelo tratamento. Considerando que dentro de cada área governativa existem diversos serviços, cada um com as suas especificidades, o trabalhador em funções públicas nomeado para EPD deverá obrigatoriamente ter conhecimento das especificidades das várias autoridades ou organismos dentro da sua área governativa, o que poderá demonstrar-se um grande desafio.

O RGPD prevê que o EPD pode exercer outras funções e atribuições. O exercício de outras funções e atribuições implica, todavia, que o responsável pelo tratamento ou subcontratante assegurem que "essas funções e atribuições não resultem num conflito de interesses"[170].

Neste sentido, a IT Governance Privacy Team (2017) esclareceu que "a ausência de conflito de interesses está intimamente ligada ao requisito de agir de maneira independente. Embora os EPD possam ter outras funções, eles só podem ser confiados com outras tarefas e deveres que não causem conflitos de interesses. Em particular, isso significa que o EPD não pode ocupar uma posição dentro da organização que o faça determinar a finalidade e os meios de tratamento de dados pessoais ou a ser responsável

[170] *Cfr*. Número 6 do artigo 38.º do RGPD.

pela prestação de serviços. (…) Em termos gerais, no entanto, isto significa que não é possível para um gestor de IT, CIO[171] ou CISO[172] também ser EPD" (p.69).

Acresce que o RGPD estabelece que este deverá estar "facilmente acessível a partir de cada estabelecimento"[173]. O GT29 (2016) esclarece que "a noção de acessibilidade refere-se às funções do EPD enquanto ponto de contacto em relação aos titulares dos dados, à autoridade de controlo e também, internamente, no seio da organização" (p.25).

A disponibilidade do EPD, seja fisicamente nas instalações da autoridade pública como que se fosse um trabalhador, via linha telefónica direta ou outro meio de comunicação, é essencial para garantir que os titulares dos dados possam facilmente entrar em contato com o EPD.

O RGPD prevê a obrigatoriedade de o responsável pelo tratamento publicar os contactos do EPD da organização, assim como, os contactos da autoridade de controlo, permitindo assim que os titulares dos dados e as autoridades de controlo possam contactar diretamente e confidencialmente o EPD, sem ter de contatar a organização de modo a poder comunicar com o EPD.

Todavia, através de uma pesquisa no portal eletrónico do Governo Regional dos Açores é possível verificar que embora se encontrem publicados alguns despachos de nomeação dos EPD de determinadas secretarias regionais, não se encontram publicitados os contatos dos EPD nomeados pelas mesas, encontrando-se, todavia, disponibilizado um requerimento para o exercício dos direitos do titular de dados[174] e uma ficha informativa dos direitos dos titulares dos dados, que estabelece que "para exercício dos direitos

[171] Por CIO entende-se responsável pela tecnologia da informação da empresa.
[172] Por CISO entende-se Executivo-chefe de segurança de informação.
[173] *Cfr.* Número 2 do Artigo 37.º do RGPD.
[174] *Cfr.* "Requerimento para Exercício dos Direitos do Titular dos Dados", disponível em: http://www.azores.gov.pt/NR/rdonlyres/24100BD0-AA41-4432-92C1-C0D8961BCD3D/0/MinutaRequerimentoDireitos.pdf, consultado a 20/09/2019.

previstos no número anterior deve ser realizado presencialmente pelo titular dos dados no respetivo Serviço, mediante requerimento próprio, apresentando documento de identificação que permita a comprovar inequivocamente da sua identidade"[175].

Por outro lado, nem o RGPD ou o GT29 especificam claramente quais são as qualidades profissionais esperadas para o candidato a EPD.

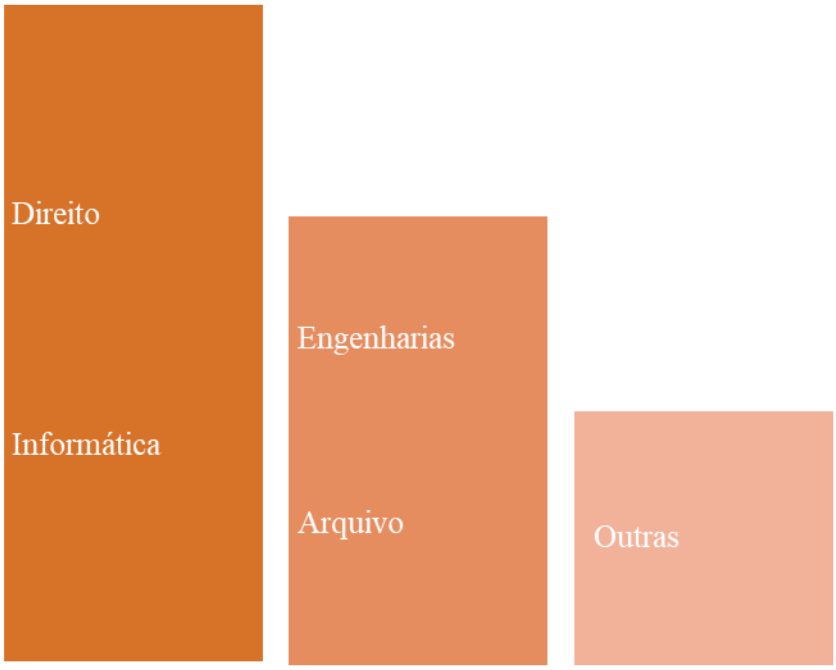
Figura 19 – Qualidades do Encarregado de Proteção de Dados

Neste sentido o GT29 apenas esclarece que as qualidades profissionais exigidas de um EPD deverão ser uma mistura de conhecimentos académicos e experiência profissional na área que o EPD será nomeado, dispondo que "os EPD devem ter competências no domínio das legislações e práticas nacionais e europeias em matéria de

[175] *Cfr.* Resumo direitos do titular dos dados, disponível em: http://www.azores.gov.pt/NR/rdonlyres/7FFE7284-23E3-49F7-A67D-42AF31DDF4D4/0/AnexoDireitosversaoresumida.pdf, consultado a 20/09/2019.

proteção de dados e um conhecimento profundo do RGPD. É igualmente conveniente que as autoridades de controlo promovam formações adequadas e regulares destinadas a EPD. Um conhecimento do setor empresarial e da organização do responsável pelo tratamento afiguram-se útil. O EPD deve também apresentar um bom conhecimento das operações de tratamento efetuadas, bem como dos sistemas de informação, da segurança e das necessidades de proteção de dados do responsável pelo tratamento. No caso das autoridades ou organismos públicos, o EPD deve igualmente ter um conhecimento sólido das regras e dos procedimentos administrativos da organização" (GT29, 2016, p.28).

Figura 20 – Áreas de formação dos Encarregados de Proteção de Dados



Na realidade, dos despachos de nomeação de encarregado de proteção de dados publicados em Jornal Oficial da Região Autónoma dos Açores[176] não é possível aferir a formação profissional dos mesmos, no entanto e considerando o conhecimento interno

[176] Disponível em:https://jo.azores.gov.pt/api/public/jornal/pdfOriginal?numeroJornal=185&ano=2018&serieId=e5b1fb74-7a34-4d76-925a-10f088b27490&suplemento=0, https://jo.azores.gov.pt/api/public/jornal/pdfOriginal?numeroJornal=33&ano=2019&serieId=e5b1fb74-7a34-4d76-925a-10f088b27490&suplemento=0, https://jo.azores.gov.pt/#/ato/121a403f-babe-42df-8f97-9694cc780564, consultado a 27/09/2019.

decorrente do exercício de atividades na administração pública regional a nomeação dos EPD tem sido feita maioritariamente entre indivíduos com formação na área do direito e da informática[177]. Todavia, verificam-se situações excecionais de nomeação de EPD sem formação nas áreas supramencionadas, sendo a sua formação base na área da engenharia, arquivo, *et cetera*[178], sendo que em tais situações a nomeação decorre do reconhecimento de detenção das qualidades profissionais e as aptidões necessárias ao desempenho das inerentes funções pelo responsável pelo tratamento.

Nestes termos, consideramos que a posição de EPD não deverá ser ocupada por iniciantes ou terceiros totalmente alheios ao *modus operandi* da entidade, devendo a nomeação feita por um indivíduo conhecedor da atividade da entidade, possuidor de conhecimentos na área do direito, da proteção de dados e da tecnologia.

3.6 O acesso a documentos administrativos e a proteção de dados pessoais

No contexto da administração pública em Portugal, o novo paradigma de proteção de dados terá, obrigatoriamente, de ser conjugado com o regime de acesso a documentos administrativos, na medida em que o direito de acesso a documentos administrativos poderá entrar em conflito com o direito à proteção de dados pessoais quando o exercício de direito de acesso incida sobre documentos que contenham dados pessoais de terceiros.

Tanto o artigo 11.º[179] da Carta dos Direitos Fundamentais da União Europeia como o artigo 10.º[180] da Convenção Europeia dos Direitos Humanos consagram o direito à

---

[177] A título de exemplo, *vide,* o Encarregado de Proteção de Dados da Universidade dos Açores cuja formação base é na área da informática, tal como o Encarregado de Proteção de Dados da Vice-Presidência do Governo Regional dos Açores. Por sua vez a Secretária Regional da Energia, Ambiente e Turismo e a Secretaria Regional da Solidariedade Social nomearam um EPD cujo área de formação é o Direito (cfr. http://www.vpgr.azores.gov.pt/Sites/cid/EncProtDadosGRA.html, consultado a 29/09/2019).

[178] Infelizmente não nos foi possível encontrar dados estatísticos relativamente às habilitações académicas dos EPD. A figura 20 tem por base o conhecimento pessoal e profissional neste âmbito, por conseguinte, não tem carácter científico mas meramente indicativo.

[179] Artigo 11.º da Carta dos Direitos Fundamentais da União Europeia: ". Todas as pessoas têm direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber e de transmitir informações ou ideias, sem que possa haver ingerência de quaisquer poderes públicos e sem consideração de fronteiras. 2. São respeitados a liberdade e o pluralismo dos meios de comunicação social."

[180] Artigo 10.º da Convenção Europeia dos Direitos Humanos: "1. Qualquer pessoa tem direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber ou de transmitir informações ou ideias sem que possa haver ingerência de quaisquer autoridades públicas e sem considerações de fronteiras. O presente artigo não impede que os Estados submetam as empresas

liberdade de expressão e de informação, estabelecendo que todos têm a liberdade de receber e de transmitir informações, sem que haja ingerências de quaisquer poderes públicos e sem considerações de fronteiras. Esta vertente do direito a receber informações constitui uma concretização da necessária transparência da atividade administrativa numa sociedade democrática, garantindo uma maior participação do cidadão no processo de decisão.

Por sua vez o artigo 15.º do Tratado Sobre o Funcionamento da União Europeia consagra o direito de acesso a documentos oficiais, estabelecendo no seu número 3 que "todos os cidadãos da União e todas as pessoas singulares ou coletivas que residam ou tenham a sua sede estatutária num Estado-Membro têm direito de acesso aos documentos das instituições, órgãos e organismos da União, seja qual for o respetivo suporte, sob reserva dos princípios e condições a definir nos termos do presente número", acrescentado que "os princípios gerais e os limites que, por razões de interesse público ou privado hão-de reger o exercício do direito de acesso aos documentos serão definidos por meio de regulamentos adotados pelo Parlamento Europeu e o Conselho".

Neste sentido, o Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão[181] visa definir os princípios, condições e os limites que, por razões de interesse público ou privado, regem o direito de acesso aos documentos do Parlamento Europeu, do Conselho e da Comissão, de modo a que o acesso aos documentos seja o mais amplo possível, assim como estabelecer normas que garantam a

---

de radiodifusão, de cinematografia ou de televisão a um regime de autorização prévia. 2. O exercício desta liberdades, porquanto implica deveres e responsabilidades, pode ser submetido a certas formalidades, condições, restrições ou sanções, previstas pela lei, que constituam providências necessárias, numa sociedade democrática, para a segurança nacional, a integridade territorial ou a segurança pública, a defesa da ordem e a prevenção do crime, a protecção da saúde ou da moral, a protecção da honra ou dos direitos de outrem, para impedir a divulgação de informações confidenciais, ou para garantir a autoridade e a imparcialidade do poder judicial."

[181] Jornal Oficial nº L 145 de 31/05/2001 p. 0043 – 0048.

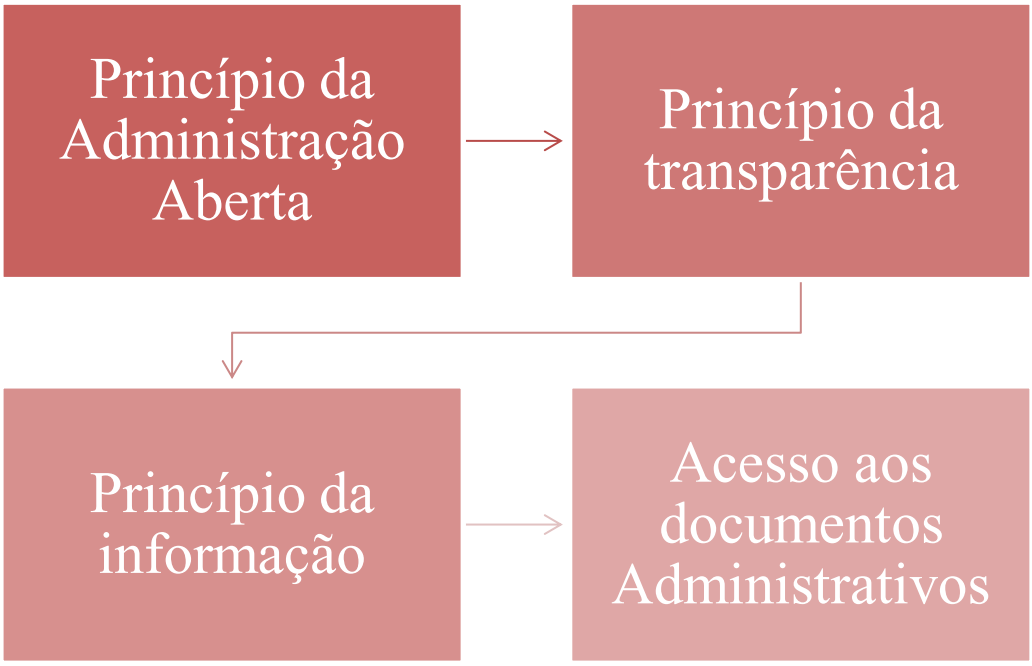
maior facilidade possível do exercício do direito de acesso e promoção de boas práticas administrativas em matéria de acesso aos documentos[182].

A nível nacional, o número 4 do artigo 35.º da CRP consagra que "é proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei"[183], sendo que o RGPD prevê que o tratamento de dados pessoais, onde se inclui o acesso, é legítimo quando se verifique uma das situações do seu artigo 6.º, nomeadamente, quando o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas, o tratamento for necessário para a execução de um contrato, cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito, para a defesa de interesses vitais ou titular dos dados ou de terceiro, quando o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento ou o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiro, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Por sua vez, no ordenamento jurídico português, o acesso a documentos administrativos integra o catálogo constitucional dos direitos e garantias dos administrados, permitindo-se assim o acesso a dados pessoais de terceiros, quando se verifiquem os requisitos da Lei n.º 26/2016, de 22 de agosto[184].

[182] Artigo 1.º do Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio.
[183]Um desses casos excecionais é o que resulta da Lei n.º 64/2013, que regula a obrigatoriedade de publicitação dos benefícios concedidos pela Administração Pública a particulares.
[184] Publicada no Diário da República n.º 160/2016, Série I de 2016-08-22, p. 2777 – 2788.

Figura 21 - Princípios orientadores do acesso aos documentos administrativos



A atuação da Administração Pública portuguesa é vinculada por princípios orientadores da atuação administrativa, que garantem a liberdade de atuação da Administração Pública. Neste sentido, um dos princípios basilares do estado de direito democrático português é o princípio da administração aberta, constituindo, na aceção do Tribunal Constitucional, "um valioso contributo para a superação, do sistema clássico da administração essencialmente burocrático, autoritário, centralizado, fechado sobre si e eivado de secretismo, e significa um decisivo passo na direção da plena democratização da vida administrativa"[185].

O princípio da administração aberta insere-se no novo padrão de atuação da Administração Pública "de negação da *arcana praxis e* sublimação da transparência administrativa, intimamente ligada a outros valores procedimentais, tais como os da participação, imparcialidade, justiça, proporcionalidade"[186].

[185] *Cfr.* Acórdão do Tribunal Constitucional n.º 176/92 – Processo n.º 214/90, DR., II Série, n.º 216, de 18 de setembro de 1992, p. 8775.
[186] *Cfr.* Acórdão do Tribunal Central Administrativo Norte, de 23 de setembro de 2015, processo n.º 01306/15.0BEBRG. Disponível em: http://www.dgsi.pt/jtcn.nsf/-/3DA13F65F20B5EA180257F0100407674, consultado a 23/09/2019.

O princípio da administração aberta encontra-se consagrado no número 2 do artigo 268.º da CRP[187], concretizando-se no direito à informação e no direito à participação na vida pública, direitos estes constitucionalmente consagrados nos artigos 37.º[188] e 48.º[189] da CRP, respetivamente.

O artigo 268.º da Constituição da República Portuguesa, com a epígrafe direitos e garantias dos administrados, consagra o direito à informação administrativa, estipulando que "os cidadãos têm o direito a ser informados pela Administração, sempre que o requeiram, sobre o andamento dos processos em que sejam diretamente interessados, bem como de conhecer as resoluções definitivas que sobre eles forem tomadas", acrescentando o número 2 do artigo 268.º da CRP que "os atos administrativos de eficácia externa estão sujeitos a notificação aos interessados, quando não tenham de ser oficialmente publicado, e carecem de fundamentação expressa quando afetem diretos ou interesses legalmente protegidos dos cidadão".

Por sua vez, o Código do Procedimento Administrativo no seu artigo 18.º consagra o direito de todos os particulares à proteção dos dados pessoais, assim como o direito à segurança e integridade dos suportes, sistemas e aplicações utilizados para o efeito, consagrando igualmente no seu artigo 17.º o princípio da administração aberta, que atribui a todas as pessoas o direito de acesso aos arquivos e registos administrativos, "mesmo

---

[187] Artigo 268.º da Constituição da República Portuguesa – "Direitos e garantias dos administrados. 1. Os cidadãos têm o direito de ser informados pela Administração, sempre que o requeiram, sobre o andamento dos processos em que sejam diretamente interessados, bem como o de conhecer as resoluções definitivas que sobre eles forem tomadas. 2. Os atos administrativos de eficácia externa estão sujeitos a notificação aos interessados, quando não tenham de ser oficialmente publicados, e carecem de fundamentação expressa quando afetem direitos ou interesses legalmente protegidos dos cidadãos. 3. É garantido aos interessados recurso contencioso, com fundamento em ilegalidade, contra quaisquer atos administrativos definitivos e executórios, independentemente da sua forma, bem como para obter o reconhecimento de um direito ou interesse legalmente protegido."

[188] Artigo 37.º da Constituição da República Portuguesa – "Liberdade de expressão e informação. 1 – Todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, pela imagem ou por qualquer outro meio, bem como o direito de se informar, sem impedimentos nem discriminações. 2 – O exercício destes direitos não pode ser impedido ou limitado por qualquer tipo ou forma de censura. 3 – As infrações cometidas no exercício destes direitos ficarão submetidas ao regime de punição da lei geral, sendo a sua apreciação da competência dos tribunais judiciais. 4 – A todas as pessoas, singulares ou coletivas, é assegurado, em condições de igualdade e eficácia, o direito de resposta."

[189] Artigo 47.º da Constituição da República Portuguesa – "Participação na vida pública. 1- Todos os cidadãos têm o direito de tomar parte na vida política e na direção dos assuntos públicos do país, diretamente ou por intermédio de representantes livremente eleitos. 2 – Todos os cidadãos têm o direito de ser esclarecidos objetivamente sobre atos do Estado e demais entidades públicas e de ser informados pelo Governo e outras autoridades acerca da gestão dos assuntos públicos."

quando nenhum procedimento que lhes diga respeito esteja em curso, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal, ao sigilo fiscal e à privacidade das pessoas"[190], constituindo "um dos pilares da República sobre o qual assenta um conjunto vasto de direitos, liberdades e garantias dos cidadãos, quer seja entendido no seu âmbito mais restrito – de acesso aos documentos, dados e processos administrativos-, quer seja compreendido no seu âmbito mais vasto – que inclui também a divulgação ativa e de forma acessível de documentos, dados e informação por parte da Administração Pública, bem como políticas de promoção da participação pública"[191].

Também o artigo 2.º[192] da 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, transpondo a Diretiva 2003/4/CE, do Parlamento Europeu e do Conselho, de 28 de janeiro, e a Diretiva 2003/98/CE, do Parlamento Europeu e do Conselho, de 17 de novembro, doravante designada por LADA, prevê o princípio da administração aberta, estipulando que o acesso e a reutilização da informação administrativa deverá ser garantida de acordo com os princípios da atividade administrativa, designadamente os princípios da igualdade, da proporcionalidade, da justiça, da imparcialidade e da colaboração com os particulares.

Todavia, para que seja alcançada uma autêntica administração aberta, é necessário que seja acautelada a transparência administrativa e o direito à informação dos cidadãos.

---

[190] Artigo 17.º do Código do Procedimento Administrativo.

[191] Exposição de Motivos da Proposta de Lei n.º 18/XII, disponível em http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c7561573570 59326c6864476c3259584d7657456c4a535339305a58683062334d76634842734d54677457456c4a5353356b62324d3d&fich=ppl18-XIII.doc&Inline=true, consultado a 8/08/2019.

[192] Artigo 2.º da LADA Princípio da administração aberta – "1- O acesso e a reutilização da informação administrativa são assegurados de acordo com os demais princípios da atividade administrativa, designadamente os princípios da igualdade, da proporcionalidade, da justiça, da imparcialidade e da colaboração com os particulares. 2 – A informação pública relevante para garantir a transparência da atividade administrativa, designadamente a relacionada com o funcionamento e controlo da atividade pública, é divulgada ativamente, de forma periódica e atualizada, pelos respetivos órgãos e entidades. 3 – Na divulgação de informação e na disponibilização de informação para reutilização através da Internet deve assegurar-se a sua compreensibilidade, o acesso e universal, bem como a acessibilidade, a interoperabilidade, a qualidade, a integridade e a autenticidade dos dados publicados e ainda a sua identificação e localização."

Embora a Constituição da República Portuguesa não consagre o princípio da transparência enquanto princípio fundamental da Administração Pública, diversa legislação em matéria administrativa alude à transparência, contudo, e na aceção de Fernandes (2015) "a multiplicidade de referências legais à ideia de transparência no quadro do direito administrativo aponta no sentido de que a mesma, ao ser expressamente acolhida como valor ou interesse a proteger e promover, como fim em si mesmo, ao ser expressamente acolhida como valor ou interesse a proteger e promover com fim em si mesmo, pode assumir a natureza de verdadeiro princípio normativo. Neste sentido, não são raros os autores que, na doutrina nacional, enxergam a existência de um princípio da transparência administrativa", sendo que o princípio da transparência administrativa "impõe a visibilidade e proíbe a opacidade do funcionamento e da atuação da Administração. Numa outra formulação, o princípio da transparência obriga a que a organização e o procedimento administrativos estejam regulados e ordenados, por um lado, e que a Administração sempre se comporte, por outro, de tal modo que seja permitido ver para dentro da Administração" (p.436).

Por sua vez, o direito à informação, direito constitucionalmente consagrado[193], no direito administrativo ergue-se ao abrigo do princípio da colaboração com os particulares[194], que estipula que os órgão da Administração Pública devem atuar em estreita colaboração com os particulares, cumprindo-lhes prestar aos particulares as informações e os esclarecimentos de que careçam, e do princípio da participação, que consagra a obrigatoriedade de os órgãos da Administração Pública assegurarem a

[193] Artigo 37.º da CRP "Liberdade de expressão e de informação. 1 – Todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, pela imagem ou por qualquer outro meio, bem como o direito de se informar, sem impedimentos nem discriminações. 2 – O exercício destes direitos não pode ser impedido ou limitado por qualquer tipo ou forma de censura. 3 – As infrações cometidas no exercício destes direitos ficarão submetidas ao regime de punição da lei geral, sendo a sua apreciação da competência dos tribunais judiciais. 4 – A todas as pessoas singulares ou coletivas, é assegurado, em condições de igualdade e eficácia, o direito de resposta."

[194] Artigo 11.º do CPA "Princípio da colaboração com os particulares. 1 – Os órgãos da Administração Pública devem atuar em estreita colaboração com os particulares, cumprindo-lhes, designadamente, prestar aos particulares as informações e os esclarecimentos de que careçam, apoiar e estimular as suas iniciativas e receber as suas sugestões e informações. 2 – A Administração Pública é responsável pelas informações prestadas por escrito aos particulares, ainda que não obrigatórias."

participação dos procedimentos na formação das decisões que lhes digam respeito[195], traduz-se, no âmbito do direito administrativo, nos direitos dos interessados de serem informados sobre o andamento dos procedimentos que lhes digam diretamente respeito, bem como o direito de conhecer as resoluções definitivas que sobre eles forem tomadas[196], sendo que o direito à informação estende-se a qualquer pessoa que prove um interesse legítimo no conhecimento dos elementos que pretendam[197], traduzindo-se em um autêntico direito subjetivo, concernente aos atos e factos que consubstanciam a tramitação do procedimento administrativo, visando precaver o conhecimento dos particulares das posições e decisões da Administração Pública.

Como decorrência do princípio da administração aberta, a todos os cidadãos é reconhecido o direito de acesso a documentos administrativos, quer se encontre ou não em curso um procedimento administrativo em que seja diretamente interessado[198].

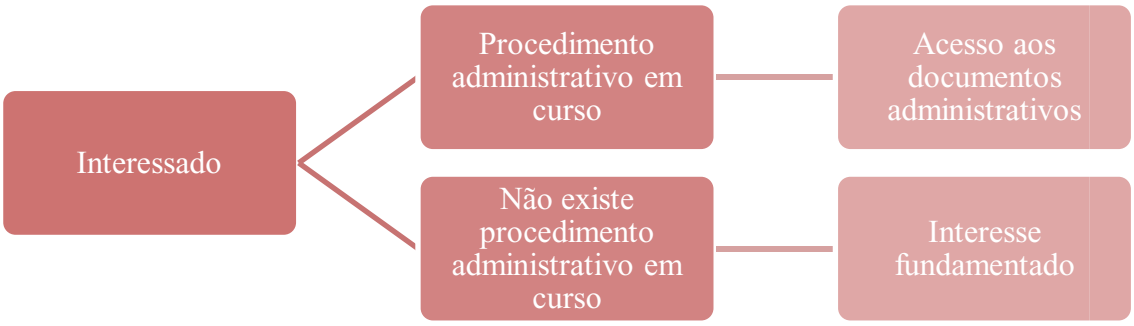
Figura 22 – Acesso a documentos administrativos.

[195] Artigo 12.º do CPA "Princípio da participação. Os órgãos da Administração Pública devem assegurar a participação dos particulares, bem como das associações que tenham por objeto a defesa dos seus interesses, na formação das decisões que lhes digam respeito, designadamente através da respetiva audiência nos termos do presente Código."

[196] Artigo 82.º do CPA "Direito dos interessados à informação. 1 – Os interessados têm o direito de ser informados pelo responsável pela direção do procedimento, sempre que o requeiram, sobre o andamento dos procedimentos que lhes digam diretamente respeito, bem como o direito de conhecer as resoluções definitivas que sobre eles forem tomadas. 2 – As informações a prestar abrangem a indicação do serviço onde o procedimento se encontra, os atos e diligências praticados, as deficiências a suprir pelos interessados, as decisões adotadas e quaisquer outros elementos solicitados. 3 – As informações a prestar abrangem a indicação do serviço onde o procedimento se encontra, os atos e diligências praticados, as deficiências a suprir pelos interessados, as decisões adotadas e quaisquer outros elementos solicitados. 4 – Nos procedimentos eletrónicos, a Administração deve colocar à disposição dos interessados, na internet, um serviço de acesso restrito, no qual possam, mediante prévia identificação, obter por via eletrónica a informação sobre o estado de tramitação do procedimento. 5 – Salvo disposição legal em contrário, a informação eletrónica sobre o andamento dos procedimentos abrange os elementos mencionados no n.º 2."

[197] Artigo 85.º do CPA "Extensão do direito à informação. 1 – Os direitos reconhecidos nos artigos 82.º a 84.º são extensivos a quaisquer pessoais que provem ter interesse legítimo no conhecimento dos elementos que pretendam. 2 – O exercício dos direitos previstos no número anterior depende de despacho do dirigente do serviço, exarado em requerimento escrito, instruído com os documentos probatórios do interesse legítimo invocado."

[198] Neste sentido referem Amorim & Oliveira (2010) que "todas as pessoas cuja esfera jurídica resulta alterada pela própria instauração do procedimento ou aquelas que saiam (ou sairão provavelmente) beneficiadas ou desfavorecidas nessa sua esfera pela respectiva decisão final" têm acesso a documentos administrativos, não confidenciais, acrescentando ainda que "qualquer interesse atendível, protegido ou não proibido juridicamente que justifique, razoavelmente, dar-se ao requerente informação" (p.328 e 340).



Existindo um procedimento administrativo em curso, o direito de acesso a documentos administrativos compõe uma garantia do direito à informação, na medida em que no decurso de um procedimento administrativo, o cidadão interessado tem o direito a ser informado da marcha procedimental, seja por escrito ou oralmente, assim como o direito de consultar o mesmo, com todos os documentos e registos administrativos que o constituam, bem como, de obter certidões, desde que não reverenciem a segurança interna e externa, investigação criminal e a intimidade das pessoas[199]. Neste sentido, o direito à informação e o direito de acesso aos documentos administrativos são dois direitos distintos estritamente interligados, devendo ser interpretados e dissecados concomitantemente.

Não existindo um procedimento administrativo em curso que diga respeito diretamente ao cidadão, mas este detenha fundamentado interesse em conhecer o procedimento administrativo, deverá ser chamado à colação o número 2 do artigo 268.º da CRP, tratando-se de um "preceito material *self executing*, que contém um núcleo

[199] Acórdão do Tribunal Constitucional n.º 176/92 – Processo n.º 214/90, DR., II Série, n.º 216, de 18 de setembro de 1992, p. 8775.

efetivo ou operativo por si próprio e que pode ser oposto a Administração Pública por aquele cidadão, independentemente de expressão previsão ou regulamentação legal"[200].

Por sua vez, o direito de acesso aos documentos administrativos não aliena por si só o direito à proteção de dados, ou seja, o direito de acesso a documentos administrativos não compõe um direito absoluto e ilimitado, podendo sofrer restrições, nomeadamente no que concerne à reserva da intimidade da vida privada, todavia, e considerando a extensão do regime jurídico dos direitos, liberdades e garantias ao direito de acesso a documentos administrativos, enquanto direito fundamental de natureza análoga, nos termos dos artigos 17.º e 18.º da CRP, "as restrições admissíveis têm, designadamente, de ser constitucionalmente autorizadas, explicitadas por lei, conter-se nos limites do princípio da proporcionalidade e ser aplicadas nos seus estritos termos" (Provedor de Justiça, 2006).

Uma das mais chamadas à colação restrições ao direito de acesso aos documentos administrativos é a decorrente da reserva da intimidade da vida privada e familiar. O artigo 26.º da CRP consagra que a todos os indivíduos é reconhecida a reserva da intimidade da vida privada e familiar, traduzindo-se este, na aceção do Tribunal Constitucional, "no direito de cada um a ver protegido o espaço interior ou familiar da pessoa ou do seu lar contra intromissões alheias", correspondendo a uma "esfera própria inviolável, onde ninguém deve poder penetrar sem autorização do respetivo titular" compreendendo "a autonomia, ou seja, o direito a ser o própria a regular, livre de ingerências estatais e sociais, essa esfera de intimidade; o direito a não ver difundido o que é próprio dessa esfera de intimidade, a não ser mediante autorização do

[200] *Idem.*

interessado"[201]. Nestes termos, o direito à reserva da intimidade da vida materializa-se na impossibilidade de acesso e divulgação de dados pessoais de terceiros.

O direito à reserva da intimidade da vida privada encontra-se igualmente consagrado em diversos diplomas europeus e internacionais, nomeadamente no artigo 12.º da Declaração Universal dos Direitos do Homem, artigo 8.º da Convenção Europeia dos Direitos do Homem, assim como nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, constituindo um direito especial de personalidade nos termos do Código Civil, encontrando-se fora do escopo de aplicação do artigo 70.º do Código Civil que dispõem sobre a tutela geral dos direitos de personalidade, encontra-se, por sua vez, consagrado no artigo 80.º do referido diploma.

Perante situações de conflito entre o direito de acesso e o direito à reserva da intimidade da vida privada deverá atender-se à finalidade, sendo que só são legitimados sacrifícios do direito fundamental do direito de acesso aos arquivos e registos administrativos perante direitos e valores constitucionais de igual ou superior valor, designadamente, relativos à segurança interna e externa, à investigação criminal e à reserva da intimidade da vida privada[202].

Uma das herméticas questões associadas ao direito de acesso aos documentos administrativos e ao direito à proteção de dados pessoais é a do conceito de interessado, na medida que a definição ampla de interessado poderá potencialmente gerar situações de violações de dados pessoais.

O artigo 67.º do Código de Procedimento Administrativo preceitua que "os particulares têm o direito de intervir pessoalmente no procedimento administrativo ou de

---

[201] Acórdão do Tribunal Constitucional n.º 128/92 - Processo: n.º 260/90, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19920128.html, consultado a 06/07/2019.

[202] Acórdão do Supremo Tribunal Administrativo, de 24/01/2012, processo n.º 0668/11, disponível em: http://www.dgsi.pt/jsta.nsf/35fbbbf22e1bb1e680256f8e003ea931/5d83b3dc6602348280257996005 9b84c?OpenDocument&ExpandSection=1, consultado a 06/07/2019.

nele se fazer representar ou assistir através de mandatário", acrescentando o artigo 68.º do referido código que "têm legitimidade para iniciar o procedimento ou para nele se constituírem como interessados os titulares de direitos, interesses legalmente protegidos, deveres, encargos, ónus ou sujeições no âmbito das decisões que nele forem ou possam ser tomadas, bem como as associações, para defender interesses coletivos ou proceder à defesa coletiva de interesses individuais dos seus associados que caibam no âmbito dos respetivos fins". A definição de interessado do CPA é bastante ampla, o que poderá originar problemas em matéria de proteção de dados pessoais.

Assim, e de modo a que a proteção dos dados pessoais seja acautela, não deverá bastar um interesse legítimo, devendo o princípio da transparência e o direito a acesso a documentos administrativos conjugar o interesse com as finalidades de tratamento, assim como com o artigo 6.º do RGPD, que define os fundamentos de licitude de tratamento de dados pessoais.

3.6.1 O acesso a documentos administrativos nominativos

A Lei n.º 26/2016, de 22 de agosto, doravante denominada por LADA, classifica como documento administrativo qualquer conteúdo que esteja na posse ou seja detido em nome dos órgãos e entidades estabelecidas no artigo 4.º do referido diploma[203], seja o suporte de informação sob forma escrita, visual, sonora, eletrónica ou outra forma material[204], excluindo-se do conceito de documento administrativo as notas pessoais, esboços, apontamentos, comunicações eletrónicas pessoais e outros registos de natureza

[203] O Acórdão do Supremo Tribunal de Justiça proferido no âmbito do processo n.º 0758/11 esclarece que "*para que um documento seja considerado "documentos administrativo" para efeitos da alínea a) do n.º 1 dp referido art. 3.º daquela Lei, não se exige que ele esteja conexionado com alguma das atividades administrativas, bastando que ela esteja na posse dos órgãos e entidades referidos no artigo seguinte, ou detidos em seu nome*".

[204] Alínea a) do número 1 do artigo 3.º da Lei n.º 26/2016, de 22 de agosto: "«Documento administrativo» qualquer conteúdo, ou parte desse conteúdo, que esteja na posse ou seja detido em nome dos órgãos e entidades referidas no artigo seguinte, seja o suporte de informação sob forma escrita, visual, sonora, eletrónica ou outra forma material, neles se incluindo, designadamente, aqueles relativos a; i) Procedimentos de emissão de atos e regulamentos administrativos; ii) Procedimentos de contratação pública, incluindo os contratos celebrados; iii) Gestão orçamental e financeira dos órgãos e entidades; iv) Gestão de recursos humanos, nomeadamente os dos procedimentos de recrutamento, avaliação, exercício do poder disciplinar e quaisquer modificações das respetivas relações jurídicas".

semelhante, qualquer que seja o seu suporte, os documentos cuja elaboração não releve da atividade administrativa, ou os documentos produzidos no âmbito das relações diplomáticas do Estado português[205], qualificando como documentos nominativos os documentos administrativos que contenham dados pessoais, definidos nos termos do regime legal de proteção de dados pessoais[206].

O Acórdão do Supremo Tribunal Administrativo no processo n.º 0758/11 esclarece que "para que um documento seja considerado documento administrativo (…) não se exige que ele esteja conexionado com alguma das atividades administrativas, bastando que esteja na posse dos órgãos e entidades referidos no artigo seguinte, ou detidos em seu nome"[207].

O regime de acesso aos documentos administrativos encontra-se consagrado no artigo 5.º da LADA, estipulando que "todos, sem necessidade de enunciar qualquer interesse, têm o direito de acesso aos documentos administrativos, o qual compreende os direitos de consulta, de reprodução e de informação sobre a sua existência e conteúdo", assim, a regra geral no regime de acesso aos documentos administrativos é a do livre acesso dos cidadãos aos documentos administrativos, não devendo esse direito ficar prejudicado pela integração dos documentos administrativos em arquivo corrente, intermédio ou definitivo.

Todavia, o artigo 6.º do referido diploma consagra as restrições ao direito de acesso por terceiros, referindo as limitações de acesso a documentos nominativos[208],

---

[205] Número 2 do artigo 3.º da Lei n.º 26/2016, de 22 de agosto.
[206] Alínea b) do número 1 do artigo 3.º da Lei n.º 26/2016, de 22 de agosto.
[207] Disponível em: http://www.dgsi.pt/jsta.nsf/-/DB1D78475C15829D802578FF003EE3CB, consultado a 23/09/2019.
[208] A CADA no seu Parecer n.º 241/2013 classificou os dados nominativos, estabelecendo que "no quadro da LADA, serão de classificar nessa categoria os que revelem informação do foro íntimo de um indivíduo, como, por exemplo, a sua informação genética ou de saúde, a que se prenda com a sua vida sexual, a relativa às suas convicções ou filiações filosóficas, políticas, religiosas, partidárias ou sindicais, a que contenha opiniões sobre a pessoa, designadamente quando expressas em processos de averiguações, de inquérito ou disciplinares, ou a que traduza descontos no respetivo vencimento, feitos não *ope legis*, mas *ope voluntatis* ou na sequência de decisão judicial. Assim, não são documentos nominativos aqueles que apenas revelem o nome, a filiação, os números de bilhete de identidade ou de contribuinte fiscal; como também os curricula vitae, elaborados pelos próprios titulares e descrevendo as respetivas habilitações académicas e qualificações profissionais, não revestem, por regra, carácter nominativo. De igual forma, porque abonadas em obediência a critérios legais, não têm natureza nominativa as remunerações ilíquidas auferidas pelos servidores

estabelecendo que um terceiro apenas terá direito de acesso a documentos nominativos nos casos em que "estiver munido de autorização escrita do titular dos dados que seja explícita e específica quanto à sua finalidade e quanto ao tipo de dados a que quer aceder, se demonstrar fundamentadamente ser titular de um interesse direto, pessoal, legítimo e constitucionalmente suficientemente relevante, após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, que justifique o acesso à informação"[209].

Nas situações em que os documentos nominativos são comunicados a terceiros, não podem os mesmos ser utilizados ou reproduzidos de forma incompatível com a autorização concedida, com o fundamento de acesso, com a finalidade determinante da recolha ou com o instrumento de legalização, sob pena de responsabilidade por perdas e danos e responsabilidade criminal[210].

Para além das restrições relativas aos documentos nominativos, a LADA consagra diversas restrições ao direito de acesso aos documentos administrativos no seu artigo 6.º, nomeadamente, nas situações de documentos que contenham informações cujo conhecimento ponha em risco interesses fundamentais do Estado, designadamente, situações de segredo de Estado, documentos protegidos por direitos de autor ou direitos conexos, nomeadamente, propriedade literária, artística, industrial, cientifica e intelectual, documentos administrativos preparatórios de uma decisão, conteúdo de auditorias, inspeções, inquéritos, sindicâncias ou averiguações, segredos comerciais, industriais ou sobre empresas.

---

do Estado ou de outras entidades públicas, nem mesmo as remunerações líquidas, desde que, sobre elas, apenas incidam os descontos a que a lei obriga" (disponível em: http://www.utap.pt/CADA/img-X22165832-0001.pdf, consultado a 20/08/2019).

[209] Número 5 do artigo 6.º da Lei n.º 26/2016, de 22 de agosto.

[210] Número 2 do artigo 8.º da Lei n.º 26/2016, de 22 de agosto.

Estabelece o n.º 8 do artigo 6.º da LADA que os documentos administrativos sujeitos a restrições de acesso devem ser objeto de comunicação parcial quando se demonstre possível a expurgação da informação relativa à matéria reservada. Nestes termos, mesmo que um terceiro demonstre um interesse legítimo, não deverá ser concedido acesso ilimitado, devendo ser expurgados os dados pessoais cujo conhecimento não se demonstre abrangido pela finalidade invocada.

Considerando que o interesse legítimo consiste num conceito impreciso, abrangendo uma variedade de interesses, nomeadamente, económicos e financeiros do cidadão, a sua definição consiste num verdadeiro poder discricionário da entidade pública, que deverá pesar os bens jurídico constitucionais conflituantes, ponderando a vantagem que o cidadão pretende obter e o princípio da administração aberta e os direitos, liberdades e garantias de reserva de intimidade da vida privada e de proteção de dados, competindo às entidades públicas a quem é requerido o acesso a determinados documentos administrativos o poder de permitir o acesso a documentos nominativos, devendo basear a sua decisão em critérios de proporcionalidade e de razoabilidade, todavia, muitas vezes tutela-se a curiosidade.

À problemática da definição discricionária do que compõe um interesse legítimo, acresce a circunstância de tanto a CNPD (Comissão Nacional de Proteção de Dados) como a CADA (Comissão de Acesso a Documentos Administrativos) consideram-se habilitadas para se pronunciar sobre o acesso a dados pessoais, gerando dificuldades na perceção do regime legal aplicável, assim como o facto de ao contrário do disposto na LADA, a Lei de Proteção de Dados Pessoais no seu artigo 6.º fazer depender o tratamento de dados pessoais, onde se inclui o acesso por terceiros na aceção do RGPD, do consentimento inequívoco do seu titular ou da necessidade para execução de contrato, para cumprimento de obrigações legais a que o responsável pelo tratamento se encontre

sujeito, para proteção de interesses vitais do titular de dados quando este seja incapaz de dar o seu consentimento, assim como para execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados, ou para prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro, desde que não devam prevalecer os direitos, liberdades e garantias do titular dos dados, estabelecendo como regra geral a proibição de tratamento de dados sensíveis no seu artigo 7.º.

A Comissão de Acesso a Documentos Administrativos (CADA), nos termos do artigo 28.º da Lei n.º 26/2016, de 22 de agosto, compõe uma entidade administrativa independente, que funciona junto da Assembleia da República, a quem cabe zelar pelo cumprimento das disposições da Lei n.º 26/2016, de 22 de agosto, competindo-lhe, entre outras, apreciar as queixas que lhe sejam apresentadas nos termos dos artigos 16.º a 26.º da referida lei e emitir pareceres sobre o acesso a documentos administrativo.

Figura 23 - Processos iniciados e findos no período de 2016 a 2018 da atividade da CADA.

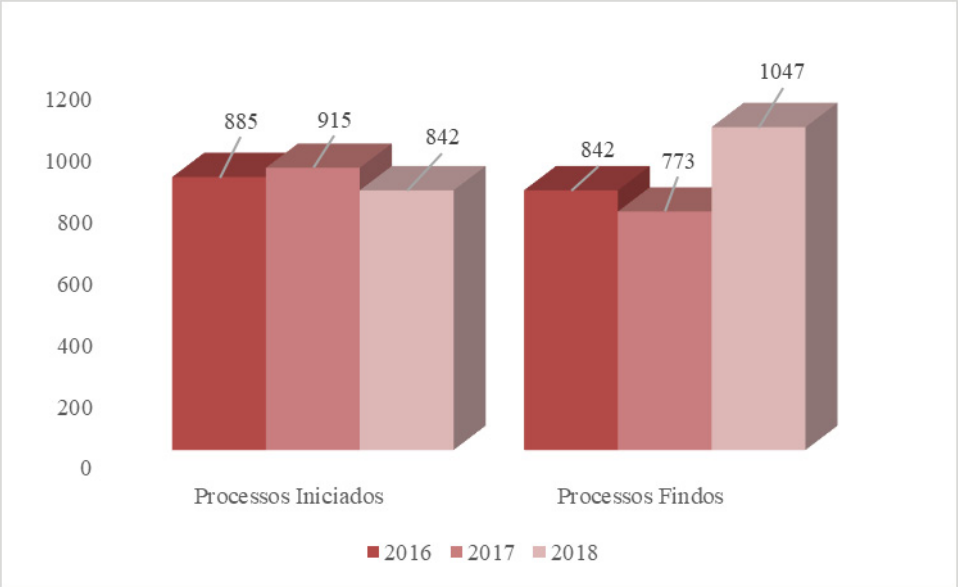
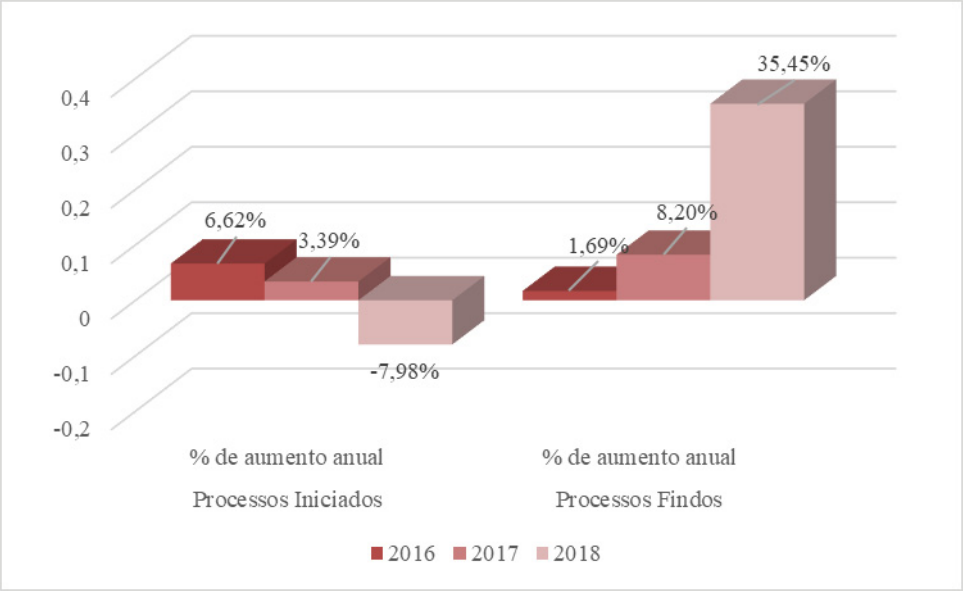


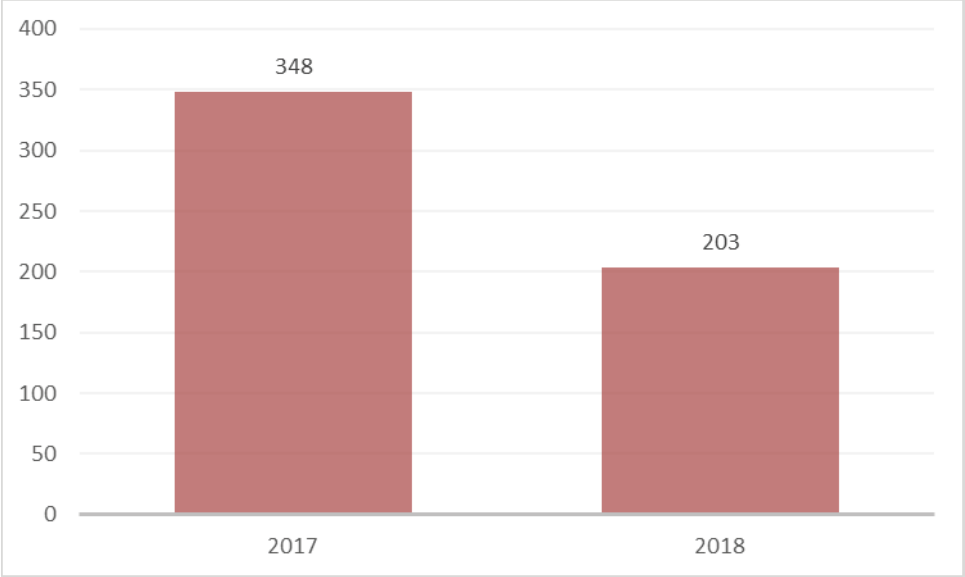
Figura 24 - Percentagem de acréscimo e decréscimo anual no período de 2016 a 2018 da atividade da CADA.



Em 2018 a CADA iniciou 842 processos, menos 7,98% que em 2017, e findado 1047 processos, mais 35,45% do que em 2017. Dos 842 processos abertos 672 reportam-se a queixas e 164 a pedidos de parecer sobre específicas pretensões de acesso a documentos administrativos e 6 a outras matérias (Comissão de Acesso aos Documentos Administrativos, 2018).

Por sua vez em 2017 foram abertos pela CADA 904 novos processos, tendo sido reabertos 11, resultando num total de 915 processos aberto. Dos 915 processos abertos, 629 reportam-se a queixas decorrentes de denegação total ou parcial de acesso, 284 de pedidos de parecer relativos a dúvidas manifestadas por entidades da Administração Pública sobre a possibilidade de ser facultado o acesso a documentos administrativos e 3 a outras situações (Comissão de Acesso aos Documentos Administrativos, 2017).

Figura 25 - Pareceres sobre proteção de dados.



No que concerne ao número de pareceres emitidos, verificou-se que em 2017 foram emitidos 348 sobre a proteção de dados pessoais, sendo que em 2018 foram emitidos 203 pareceres sobre o RGPD.

Dos dados supra é possível aferir que o RGPD não teve um efeito direto no número de queixas e pedidos de pareceres à CADA, verificando-se, na realidade, uma diminuição do número de pareceres relacionados com a proteção de dados.

Demonstrava-se relevante fazer a comparação entre 2018 e 2019 na presente dissertação de modo a analisar a existência de impacto pelo RGPD, no entanto, até ao momento ainda não foram publicados dados referentes ao ano de 2019.

Por sua vez, a Comissão Nacional de Proteção de Dados (CNPD), nos termos do artigo 21.º da Lei n.º 67/98, de 26 de outubro, é uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da

República, que tem como atribuição controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais[211].

A CNPD na sua Deliberação n.º 241/2014, que sugeria à Assembleia da República a revisão da Lei n.º 46/2004, de 24 de agosto, que foi revogada pela Lei n.º 26/2016, de 22 de agosto, teceu duras críticas ao regime de acesso aos documentos administrativos, que mantém a sua pertinência no quadro legal atual.

Nestes termos, a CNPD na referida deliberação censurou a não regulação dos direitos de informação, retificação, atualização e oposição, o acesso por terceiros a dados pessoais contidos em documentos, considerando tal acesso inconstitucional na medida que a Constituição da República Portuguesa proíbe no número 4 do artigo 35.º o acesso a dados pessoais de terceiros, a ausência de definição de um regime mais restrito no que concerne aos dados sensíveis, assim como, os meros interesses pessoais, diretos e legítimos que traduzem em vantagens económicas em oposição a direitos, liberdades e garantias e o facto de serem as próprias entidades a decidir autorizar o acesso a documentos administrativos que contêm dados pessoais. Salientando ainda o facto de o objetivo primordial da LADA ser "assegurar um controlo pelos cidadãos das decisões administrativas, prevenindo por esta via atuações administrativas parciais ou inquinadas de vício de desvio de poder. E para tal controlo, os cidadãos não precisam, por regra, de conhecer, de ter acesso a informação individualizada ou individualizável; na generalidade das situações, será suficiente o conhecimento dos dados anonimizados" (Comissão Nacional de Proteção de Dados, 2014).

Por sua vez, a CADA emitiu o parecer n.º 132/2014, de 8 de abril de 2014, sobre a deliberação n.º 241/2014, salientado que o direito de acesso aos arquivos e registos

[211] Artigo 22.º da Lei n.º 67/98, de 26 de outubro.

administrativos constitui um direito fundamental de natureza análoga aos direitos, liberdades e garantias, assim como a competência exclusiva da CADA para se pronunciar sobre o acesso a documentos administrativos, em geral, e, em especial, a documentos nominativos, afastando a competência da CNPD na matéria.

Diversas são as situações em que a CNPD e a CADA se contradizem, em que a CNPD entende que não deverá ser facultado o acesso a documentos que contenham dados pessoais de terceiros, considerando muitas vezes que as autorizações escritas, condição *sine qua none* da LADA, não cumprem com os requisitos de um consentimento livre, por exemplo, por o clausulado contratual não ser negociável na integra. Contrariamente, a CADA emite parecer favorável ao acesso em todas as situações que se verifiquem as condições estipuladas no número 5 do artigo 6.º da LADA, nomeadamente, autorização escrita ou interesse direto, pessoal e legítimo suficientemente relevante segundo o princípio da proporcionalidade.

Deste modo, o RGPD deverá ser interpretado e aplicado em coordenação com a legislação nacional na matéria, que consente o acesso aos documentos administrativos, nomeadamente o CPA e a LADA, não devendo ser encarado como uma proibição geral de acesso a documentos administrativos nominativos, na medida em que a legislação do Estado-Membro prevê o acesso a esses documentos, existindo um fundamento de licitude nos termos do artigo 6.º do RGPD, nomeadamente, obrigação jurídica.

Na realidade, o RGPD acautela o acesso dos interessados aos documentos administrativos no seu capítulo IX referente a disposições relativas a situações específicas de tratamento, na medida em que o acesso do público aos documentos oficiais pode ser considerado de interesse público, devendo as legislações dos Estados-Membros conciliar o acesso do público aos documentos oficiais e a reutilização da informação do setor

público com o direito à proteção dos dados pessoais[212], estipulando no seu artigo 86.º que os "dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para a prossecução de atribuições de interesse público podem ser divulgados pela autoridade ou organismo nos termos do direito da União ou do Estado-Membro (…) a fim de conciliar o acesso do público a documentos oficiais com o direito à proteção dos dados pessoais" nos termos do RGPD.

Esclarece o considerando 154 do RGPD que o regulamento pondera o princípio do direito de acesso do público aos documentos oficiais na aplicação do mesmo, estipulando que "o acesso do público aos documentos oficiais pode ser considerado de interesse público. Os dados pessoais que constem de documentos na posse dessas autoridades públicas ou organismos públicos deverão poder ser divulgados publicamente por tais autoridades ou organismos, se a divulgação estiver prevista no direito da União ou do Estado-Membro que lhe for aplicável. Essas legislações deverão conciliar o acesso do público aos documentos oficiais e a reutilização da informação do setor público com o direito à proteção dos dados pessoais e podem, pois, prever a necessária conciliação com esse mesmo direito nos termos do presente regulamento".

Nestes termos, somente porque um documento administrativo contenha dados pessoais, tal não deverá significar que constitui informação fora do domínio público[213], sendo que o acesso é permitido no quadro das finalidades que justificam ou do fundamento legítimo previsto na lei.

Todavia, e conforme resulta do RGPD, há que distinguir, na categoria de dados pessoais, entre os dados pessoais gerais e os dados pessoais sensíveis.

---

[212] Considerando 154 do RGPD.

[213] Neste sentido *vide* Acórdão do Tribunal Europeu dos Direitos do Homem, de 8 de novembro de 2016, processo n.º 18030/11, disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-167828%22]}, consultado a 25/09/2019.

Por sua vez, a Lei n.º 58/2019, de 8 de agosto no seu artigo 26.º estabelece que o acesso a documentos administrativos "que contenham dados pessoais rege-se pelo disposto na Lei n.º 26/2016, de 22 de agosto", tendo aditado um número 9 ao artigo 6.º da Lei n.º 26/2016, de 22 de agosto, convencionando 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 técnica, 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 indicativo pelo requerente, que o pedido se fundamenta no direito de acesso a documentos administrativos".

Assim, sempre que os dados nominativos não contenham dados sensíveis e o pedido de acesso a dados pessoais não seja fundamentado, deverá presumir-se que o pedido se fundamenta no direito de acesso a documentos administrativos.

Neste sentido, não devem as entidades públicas, em cumprimento do RGPD, proibir o acesso dos cidadãos a documentos nominativos, assim como, por excesso de zelo, a título de exemplo, expurgar dados pessoais aquando da publicação dos contratos obrigatória no portal Base.gov, sendo que no caso em concreto adotam a prática de supressão de dados pessoais em relação a dados que devem ser legalmente e oficiosamente publicados e colocados à disposição dos interessados, dando azo a retrocessos na transparência da atividade administrativa, devendo ser sempre acauteladas as obrigações decorrentes da legislação nacional que legitimam o tratamento desses dados, na medida em que o RGPD não revogou a legislação nacional na matéria, sendo que a mesma mantém-se em vigor desde que não disponha em sentido contrário ao previsto no RGPD. Por sua vez, o direito à proteção de dados não é um direito absoluto,

devendo "ser considerando em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade"[214].

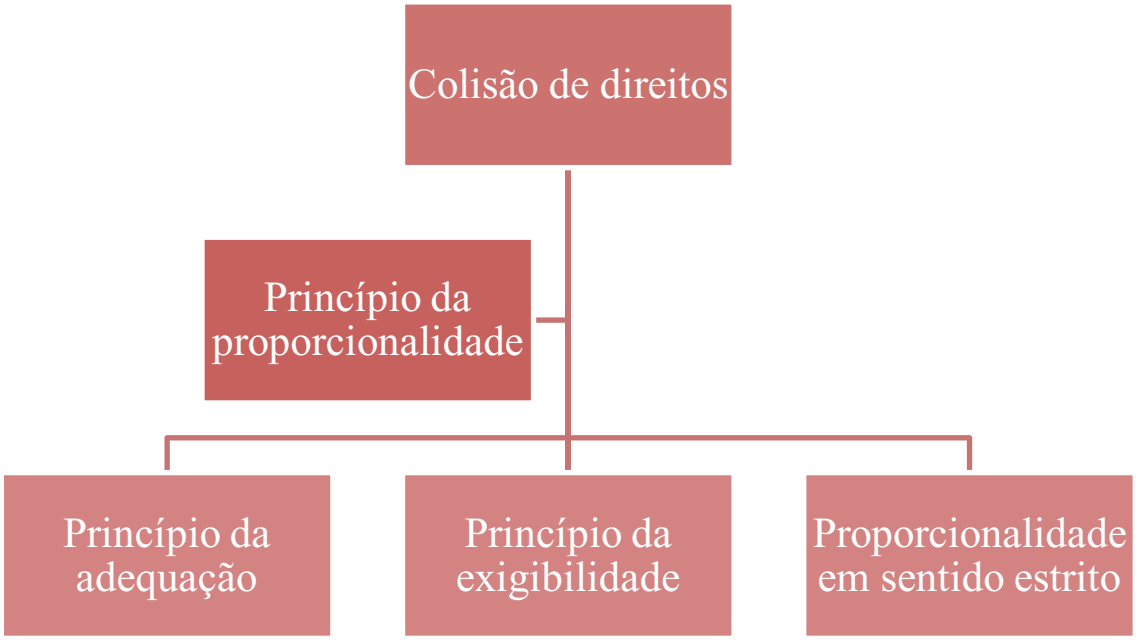
Todavia, na ponderação de deferimento de acesso a documentos nominativos, deverá considerar-se os princípios da licitude, lealdade e transparência, limitação das finalidades, minimização dos dados, integridade e confidencialidade do artigo 5.º do RGPD, que estabelecem que os dados pessoais devem ser "objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (…) recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades", devendo os mesmos ser "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados" e "tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito".

Assim, e em jeito de suma, aquando de requerimento para acesso a informação administrativa que contenha elementos nominativos, deverá ser dado enfoque às finalidades de tratamento de dados pessoais, competindo à entidade pública apurar a necessidade de vedar ou permitir o acesso, segundo critérios de proporcionalidade, em razão da presença de dados nos documentos administrativos que devam ser objeto de proteção, devendo ser analisada a possível afetação do direito à privacidade do titular dos dados, devendo a informação a fornecer cingir-se ao estritamente necessário no âmbito da finalidade invocada, devendo ser objeto de comunicação parcial sempre que tal se demonstre possível, expurgando-se os dados pessoais que não relevem para essa finalidade.

3.6.2 O princípio da proporcionalidade

[214] Considerando 4 do RGPD.

Figura 26 - Resolução de colisão de direitos fundamentais.



Conforme descrito supra perante situações de conflito entre o direito de acesso e o direito à reserva da intimidade da vida privada deverá atender-se à finalidade, sendo que só são legitimados sacrifícios do direito fundamental do direito de acesso aos arquivos e registos administrativos perante direitos e valores constitucionais de igual ou superior valor, designadamente, relativos à segurança interna e externa, à investigação criminal e à reserva da intimidade da vida privada.

Facilmente se verifica uma situação de colisão de direitos fundamentais, nomeadamente, direito à proteção de dados e do direito de acesso a documentos administrativos, tendo os órgãos da autoridade pública de dissipar aquando da conjugação dos regimes.

Como refere Andrade (2012), haverá colisão ou conflito sempre que se deva entender que a Constituição protege simultaneamente dois valores ou bens em contradição numa determinada situação concreta (…). A esfera de proteção de um direito é

constitucionalmente protegida em termos de intersetar a esfera de outro direito ou de colidir com uma outra ou princípio constitucional" (p.229).

Conforme Oliveira, Gomes & Santos (2015) explicam "os direitos fundamentais não são direitos ilimitados ou ilimitáveis. Vivendo os indivíduos numa sociedade, é normal que o Direito seja chamado a limitar os direitos fundamentais de modo a proteger os direitos fundamentais de outras pessoas ou ainda a garantir bens jurídicos de relevo específico, como a segurança ou a ordem pública. Apesar de os direitos fundamentais serem universais e inalienáveis, a sua interdependência e a vida em sociedade trazem, na prática do dia-a-dia, a necessidade de determinar os limites aos direitos fundamentais" (pp. 311 e 312).

O número 2 do artigo 18.º da Constituição da República estipula que a "lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos".

Na aceção de Canotilho & Moreira (1984) para que a restrição de direitos fundamentais seja constitucionalmente legítima deverá verificar-se cumulativamente as seguintes condições, designadamente, a restrição deverá estar prevista expressamente prevista na Constituição, a restrição vise salvaguardar outro direito ou interesse constitucionalmente protegido, que a restrição seja exigida por essa salvaguarda, seja apta para o efeito e se limite à medida necessária para alcançar esse objeto e que não aniquilo o direito em causa atingindo o conteúdo essencial do respetivo preceito (pp.391 a 393).

Conforme estabelece o Acórdão do Supremo Tribunal de Justiça, de 29 de novembro de 2016, no processo número 7613/09.3TBCSC.L1.S1, "uma das principais

características dos direitos fundamentais, enquanto princípios que são, é a sua relatividade, ou seja, não se revestem de caráter absoluto, antes são limitados internamente, para assegurar os mesmos direitos a todas as outras pessoas, e também externamente, para assegurar outros direitos fundamentais ou interesses legalmente protegidos que com eles colidam, mediante a harmonização entre uns e outros, a qual sempre implicará o sacrifício, total ou parcial, de um ou mais valores. (…) São frequentes as colisões entre direitos fundamentais: os conflitos entre o direito fundamental de um sujeito e o mesmo ou outro direito fundamentalmente ou interesse legalmente protegido de outro sujeito hão-de ser solucionados pelo poder judicial mediante a respectiva ponderação e harmonização, em concreto, à luz do princípio da proporcionalidade, evitando o sacrifício total de uns em relação aos outros e realizando, se necessário, uma redução proporcional do âmbito de alcance de cada qual"[215].

O referido acórdão acrescenta ainda que "a essência e a finalidade deste princípio da proporcionalidade é a preservação, tanto quanto possível, dos diversos direitos fundamentais com amparo na Constituição e, em concreto, colidentes, através da sua harmonização e da otimização do meio escolhido com a observação das seguintes regras ou subprincípios: i) a sua adequação ao fim em vista; ii) a sua indispensabilidade em relação a esse fim (devendo ser, ainda, a que menos prejudica os cidadãos envolvidos ou a coletividade); iii) a sua racionalidade medida em função do balanço entre as respetivas vantagens e desvantagens".

O princípio da proporcionalidade desdobra-se em três subprincípios, designadamente, princípio da adequação, que estabelece que "as medidas restritivas de direitos, liberdades

[215] *Cfr*. Acórdão do Supremo Tribunal de Justiça, de 29 de novembro de 2016, no processo número 7613/09.3TBCSC.L1.S1, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/a4ad03aaa6d934278025807a00589b2f?OpenDocument, consultado a 20/09/2019.

e garantias devem revelar-se como um meio para a prossecução dos fins visados, com salvaguarda de outros direitos ou bens constitucionalmente protegidos"; princípio da exigibilidade, em que "essas medidas restritivas têm de ser exigidas para alcançar os fins em vista, por o legislador não dispor de outros meios menos restritivos para alcançar o mesmo desiderato" e, por fim, o princípio da justa medida ou proporcionalidade em sentido estrito, onde "não poderão adotar-se medidas excessivas, desproporcionadas para alcançar os fins pretendidos"[216].

Assim, perante um conflito de direitos fundamentais, *in casu*, direito à proteção de dades e direito de acesso aos documentos administrativos, deverá atender-se ao princípio da proporcionalidade no caso concreto, devendo ser feito um juízo sobre o interesse direto, pessoal e legítimo do terceiro suficientemente relevante para a finalidade segundo o princípio da proporcionalidade (na sua vertente de adequação, necessidade e proibição de excesso).

Ambos os direitos fundamenteis devem ceder reciprocamente, delimitando-se a dimensão dessa cedência pela natureza dos interesses em causa. Assim deverá ponderar-se a solução adequada ao caso, devendo para o efeito ser definida qual a justa medida em que um ou cada um desses direitos há de prevalecer sobre o outro ou há de ser sacrificado em favor do outro, cabendo ao organismo público fazer um juízo de proporcionalidade com base nos critérios que, casos a caso, entenda serem de avaliar, decidindo conforme o juízo resultante dessa ponderação, podendo, em última instância, solicitar parecer à CADA.

3.7 Considerações finais

[216] *Cfr*. Acórdão do Tribunal Constitucional n.º 634/93– Processo nº 94/92, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19930634.html, consultado a 22/09/2019.

A atividade da Administração Pública encontra-se inevitavelmente sujeita ao RGPD, na medida em que no âmbito das suas competências e atribuições conferidas por lei aos serviços públicos, tem legitimidade para tratar dados pessoais dos administrandos, devendo esse tratamento ser pautado pelos princípios fundamentais de tratamento de dados pessoais consagrados no RGPD, devendo adaptar-se às novas alterações de paradigma no que concerne aos tratamentos de dados pessoais que efetua, para tal deverá adotar uma metodologia de implementação eficaz, na medida em que o RGPD exige um exaustiva análise e revisão de todos os processos de tratamento de dados, com vista a garantir a conformidade da sua atuação com o RGPD.

A atividade administrativa é pautada por princípios gerais que devem ser acautelados, tais como o princípio da administração aberta e o princípio da proteção de dados. Para o efeito, os organismos públicos devem proceder à análise da necessidade de vedar ou permitir o acesso aos documentos administrativos nominativos, segundo critérios de proporcionalidade, em razão da presença de dados nos documentos administrativos que devam ser objeto de proteção, devendo a informação a fornecer cingir-se ao estritamente necessário no âmbito da finalidade invocada, devendo ser objeto de comunicação parcial sempre que tal se demonstre possível, expurgando-se os dados pessoais que não relevem para essa finalidade.

Embora o sector público nacional não se demonstre tão aficionado pelo *big data* como o sector privado, a realidade é que a sociedade da informação e da tecnológica passa atualmente por diversas alterações, sendo que o sector público não poderá abster-se dessas. Exatamente como o SIMPLEX, enquanto programa nacional, global e integrado de modernização, simplificação e desburocratizarão administrativas potenciou a desburocratização e simplificação administrativa, o RGPD deverá ser encarado pelos organismos públicos como uma oportunidade.

Embora as administrações públicas demonstram-se pouco preparadas para lidar com grandes mudanças de paradigma legais e culturais, assim como apresentem inúmeras dificuldades no que concerne aos meios técnicos e económicos para se adaptar à nova realidade introduzida pelo RGPD, os organismos públicos, em articulação com os entes privados, desempenharão um papel central no cumprimento das novas disposições em matéria de proteção de dados, sendo que o RGPD constitui uma excelente oportunidade para que os entes públicos ponderem sobre os tratamentos de dados realizados no âmbito da sua atividade, assim como sobre os sistemas de segurança de redes e sistemas de informação utilizados.

CAPÍTULO IV - CONCLUSÕES

A proteção de dados constitui uma temática cuja importância tem sido apontada desde muito cedo, sendo que a Declaração Universal dos Direitos do Homem de 1948 já consagrava no seu artigo 12.º o direito à privacidade. Todavia, a evolução da sociedade de informação e da tecnologia despoletou a necessidade de consagração de um novo regime de proteção dos titulares de dados pessoais a nível europeu.

As organizações europeias já operavam sobe a égide da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, sendo que o RGPD apenas veio desenvolver, alargar e aplicar as normas, princípios e direitos estabelecidos na Diretiva 95/46/CE, nomeadamente, atribuindo novos direitos aos titulares dos dados pessoais, fortalecendo os princípios da transparência, minimização dos dados e limitação da finalidade consagrados na diretiva, assim como as regras relativas ao consentimento e à notificação da violação dos direitos dos titulares de dados pessoais, aperfeiçoando a sua aplicação nos Estados-membros.

Da análise do RGPD é possível concluir uma mudança de paradigma, na medida que procedeu à correção dos quatro problemas da anterior Diretiva que terão grande impacto, nomeadamente, veio proceder à harmonização do quadro legislativo em toda a União Europeia, assim como, veio dotar as autoridades de controlo das ferramentas necessárias para impor a proteção de dados, estabelecendo um quadro sancionatório mais gravosos, permitindo que empresas sediadas em países terceiros sejam responsabilizadas pelos tratamentos de dados pessoais que fazem de cidadãos localizados no território da União Europeia. E por fim, aumentou o conceito de dados pessoais de modo a abranger os avanços tecnólogicos processadores de dados e dotou os titulares de dados pessoais de

novos direitos, tais como direito a ser esquecido, direito à portabilidade dos seus dados e direito à limitação do tratamento.

O RGPD fornece uma base para o desenvolvimento de novos modelos de negócio e a habilidade das organizações tratatarem dados pessoais dos seus consumidores, implicando, todavia, um maior nível de segurança jurídica do titular dos dados, assim como uma maior coerência jurídica nos 28 Estados-Membros da União Europeia, introduzindo uma abordagem de autoregulação e análise de risco, com notificações de violação de dados, avaliações de impacto na proteção de dados, assim como nomeação de um Encarregado de Proteção de Dados.

Todavia, é indiscutível que a implementação do RGPD apresenta um desafio para as organizações, na medida em que prevê novos direitos do titular dos dados pessoais, o que implica, forçosamente, novos deveres para os responsáveis pelo tratamento e subcontratantes. Tal significa que as entidades processadoras de dados pessoais devem dissecar as suas práticas em matéria de proteção de dados pessoais, de modo a garantir *compliance* com o RGPD e adaptação a um quadro legal mais rígido. Conforme explica Mamede (2015) "o que se pode esperar é a necessidade de as organizações terem de fazer investimentos em tecnologia para reduzir o impacto da nova regulamentação de proteção de dados, em geral, com foco na criptografia e em capacidade analítica e de produção de relatórios na área da segurança" (p. 97).

Embora o RGPD surja como uma continuação da Diretiva de 95, a verdade é que a proteção de dados até 2016 não constituiu uma preocupação das organizações públicas e de muitas pequenas e média empresas, que não valorizavam os temas relacionados com a privacidade e a segurança da informação ou o valor económico dos seus dados, logo o investimento que o RGPD poderá implicar, acarretará sérias dificuldades às pequenas e

médias empresa, que até então não empregaram sistemas de segurança de informação e não detêm meios técnicos e económicos para a nova realidade introduzida pelo RGPD, sendo que assegurar um nível de competência especializado constituirá um dos grandes desafios destas empresas, devendo as mesmas investir na formação da organização e dos colaboradores em matéria de proteção de dados e da privacidade, fomentando uma maior consciencialização sobre esta temática e cultivando culturas de segurança de informação.

De igual modo, a Administração Pública encontra-se sujeita às regras do RGPD na medida que no âmbito das suas competências e atribuições conferidas por lei aos serviços públicos, tem legitimidade para tratar dados pessoais dos administrandos, devendo esse tratamento ser pautado pelos princípios fundamentais de tratamento de dados pessoais consagrados no RGPD, nomeadamente, tratamento equitativo e lícito, limitação da finalidade, minimização dos dados e conservação dos dados, devendo verificar-se uma mudança de paradigma tal como nas organizações do sector privado, devendo os procedimentos ser, necessariamente, uniformizados para toda a Administração Pública e efetuados investimentos na área da segurança da informação, assim como, em recursos humanos especializados, devendo ser criados equipas multidisciplinares, compostas por elementos com formação na área do direito, informática, gestão, dotados de competências na área da gestão de risco, por forma a serem acauteladas possíveis lacunas e aproveitadas sinergias.

A implementação do RGPD na Administração Pública, tal como nas entidades do sector privado, deverá ser um processo contínuo que envolve a totalidade do organismo, na medida em que serão os trabalhadores que no seu dia a dia trataram os dados no exercício das suas atividades. No âmbito do acesso aos documentos administrativos nominativos, deverão os trabalhadores adstritos ao atendimento ao público estar dotados de conhecimentos no âmbito do direito administrativo, especialmente sobre o princípio

da proporcionalidade, e proteção de dados, de modo a que as pretensões de terceiros, que pretendem aceder a documentos administrativos nominativos, e o regime da proteção de dados seja devidamente acautelado, evitando-se tutelas de curiosidades alheias, tornando-se ainda imperioso que os Encarregados de Proteção de Dados estejam dotados de competências para o o exercicio das funções que lhes são cometidas pelo artigo 39.º do RGPD, defendendo-se que a certificação poderá ser uma forma de garantir a qualificação profissional do EPD, assim como garantia de um nível de competência miníma dos profissionais.

Em jeito de suma, a elaboração da presente dissertação foi bastante interessante, todavia, considerando o carácter recente da temática e o facto de muitas das organizações a nível regional e nacional ainda se encontrarem a implementar o RGPD – passados já mais de um ano desde que tornou-se aplicável – demonstrou-se bastante difícil aceder a dados de implementação ou proceder a um estudo de caso viável, tendo a realização de inquéritos não se demonstrado uma opção válida uma vez que a amostra não seria real. A título exemplificativo, é de apontar que a nível da administração pública regional somente a 9 de maio de 2019 foi publicitado o concurso público para "Aquisição de serviços de consultoria de suporte e capacitação no âmbito do Sistema Integrado de Gestão da Proteção de Dados do Governo Regional dos Açores, em cumprimento e conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD), nas vertentes processual, jurídica e tecnológica", encontrando-se a decorrer o processo de análise, sendo possível concluir que o atrasado na implementação do RGPD é indicativo do facto de a temática da proteção de dados não se afigurar ainda uma prioridade das organizações, sendo imperioso que as organizações alterem o modo como encaram a temática da proteção de dado.

REFERÊNCIAS

a) Monografias

- Almeida, M. A. de. (2015). *Teoria Geral do Direito Administrativo – O Novo Regime do Código de Procedimento Administrativo* (3.ª). Coimbra: Almedina.

- Amorim, J. P. A. de, Oliveira, M. E. de, & Gonçalves, P. C. (2010). *Código do Procedimento Administrativo - Comentado* (2.ª). Coimbra: Almedina.

- Andrade, J. C. V. de. (2012). *Os Direitos Fundamentais na Constituição Portuguesa de 1976.* Coimbra: Almedina.

- Bertino, E., & Ferrari, E. (2018). Big Data Security and Privacy. In *A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years. Studies in Big Data* (Vol. 31, pp. 425–439). Springer International Publishing. doi: 10.1007/978-3-319-61893-7.

- Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. In *Privacy Technologies and Policy* (pp. 21–37). Springer, Cham. doi: https://doi.org/10.1007/978-3-319-44760-5_2

- Canotilho, J. J. G., & Moreira, V. (1984). *Constituição da República Portuguesa – Anotada*, (2.ª, Vol. 1). Coimbra: Coimbra Editora.

- Carvalho, R. (1999*). O direito à informação administrativa procedimental*. Porto: Universidade Católica Portuguesa.

- Francisco, D., & Francisco, S. (2019). *Regulamento Geral de Proteção de Dados: 7 passos para uma metodologia de implementação do RGPD na Administração Pública*. Lisboa: Edições Sílabo.

- Team, I. T. G. P. P. (2017). ROLE OF THE DATA PROTECTION OFFICER. In *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second edition* (pp. 53–82). IT Governance Publishing. doi: 10.2307/j.ctt1trkk7x.6.

- Oliveira, B. N., Gomes, C. de M. e, & Santos, R. P. dos (2015). *Os Direitos Fundamentais em Timor-Leste: Teoria e Prática* (1.ª). Coimbra: Coimbra Editora, S.A.

- Pinheiro, A. S. (2016). A protecção de dados no novo Código do Procedimento Administrativo. In *Comentários ao novo Código do Procedimento Administrativo - Coordenação de Carla Amado Gomes, Ana Fernanda Neves e Tiago Serrão* (3.ª, Vol. I, pp. 339–366). AAFDL Editora.

- Reynolds, P. D. (1979). *Ethical Dilemmas and Social Science Research*. San Francisco, CA: Jossey-Bass Publishers. doi: https://doi.org/10.1177/016224398000500441.

- Shalev-Shwartz, S., & Ben-David, S. (2014*). Understanding Machine Learning: From Theory to Algorithms*. Cambridge University Press. doi: 10.1017/CBO9781107298019.

- Silveira, A., & Canotilho, M. (2013). *Carta dos Direitos Fundamentais da União Europeia Comentada*. Coimbra: Almedina.

- Sloot, B. van der, Broeders, D., & Schrijvers, E. (2016). *Exploring the Boundaries of Big Data*. Amsterdam: Amsterdam University Press.

b) Artigos

- AA.VV. *Memorando da Comissão de Ética sobre Orientações Éticas para investigação com sujeitos humanos em contextos letivos*. Universidade dos Açores, 2018.

- Alves, D. & Castilho, D. (2016). "A evolução dos direitos humanos na Europa: Os principais momentos desde a ausência de direitos fundamentais na União Europeia até a atualidade". Disponível em: http://repositorio.uportu.pt/jspui/bitstream/11328/1461/1/A%20EVOLU%C3%87%C3%83O%20DOS%20DIREITOS%20HUMANOS%20NA%20EUROPA.pdf

- Cavoukian, A. (2011). "*Privacy by Design - The 7 Foundational Principles*". Disponível em: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf;

- Crabtree, A., Lodge, T., Colley, J., Greenhalgh, C., Glover, K., Haddadi, H., … McAuley, D. (2018). Building accountability into the Internet of Things: the IoT Databox model. *Journal of Reliable Intelligent Environments*, 4(1), 39–55. doi: https://doi.org/10.1007/s40860-018-0054-5.

- Ghani, N. A., Hamid, S., & Udzir, N. I. (2016). Big Data and Data Protection: Issues with Purpose Limitation Principle. *International Journal of Advances in Soft Computing an Its Application*, 8(3), 116–121. Disponível em: http://home.ijasca.com/data/documents/ID-40_Pg116-121_Big-Data-and-Data-Protection-Issues-with-Purpose-Limitation-Principle_2.pdf

- Hert, P. D., PAPAKONSTANTINOU, V., MALGIERI, G., BESLAYC, L., & SANCHEZ, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, 34(2), 193–203. doi: https://doi.org/10.1016/j.clsr.2017.10.003.

- Hirsch, D. D. (2014). "The glass house effect: big data, the new oil, and the power of analogy". *Maine Law Review*, 66(2). Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393792.

- Houser, K. A., & Voss, W. G. (2018). GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *SSRN Electronic Journal*. doi: 10.2139/ssrn.3212210.

- Lachaud, E. (2018). Certification of Data Protection Officers Should Be Regulated. *SSRN Electronic Journal*. doi: 10.2139/ssrn.3176471.

- Mamede, H. S. (2015). Notas leitura /Recensão crítica [de] Protection of Personal Data. *Revista de Ciências da Computação*, 10.

- Martins, C. F. (2019, janeiro 24). Aprovada decisão de adequação para transferências de dados entre UE-Japão. *Macedo Vitorino & Associados, Sociedade De Advogados, RL.* Disponível em https://www.macedovitorino.com/xms/files/20190124-Decisao_de_Adequacao_UE-Japao.pdf

- Fernandes, D. M. (2015). *O princípio da transparência administrativa: Mito ou Realidade?* Revista Da Ordem Dos Advogados, Janeiro – Junho , 425–457.

- Nati, M. (2018). Personal Data Receipts: How transparency increases consumer trust. *MyData Journal*. Disponível em https://medium.com/mydata/personal-data-receipts-how-transparency-increases-consumer-trust-bb96d6cd4fb1;

- Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consente under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, 4(1). doi: https://doi.org/10.1093/cybsec/tyy001

- Raab, C. D., & Bennett, C. J. (1994). Protecting Privacy Across Borders: European Policies And Prospects. *Public Administration*, 72(1), 95–112. doi: 10.1111/j.1467-9299.1994.tb01001.x

- Raposo, Sá Miranda & Associados, Sociedade de Advogados, R.L (2015). Safe Harbor: Perguntas e Respostas. Disponível em: https://www.pra.pt/site/assets/files/1222/safe_harbor_nota_informativa.pdf

- Santín, M. (2017). The problem of the right to be forgotten from the perspective of self-regulation in journalism. El Profesional De La Información, 26(2), 303. doi: 10.3145/epi.2017.mar.17

- Silveira, S., Avelino, R., & Souza, J. (2016). A privacidade e o mercado de dados pessoais. *Liinc Em Revista*, 12(2), 217–230. doi: 10.18617/liinc.v12i2.902

- Vicente, L. N. (2014). O Princípio da Proporcionalidade Uma Nova Abordagem em Tempos de Pluralismo. *Instituto Jurídico*. Disponível em https://www.ij.fd.uc.pt/publicacoes/premios/pub_1_ms/numero1_pms.pdf.

c) Legislação

- Carta dos Direitos Fundamentais da União Europeia (2000/C 364/01), *Jornal Oficial n.º C 364 de 18/12/2000 p. 0001 - 0022;*

- Constituição da República Portuguesa, Diário da República n.º 86/1976, Série I de 1976-04-10.

- Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108), *Diário da República I-A, n.º 159, de 09/07/1993 (Resolução da Assembleia da República n.º 23/93)*

- Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, *Jornal Oficial n.º L 350 de 30/12/2008 p. 60-71;*

- Declaração Universal dos Direitos do Homem, *Diário da República I Série A n.º 57/78* ;

- Decreto-Lei n.º 18/2008, *Diário da República n.º 20/2008, Série I de 2008-01-29, pp. 753 – 852;*

- Decreto-Lei n.º 4/2015, *Diário da República n.º 4/2015, Série I de 2015-01-07, p. 50 – 87;*

- Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, *Jornal Oficial nº L 281 de 23/11/1995 p. 0031 – 0050;*

- Lei n.º 67/98, de 26 de outubro, *Diário da República n.º 247/1998, Série I-A de 1998-10-26;*

- Lei n.º 26/2016, *Diário da República n.º 160/2016, Série I de 2016-08-22, p. 2777 – 2788;*

- Lei n.º 58/2019, de 8 de agosto, *Diário da República n.º 151/2019, Série I de 2019-08-08, p. 3-40;*

- Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão, *Jornal Oficial n.º 145 de 31/05/2001, p. 43-28.*

- 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, *Jornal Oficial n.º L 119, 4/05/2016, p. 1–88;*

- Regulamento n.º 789/2018 da CNPD, Lista de tratamentos de dados pessoais sujeitos a avaliação de impacto sobre a proteção de dados, *Diário da República n.º 231/2018, Série II de 2018-11-30;*

- Retificação do 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), *Jornal Oficial da União Europeia N.º L 127/2, 23/5/2018;*

- Tratado de Lisboa, *Jornal Oficial da União Europeia n.º C 306, 17/12/2007, P. 1-271;*

- Tratado Sobre o Funcionamento da União Europeia (2012/C 326/01), *Jornal Oficial nº C 326 de 26/10/2012 p. 0001 – 0390;*

- Proposta de Lei n.º 120/XIII/3ª, *Diário da República, II série A, N. º89/XIII/3 de 26/03/2018 p. 30-48;*

d) Dissertações de Mestrado

- Couto, M. L. dos S. A. (2016). *O E-Commerce à luz do direito – Análise do Regulamento Geral da Proteção de Dados – A Uniformização na União Europeia* (Dissertação de Mestrado). Universidade Católica Portuguesa.

- Moreira, T. F. M. (2018). *O impacto da proteção de dados nas organizações: Um novo paradigma* (Dissertação de Mestrado). Instituto Politécnico de Coimbra.

- Oliveira, M.V. G. (2015). *Proteção de Dados Pessoais nas Comunicações Eletrónicas: O papel da CNPD e da ANACOM (*Dissertação de Mestrado). Universidade Católica de Lisboa.

- Bravo, R. A. G. (2017). *E-Commerce: a influenciada Confiança na Intenção de Compra Online* (Dissertação de Mestrado). Escola Superior de Comunicação Social.

e) Acórdãos

- Acórdão do Tribunal Central Administrativo Norte, de 23 de setembro de 2015, processo n.º 01306/15.0BEBRG. Disponível em: http://www.dgsi.pt/jtcn.nsf/-/3DA13F65F20B5EA180257F0100407674

- Acórdão do Tribunal Constitucional n.º 182/89 - Processo n.º 298/87, Diário da República n.º 51/1989, Série I de 2 de março de 1989, p. 922 – 925;

- Acórdão do Tribunal Constitucional n.º 128/92 - Processo: n.º 260/90, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19920128.html;

- Acórdão do Tribunal Constitucional n.º 176/92 – Processo n.º 214/90, Diário da República n.º 216, II Série de 18 de setembro de 1992, p. 8775.

- Acórdão do Tribunal Constitucional n.º 634/93– Processo nº 94/92, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19930634.html;

- Acórdão do Tribunal Europeu dos Direitos do Homem, processo n.º 18030/11, disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-167828%22]};

- Acórdão n.º C-131/12 do Tribunal de Justiça da União Europeia, de 13 de maio de 2014, JO C 212 de 7.7.2014.

- Acórdão do Supremo Tribunal Administrativo, de 17 de janeiro de 2008, processo n.º 0896/07, disponível em: http://www.dgsi.pt/jsta.nsf/35fbbbf22e1bb1e680256f8e003ea931/7a11a8ad079aebc9802573de00374730?OpenDocument&ExpandSection=1;

- Acórdão do Supremo Tribunal Administrativo, de 31 de agosto de 2011, processo n.º 0758/11, disponível em: http://www.dgsi.pt/jsta.nsf/-/DB1D78475C15829D802578FF003EE3CB;

- Acórdão do Supremo Tribunal Administrativo, de 24 de janeiro de 2012, processo n.º 0668/11, disponível em: http://www.dgsi.pt/jsta.nsf/35fbbbf22e1bb1e680256f8e003ea931/5d83b3dc6602348280257996005 9b84c?OpenDocument&ExpandSection=1;

- Acórdão do Supremo Tribunal de Justiça, de 29 de novembro de 2016, no processo n.º 7613/09.3TBCSC.L1.S1, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/a4ad03aaa6d934278025807a00589b2f?OpenDocument;

f) Webgrafia

- Comissão de Acesso aos Documentos Administrativos (2017). *Atividade da Comissão de Acesso aos Documentos Administrativos no ano de 2017 23.º Relatório – 2017*. Disponível no portal: http://www.cada.pt/uploads/589dc310-63c2-68d4.pdf

- Comissão de Acesso aos Documentos Administrativos (2018). *Atividade da Comissão de Acesso aos Documentos Administrativos no ano de 2018 24.º Relatório – 2018*. Disponível no portal: http://www.cada.pt/uploads/589dc30f-9197-4873.pdf

- Comissão de Acesso aos Documentos Administrativos (2014). *Parecer n.º 132/2014*. Disponível no portal: http://www.cada.pt/modules/CADA/lista.php?anoparecer=2014;

- Comissão Europeia (2010). *A comprehensive approach on personal data protection in the European Union COM(2010) 609 final*. Jornal Oficial da União Europeia N.º C121, 19.04.2011.

- Comissão Europeia (2012). *Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century COM (2012) 9 final*. Disponível no portal: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF;

- Comissão Europeia (2012). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final.* Disponível no portal: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2012:0011:FIN;

- Comissão Europeia (2014). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Para uma economia dos dados próspera COM(2014) 442 final*. Disponível no portal: https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A52014DC0442;

- Comissão Europeia (2015). *Estratégia para o Mercado Único Digital na Europa COM (2015) 192 final.* Disponível no portal: https://eur-lex.europa.eu/legal content/PT/TXT/PDF/?uri=CELEX:52015DC0192&from=EN;

- Comissão Europeia (2015). *COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO sobre a transferência de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems*) *COM (2015) 566 final.* Disponível no portal: https://ec.europa.eu/transparency/regdoc/rep/1/2015/PT/1-2015-566-PT-F1-1.PDF

- Comissão Europeia (2015). *Special Eurobarometer 431, Data Protection*. Disponível no portal: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/yearFrom/2013/yearTo/2015/s

- Comissão Europeia (2018). *Maior proteção, novas oportunidades — Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018 COM(2018) 43 final.* Disponível no portal: https://www.dgpj.mj.pt/sections/noticias/orientacoes-da-comissao/downloadFile/attachedFile_f0/ST05702.PT18.pdf?nocache=1517568283.87

- Comissão Europeia (2019). *GDPR in Numbers.* Disponível no portal: https://ec.europa.eu/commission/sites/beta-political/files/infographicgdpr_in_numbers_0.pdf.

- Comissão Europeia (2019). *Special Eurobarometer 487a, The General Data Protection Regulation*. Disponível no portal: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222;

- Comissão Nacional de Proteção de Dados (2014). *Deliberação n.º 241/2014.* Disponível no portal: https://www.cnpd.pt/bin/orientacoes/20140128_CNPD_delib241.pdf;

- Comissão Nacional de Proteção de Dados (2018). *Deliberação n.º 984/2018*. Disponível no portal: https://www.cnpd.pt/bin/decisoes/Delib/20_984_2018.pdf;

- Comissão Nacional de Proteção de Dados (2019). *Deliberação 2019/494*. Disponível no portal: https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_494.pdf?fbclid=IwAR1IQijM3fnl4JfN9jInj8C0uqW4ypczSQexMMTtE1Xa5KxkbG4DV_7J8Ds;

- Comissão Nacional de Proteção de Dados (2019). *Deliberação n.º 2019/495*. Disponível no portal: https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_495.pdf;

- Comissão Nacional de Proteção de Dados (2018). *Parecer 20/2018.* Disponível no portal: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e45544563765247396a6457316c626e527663306c7561574e7059585270646d4644623231706334e686279396a5a57593359544d794f4330325a44526c4c54526c4e546b74596a41304e4331694e54426d4f5449314d6a64684d7a45756347526d&fich=cef7a328-6d4e-4e59-b044-b50f92527a31.pdf&Inline=true;

- Comissão Nacional de Proteção de Dados (2018). *Relatório de Atividades 2017-2018*. Disponível no portal: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201718.pdf

- European Data Protection Board (2019). *1 year GDPR – taking stock*. Disponível no portal: https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en;

- Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2014). *Parecer 03/2014, relativo à notificação da violação de dados pessoais WP 213.* Disponível no portal: https://www.gpdp.gov.mo/index.php?m=content&c=index&a=print_news&catid=153&id=16;

- Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2016). *Orientações sobre os encarregados da proteção de dados (EDP) WP243rev.01*. Disponível no portal: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048;

- Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2017). *Orientações sobre o Direito à portabilidade WP 242 rev.01*. Disponível no portal: https://www.cnpd.pt/bin/rgpd/docs/wp242rev01_pt.pdf;

- Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2017*). Orientações relativas à transparência na aceção do Regulamento 2016/679 WP260 rev.01.* Disponível no portal: https://www.cnpd.pt/bin/rgpd/docs/wp260rev01_pt.pdf;

- Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2017). *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 WP248rev.01. Disponível no portal: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

- Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2017). *Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 WP250rev.01.* Disponível no portal: https://www.cnpd.pt/bin/rgpd/docs/wp250rev01_pt.pdf;

- Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2018). *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679 WP251rev.01*. Disponível no portal: https://www.cnpd.pt/bin/rgpd/docs/wp251rev01_pt.pdf;

- Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2010). *Parecer 8/2010 sobre a Proteção de Dados relativo à legislação aplicável 0836-02/10/PT WP 179.* Disponível no portal: https://www.gpdp.gov.mo/uploadfile/others/wp179_pt.pdf

- Conselho Europeu (2010). *O Programa de Estocolmo - Uma Europa aberta e segura que sirva e proteja os cidadãos.* Disponível no portal: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:PT:PDF

- Parlamento Europeu (2011). *Sobre uma abordagem global da proteção de dados pessoais na União Europeia.* Disponível no portal: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2011-0323+0+DOC+PDF+V0//PT

- Provedor de Justiça (2006). *Recomendação n.º 9/A/2006, processo n.º R-3212/05.* Disponível no portal: https://www.provedor-jus.pt/?action=5&idc=67&idi=3469

- As prioridade da Comissão Europeia – Mercado Único Digital: https://ec.europa.eu/commission/priorities/digital-single-market_pt#policy-areas

- Comissão Europeia – Proteção de dados: https://ec.europa.eu/info/law/law-topic/data-protection_pt

- Comissão Europeia - *Article 29 Working Party*: https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

- Site oficial da União Europeia:
  https://europa.eu/european-union/index_pt

- Comissão Nacional da Proteção de dados:
  https://www.cnpd.pt/

A proteção de dados pessoais – o novo paradigma jurídico

Daniela Medeiros Teves

DM

2019