Torrado, Bruno Filipe Lourenço

O encarregado da proteção de dados, à luz do novo regulamento geral da proteção de dados

http://hdl.handle.net/11067/6121

Metadata

Issue Date 2021

Abstract No ordenamento jurídico em Portugal o direito à vida privada está inserido no capítulo dos direitos fundamentais consagrados na Constituição da República Portuguesa (CRP). Sendo que o direito à reserva de intimidade da vida privada e o direito de utilização da informática estão descritos nos Direitos, Liberdades e Garantias, respetivamente, nos artigos 26.º, n.º 1 e 35.º da (CRP). O Regulamento Geral da Proteção de Dados foi aprovado em 2016 e entrou em vigor em maio de 2018, e tem trazido uma ...

Abstract: The Portuguese legal system, the right to have a private life is presented in the chapter of fundamental rights treasured in the Constitution of the Portuguese Republic (CPR). The right to preserve the intimacy of the private life and the right to use information technology are described in the Rights, Freedoms and Guarantees, respectively, in articles 26, paragraphs 1 and 35 of the CPR. The General Data Protection Regulation, that was approved in 2016 and became applicable in May 20...

Keywords Direito, Proteção de dados, Encarregado da Proteção de Dados

Type masterThesis

Peer Reviewed No

Collections [ULP-FD] Dissertações

UNIVERSIDADE LUSÍADA DO NORTE - PORTO

O ENCARREGADO DA PROTEÇÃO DE DADOS, À LUZ DO NOVO REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

Bruno Filipe Lourenço Torrado

Dissertação para obtenção do Grau de Mestre

Porto, 2020

UNIVERSIDADE LUSÍADA DO NORTE - PORTO

O ENCARREGADO DA PROTEÇÃO DE DADOS, À LUZ DO NOVO REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

Bruno Filipe Lourenço Torrado

Dissertação para obtenção do Grau de Mestre

Sob a Orientação do Professor Doutor Gravato Morais

Porto, 2020

Agradecimentos

Aos meus pais, Abílio Torrado e Natália Lourenço, por depositarem uma generosa dose de esperança em mim e por abdicarem das suas vidas em prol da realização do sucesso dos filhos.

Ao meu irmão, Hugo Torrado, que sempre me fez acreditar que tudo isto era possível.

Índice

Resumo

No ordenamento jurídico em Portugal o direito à vida privada está inserido no capítulo dos direitos fundamentais consagrados na Constituição da República Portuguesa (CRP). Sendo que o direito à reserva de intimidade da vida privada e o direito de utilização da informática estão descritos nos Direitos, Liberdades e Garantias, respetivamente, nos artigos 26.º, n.º 1 e 35.º da (CRP).

O Regulamento Geral da Proteção de Dados foi aprovado em 2016 e entrou em vigor em maio de 2018, e tem trazido uma grande discussão à volta das Organizações, que é onde o Regulamento traz um grande impacto. Existem novas metodologias a aplicar e um grande número de regras, sempre na perspetiva de salvaguardar a proteção dos titulares de dados pessoais que estejam ligados às organizações, sendo que sobre as organizações cai sempre uma grande pressão para cumprir com o regulamento, sob pena de serem instauradas coimas com um grande peso monetário.

O tema da dissertação pretende abordar o conceito novo que o Regulamento trouxe, que é o Encarrego da Proteção de Dados (EPD), ou o Data Protection Officer (DPO) conforme é mais conhecido internacionalmente. O EPD é a principal figura que o RGPD veio instituir nas Organizações, sendo que as mesmas, em determinadas situações, terão mesmo de nomear um EPD para assegurarem o cumprimento do Regulamento Geral da Proteção de Dados.

Essencialmente, este trabalho irá incidir sobre o Encarregado da Proteção de Dados, no sentido de apurar quando é obrigatória ou não a sua constituição numa organização, irá também ser abordada a questão de qual a posição do EPD na organização que o constituiu, desde o seu envolvimento na organização aos conflitos de interesse e, claro está, iremos dar uma enorme relevância a verificar quais as suas funções e obrigações.

Palavras-chave

Direito

Princípios

Legislação

Proteção de Dados

Encarregado da Proteção de Dados

Regulamento

Abstract

In the Portuguese legal system, the right to have a private life is presented in the chapter of fundamental rights treasured in the Constitution of the Portuguese Republic (CPR). The right to preserve the intimacy of the private life and the right to use information technology are described in the Rights, Freedoms and Guarantees, respectively, in articles 26, paragraphs 1 and 35 of the CPR.

The General Data Protection Regulation, that was approved in 2016 and became applicable in May 2018, has brought up a big debate surrounding Corporations – where the Regulation as, specifically, a big impact. There are new methods to be applied and a considerable number of rules, always seeking to assure the protection of the holders of the private data who are connected with the institutions, being these institutions under a great deal of pressure to comply with the Regulation – at the risk of being applied fines with a substantial financial burden.

The subject of the thesis intends to address the new concept that the Regulation brought up: the Data Protection Officer (DPO). The DPO is the key actor that the GDPR established in the organizations, being these organizations, in certain situations, compelled to appoint a DPO to assure the compliance of the General Data Protection Regulation.

In essence, this work will focus over the Data Protection Officer, in order to determine whether it is mandatory or not to establish this role in an organization; furthermore, it will be assessed the role of the DPO on its organization, ranging from its involvement in the organization to the potential conflicts of interest and, evidently, we shall address with great detail its tasks and duties.

Lista de Abreviaturas e siglas

A.E.P.D.	Autoridade Europeia para a Proteção de Dados
Al.	Alínea
Als.	Alíneas
Art.	Artigo
Arts.	Artigos
C.E.P.D.	Comité Europeu para a Proteção de Dados
Cf.	Confira
Cfr.	Conforme
Cit.	Citada (Citatum)
C.N.P.D.	Comissão Nacional de Proteção de Dados
C.N.P.D.P.I.	Comissão Nacional de Proteção de Dados Pessoais Informatizados
C.P.	Código Penal
C.R.P.	Constituição da República Portuguesa
O.C.D.E.	Organização para a Cooperação e Desenvolvimento Económico
O.N.U.	Organização das Nações Unidas
R.G.P.D.	Regulamento Geral sobre a Proteção de Dados
R.J.C.	Regime Jurídico da Concorrência
S.T.J.	Supremo Tribunal de Justiça
T.C.	Tribunal Constitucional
T.I.C.	Tecnologias de Informação e Comunicação

Introdução

No ordenamento jurídico em Portugal o direito à vida privada está inserido no capítulo dos direitos fundamentais consagrados na Constituição da República Portuguesa (CRP). Sendo que o direito à reserva de intimidade da vida privada e o direito de utilização da informática estão descritos nos Direitos, Liberdades e Garantias, respetivamente, nos artigos 26.º, n.º 1 e 35.º da (CRP).

Este direito fundamental está cada vez mais saliente nos dias de hoje, devido às mudanças de mentalidades, acompanhadas pela evolução tecnológica e da globalização. Foi com o surgimento das redes sociais e das aplicações informáticas que a ideia de invasão dos dados pessoais dos indivíduos se tornou um desafio em matéria de proteção de dados no âmbito jurídico-legal[1].

O Regulamento Geral de Proteção de Dados (RGPD) entrou em vigor em 25 de maio de 2018 e substituiu a diretiva e lei de proteção de dados que se encontrava em vigor.

Tendo em consideração o Regulamento (UE) nº 2016/679, do Parlamento Europeu e do Conselho de 27 de abril de 2016, relacionado com a proteção das pessoas singulares no respeito ao tratamento de dados pessoais e à livre circulação desses mesmos dados, designado por Regulamento Geral da Proteção de Dados, ou RGPD, consagra nos seus artigos 37º a 39º, a figura do Encarregado da Proteção de Dados, exigindo continuamente o tratamento efetuado por uma autoridade ou organismo público, com exceção dos tribunais no exercício da sua função jurisdicional.

Neste sentido, o RGPD[2], que entrou em vigor no ano de 2018, proporciona o quadro de cumprimento mais moderno e com base na responsabilidade em matéria de

[1] CE. (2012). COM (2012) 11 final. Proposta de regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Acedido em 08 de janeiro de 2018. Disponível em https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=COM:2012:0011:FIN.2 Considerando (6) e (7) do RGPD.

[2] 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) (JO L 119 de 4.5.2016). O RGPD é relevante para efeitos do EEE e será aplicável depois de ser integrado no Acordo EEE

proteção de dados na Europa. O Encarregado da Proteção de Dados tem um papel no novo quadro normativo relacionado com o número de organizações, enquanto facilitam o cumprimento das disposições de RGPD.

É necessário que o nosso ordenamento jurídico seja aperfeiçoado para que possa dar respostas às reclamações da realidade constitucional (law in action), bem como às exigências de um Estado de Direito material legitimo, que seja constituído de princípios de justiça e dignidade da pessoa humana e, que se efetive uma "*maior autenticidade da democracia*"[3].

Neste contexto, é o legislador que ao assumir a responsabilidade da catalogação de um conjunto de direitos, liberdades e garantias, deve questionar sobre a melhor forma de os tornar efetivos. Ou seja, não será plausível se um Estado constitucionalizar direitos, se não se comprometer a atribuir-lhes a eficácia adequada. A preocupação principal neste caso, deve centrar-se na efetividade sob pena de existirem afirmações vazias e sem sentido[4].

Ora, em termos do ordenamento jurídico português, o modelo nacional de justiça constitucional possui somente o acesso à Constituição por via indireta, ou seja, através do exercício do seu direito de petição ou queixa, o que como consequência, pode tentar sensibilizar os titulares de legitimidade processual ativa.

Consubstancia-se que o modelo português de justiça constitucional possui somente um acesso à Constituição através da via indireta, ou seja, por meio do exercício do seu direito de petição ou de queixa, poderá sensibilizar os titulares de legitimidade processual ativa em processos de fiscalização abstrata da constitucionalidade, conforme artigo 281º, nº 2, alínea d), CRP).

O tema desta dissertação pretende abordar o conceito novo que o Regulamento trouxe, que é o Encarrego de Proteção de Dados (EPD), ou o Data Protection Officer (DPO) conforme é mais conhecido internacionalmente. O EPD é a principal figura que o RGPD veio instituir nas Organizações, sendo que as mesmas, em determinadas

[3] JORGE MIRANDA, Ideias para uma revisão constitucional… cit. p. 15.
[4] Cfr. CATARINA Santos Botelho, A Tutela Directa dos Direitos Fundamentais… cit., p. 151, e ULLI F. H. RÜHL, op. cit., p. 157.

situações, terão mesmo de nomear um EPD para assegurarem o cumprimento do Regulamento Geral sobre a Proteção de Dados.

Essencialmente, este trabalho irá incidir sobre o Encarregado de Proteção de Dados, no sentido de apurar quando é obrigatória ou não a sua constituição numa organização, irá também ser abordada a questão de qual a posição do EPD na organização que o constituiu, desde o seu envolvimento na organização aos conflitos de interesse e, claro está, iremos dar uma enorme relevância a verificar quais as suas funções e obrigações.

Esta investigação terá por base uma metodologia do tipo qualitativo assente na recolha e análise bibliográfica e documental, constituindo, por isso, um estudo interpretativo fruto de uma revisão bibliográfica narrativa. Num primeiro momento da investigação procedeu-se a um levantamento bibliográfico de aspetos históricos, socioeconómicos, culturais sobre o conceito de Encarregado de tratamento de dados que servissem de base à contextualização e enquadramento do Direito Português, assim como ao conjunto de componentes subjacentes a este.

Deste modo, colocou-se como questão de investigação: O que o novo Regulamento trouxe de novo para o EPD?

Tornando esta pergunta como um princípio, esta tese apresenta contribuições e propostas para este fim, com base em vários pontos de vista e boas práticas provenientes dos diversos pontos do globo. O que diferencia esta forma de avaliar a qualidade dos processos das outras formas de avaliar é que a esta irá agregar todos os pontos de vista das entidades e pareceres individuais selecionados, todos os itens defendidos por estas entidades, todas as culturas, todas as missões e todos os objetivos para construir uma só forma de avaliar os materiais institucionais e, nesta perspetiva não foi encontrado nenhum estudo semelhante.

A pesquisa e a escrita jurídica é uma matéria que lida com habilidades e técnicas adequadas para encontrar materiais legais relevantes e usá-los no processo de escrever ou na lei ou sobre a lei.

O método jurídico abrange, assim, o procedimento utilizado pelos tribunais, advogados, consultores jurídicos e qualquer outra pessoa que precise tomar uma posição sobre uma questão jurídica específica para encontrar a solução certa para um problema de uma perspetiva jurídica. Em primeiro lugar, o método consiste numa descrição e uma identificação das fontes do direito, que formam a base válida do argumento jurídico. Em segundo lugar, é a teoria de como as fontes do direito devem ser interpretadas. O método jurídico contém elementos significativos de avaliação e estimativa e é, consequentemente, menos exato do que os métodos usados em muitas outras áreas.

Toda a pesquisa científica, incluindo a pesquisa jurídica, parte de suposições. A maioria dessas suposições são paradigmáticas. Isso significa que são geralmente premissas reconhecidas (‘verdades’) dos estudos jurídicos dentro desse sistema legal, ou as suposições comuns de todos os sistemas jurídicos comparados com a pesquisa. Estes constituem a estrutura paradigmática, que tende a não ser debatida como tal dentro da própria disciplina. Além disso, os pesquisadores também podem partir de premissas que são menos óbvias. Nesses casos, tem de ser explicitado, mas não necessariamente justificado. Em alguns desses casos, o resultado da pesquisa só será útil na medida em que se aceite a sua base subjacente.

Capítulo 1 – O Encarregado da Proteção de Dados

Parte introdutória ao capítulo

Ao nível internacional, o regime de proteção de dados centrava-se inicialmente nas disposições da Diretiva 95/46/CE, normas para "proteger os direitos e liberdades fundamentais das pessoas singulares e em particular o seu direito à privacidade no que diz respeito ao tratamento de dados pessoais", principalmente no Espaço Económico dos Estados-Membros[5].

As disposições padrão impõem restrições bastante severas relativamente ao direito à liberdade de expressão[6], incluindo o que tradicionalmente tem sido entendido como o núcleo desse mesmo direito, ou seja, a colheita, armazenamento e transmissão de informações e ideias pela média profissional. No entanto, no que se relaciona com a expressão dos meios de comunicação, os Estados-Membros são obrigados a prever anulações às disposições, mas somente "se forem necessárias para conciliar o direito à privacidade com as regras que regem a liberdade de expressão"[7], ou seja, somente se "necessário para efeitos de equilíbrios entre os direitos fundamentais"[8].

A Diretiva de Proteção de Dados da UE 95/46/CE vincula os 28 estados membros da UE juntamente com mais três países associados (Islândia, Liechtenstein e Noruega) que, no seu conjunto, constituem o EEA. No que diz respeito aos dados do sector privado "controllers", aplica-se qualquer "processamento" de "dados pessoais" efetuado "total ou parcialmente por meios automáticos"[9] ou parte de um sistema de arquivo manual "estruturado de acordo com critérios específicos dos indivíduos, de modo a permitir um acesso fácil aos dados pessoais em questão". Não obstante a nomenclatura técnica e abstrusa, "dados pessoais" na verdade engloba "qualquer informação relativa a uma pessoa singular identificada ou identificável ("titular de dados")[10].

[5] Diretiva 95/46, art. 1
[6] Diretiva 95/46, art. 9
[7] Artigo 9
[8] Diretiva 95/46, recital 37.
[9] Diretiva 95/46, art 3.
[10] Diretiva 95/46, recital 15.

No ano de 2017 as principais questões de privacidade e proteção de dados no mundo centraram-se mais uma vez nos desafios da transferência de dados pessoais entre a União Europeia e os Estados Unidos. E, em outubro do mesmo ano, mais de 2500 organizações tinham certificado a conformidade com as normas do *Transatlantic Privacy Shield*.

Ainda em 2017, a UE também se concentrou intensamente em si mesma. A nova proteção geral de dados e o regulamento (RGPD), que entraram em vigor em maio de 2018, deteve a atenção das empresas dentro e fora da Europa devido ao seu potencial para impor as penalidades significativas. Violações podem resultar em pagamentos de 20 milhões de euros ou 4% da faturação global, sendo que se aplica o que for maior. Além disso, o RGPD será aplicado não apenas às empresas estabelecidas na UE, mas também àqueles que processam dados sobre os europeus na UE ou monitorizarem as atividades em linha de indivíduos aí localizados. Os direitos humanos abrangem liberdade, participação, solidariedade, acesso, inclusão, equidade, justiça e interculturalidade.

Assim, “Dados pessoais" é definido como "qualquer informação relativa a uma pessoa singular identificada ou identificável" (artigo 4.º). É "identificável" se a pessoa singular puder ser identificada através de "todos os meios suscetíveis de serem utilizados", a informação é considerada dados pessoais.

O novo regulamento obriga a garantir o exercício dos direitos dos titulares dos dados. Desta forma, os pedidos de exercício desse direito passam a ser monitorizados e documentados com prazos máximos de resposta, direito à portabilidade dos dados, à eliminação dos dados e à notificação de terceiros sobre a retificação, apagamento ou limitação de tratamento solicitados pelos titulares.

1.1 Evolução e definição

Embora o direito da proteção de dados não seja um ramo jurídico novo, é inegável que somente o RGPD tenha assumido no nosso ordenamento jurídico uma

maior visibilidade jus-científica[11]. As principais razões para esta descoberta estão nos pioneiros do seu estudo que representam uma reflexão da revolução descrita pelo RGPD, destacando a densificação dos direitos dos titulares de dados pessoais, o aumento dos deveres dos responsáveis pelo tratamento de dados e dos subcontratantes, o reforço das competências das autoridades de controlo ou a obrigação da designação de encarregados de proteção de dados.

Não obstante, nos termos do RGPD os responsáveis pelo tratamento e os subcontratantes estão obrigados a designar um EPD, nomeadamente todas as autoridades e organismos públicos, e associações com atividade principal para o controlo de pessoas de forma sistemática e numa ampla escala[12].

Importa realçar que a figura do Encarregado de Proteção de Dados não é nova e absoluta do RGPD, sendo que na diretiva nº 95/46/CE de 25 de outubro, a qual previu sem uma natureza imperativa a possibilidade de que outros direitos internos consagrassem inteiramente esta função, pelo que garantia segundo o artigo 19º, nº 2, a aplicação ao nível interno das disposições nacionais exercidas no âmbito da diretiva nº 95/46/CE mantendo um registo de tratamentos efetuados pelo responsável pelo tratamento que deveriam conter (a) o nome e o endereço do responsável pelo tratamento e, eventualmente, do seu representante; (b) as finalidades do tratamento; (c) uma descrição dos dados pessoais ou dos titulares de dados; (d) os destinatários a quem os dados poderiam ser comunicados; e (e) as transferências de dados previstas para países terceiros[13].

Posteriormente, através da análise da Proposta da Comissão, o Parlamento Europeu efetuou uma grande reformulação da aliena b) do artigo 35º, nº 1, sendo que quando o "tratamento for efetuado por uma pessoa coletiva e afetar mais de 5000 titulares de dados durante um período de 12 meses consecutivos"; e adicionalmente, a

[11] Por contraste, no direito alemão, o direito da proteção de dados há longas décadas que assume enorme preponderância científica e prática. Para lá do reno, multiplicam-se anotações legislativas, revistas especializadas e densas monografias

[12] a lei n.º 67/98, de 26 de outubro, não previa essa possibilidade. a figura do EPD foi introduzida no direito alemão em 1977. Curiosamente, os critérios vigentes na Alemanha, antes da entrada em vigor do RGPD, eram mais rigorosos do que os impostos atualmente pelo direito europeu: Horst HeBerlein, Anotação ao artigo 37.º do RGPD em Ehmann/Selmayr, Datenschutz-Grundverordnung Kommentar, 2.ª ed., Beck, munique 2018, rn. 2

[13] art. 19.º/1, via art. 21.º/2, via art. 19.º/2.

designação de delegado para a proteção de dados que deveria ser obrigatória sempre que "as atividades principais do responsável pelo tratamento ou do subcontratante consistem em proceder ao tratamento de categorias especiais de dados nos termos do art. 9.º, n.º 1, dados de localização ou dados relativos a crianças ou a trabalhadores em sistemas de arquivo de grande dimensão"[14].

O EPD deve ser designado "com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39º"[15], ao mesmo tempo que o EPD pode ser um elemento responsável pelo tratamento ou pode exercer as suas funções de acordo com um contrato de prestação de serviços[16].

Não obstante, o GT29 (2016) estabeleceu o âmbito das qualidades profissionais que o EPD deve ter e esclareceu 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 para promover uma cultura de proteção de dados no seio da organização" (p.26).

Tendo em consideração que as funções do EPD devem ter como base a total independência e, de acordo com o artigo 38º nº 3, o responsável pelo tratamento e o subcontratante têm como responsabilidade assegurar 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

[14] Parlamento europeu, Relatório sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral de proteção de dados), 21-nov.-2013, 130
[15] Número 5 do artigo 37.º do RGPD.
[16] Número 6 do artigo 37.º do RGPD.

como responsabilidade do EPD. A figura seguinte demonstra as principais funções do EPD:

Figura 1 – funções do EPD

No que se relaciona com a certificação do EPD, a realidade determina que é o RGPD no seu artigo 37º, nº 5 que não exige a sua certificação para o exercício das funções relacionadas, sendo que o nº 1, do artigo 9º, da Lei nº 58/2019 de 8 de agosto dispõe do mesmo sentido.

1.2 Autoridade legislativa relacionada com o EPD

Ao nível legislativo, o EPD pode integrar ou não a estrutura interna do responsável ou mesmo o subcontratante, neste caso podendo-se tratar de um trabalhador como prestador de serviço externo, descrito no artigo 37º/6, onde a entidade designadora recorre a um trabalhador interno, sendo que no caso da posição do EPD externo, de acordo com o regime em vigor, deve ser exercido por advogados especialistas em direito de proteção de dados[17].

Os responsáveis pelo tratamento de dados, bem como os subcontratantes têm obrigação de apoiar o EPD no exercício das suas funções, enquanto lhes fornece os

[17] HeBerlein, Anotação ao artigo 37.º do RGPD em Ehmann/Selmayr, cit., rn. 41.

recursos necessários para o desempenho, artigo 38º/2[18], e devem assegurar que o EPD é envolvido adequadamente e em tempo útil, em todas as questões que se relacionam com a proteção de dados (art. 38.º/1).

As entidades designadoras devem igualmente, assegurar a presença regular do EPD nas reuniões mais importantes, e sempre que sejam tomadas as decisões relacionadas com os dados pessoais ou titulares de dados deve ser efetuada a sua presença informada.

Está previsto no artigo 37º, nº 1, do RGPD a nomeação obrigatória de um encarregado de proteção de dados para as autoridades e organismos públicos, com exceção dos tribunais, em relação ao exercício da sua função jurisdicional. Segundo o consagrado no mesmo artigo e no nº 3, está posta em causa uma autoridade ou organismo público, podendo existir um único EPD para "várias dessas autoridades e organismos, tendo em conta a respetiva estrutura organizacional e dimensão".

De acordo com as palavras de FILIPA GALVÃO[19], o "delegado assume em boa medida as funções de controlo prévio e sucessivo que tradicionalmente eram da competência da autoridade administrativa (cf. artigo 37.º), constituindo a obrigação legal da sua criação uma expressiva manifestação da transferência do poder de controlo da autoridade administrativa para o próprio responsável pelo tratamento, que em outros planos, tem vindo a ser institucionalizado como sucede do domínio do direito do ambiente".

1.3 Controlo Regular e Sistemático

Ao longo do texto do RGPD estão incluídos diversos termos abrangentes e, com necessidade de clarificação. Como exemplo, o "controlo regular e sistemático dos titulares dos dados em grande escala". Pois, de acordo com o artigo 37º, nº 1, aliena b) no caso em que a atividade principal de um determinado responsável por tratamento de dados, compreenda pela sua natureza, âmbito e finalidade ou que exija o controlo de

[18] GT 29, Orientações sobre os EPDs, cit., 16-17: apanhado dos meios e recursos que as entidades designadoras devem disponibilizar aos ePds.

[19] CALVÃO, Filipa – "O modelo de supervisão de tratamentos de dados pessoais na União Europeia: Da atual Diretiva ao futuro Regulamento", Revista Fórum de Proteção de Dados, n.º 1, julho de 2015, p. 42

titularidades de dados pessoais que a expressão indica, serão colocadas maiores obrigações, como é o caso da obrigatoriedade de designação de um Encarregado da Proteção de Dados[20].

A noção de "controlo regular e sistemático" não se encontra definida no RGPD. De acordo com o G29 esta definição inclui todo o tipo de monitorização e definição de perfis na Internet. Contudo, não se restringe apenas ao ambiente on-line. v. G29, *Guidelines on Data Protection Officers* ('DPOs'), pp. 8 e 9

Como exemplos de atividades que constituem um controlo regular e sistemático dos titulares de dados, são a exploração de uma determinada rede de telecomunicações, a prestação de serviços de telecomunicações, reorientação de mensagens de correio eletrónico, atividades de promoção comercial que se baseiam em dados, a definição de perfis específicos, a prevenção de fraudes, bem como a deteção de casos de branqueamento de capitais.

Importa ainda referir que de acordo com o GT 29, a palavra "regular" significa uma das seguintes características: contínuo ou que ocorre a intervalos específicos num determinado período, recorrente ou repetido em horários estipulados, e o constante ou periódico.

1.4 Recursos necessários

O artigo 38.º, n.º 2, do RGPD exige que a organização apoie o seu EPD, "fornecendo-lhe os recursos necessários ao desempenho [das suas] funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento". Em especial, devem ser considerados um conjunto de aspetos tais como, o apoio ativo relacionado com as funções do EPD de acordo com os quadros de gestão superiores, o tempo necessário para que estes exerçam as suas atribuições.

O RGPD exige na sua redação, que a organização apoie o EPD, nomeadamente no nº2 do artigo 38.º, quando diz "favorecendo-lhe os recursos necessário ao

[20] Cf. RGPD, Artigo 37º.

desempenho das suas funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento".

Desta forma, podemos considerar que se torna importante às organizações, darem um apoio apropriado, no que respeita aos recursos financeiros, às infraestruturas e ao pessoal, sempre que indispensável ao EPD.

É da mesma forma importante existir uma comunicação oficial da nomeação do EPD por todo o pessoal da organização, assim como dar formação contínua ao EPD, de forma a se manterem atualizadas no que diz respeito à Proteção de Dados Pessoais. De modo geral, quanto mais complexas forem as operações de tratamento, com mais recursos deve a organização munir o seu EPD.

O RGPD apenas prevê que a autoridade de controlo promova a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações de acordo com o Regulamento. De acordo com as funções do Encarregado da Proteção de Dados na organização, este pode desempenhar um papel importante na intermediação de todas as ações de sensibilização[21].

1.5 Destituição ou Penalização do EPD

Para que seja garantida a independência do EPD o legislador proíbe expressamente a sua destituição e penalização, motivada pelo exercício das suas funções legais (artigo 38º, nº 3), sendo que esta proibição deve ser interpretada extensivamente, de forma a incluir qualquer tipo de penalização, fática ou jurídica, incluindo as simples ameaças, diretas ou indiretas de destituição ou de penalização[22].

De acordo com o artigo 17.º - Encarregado de Proteção de Dados, "*O Encarregado de Proteção de Dados não recebe instruções relativamente ao exercício das suas funções, nem pode ser destituído nem penalizado pelo responsável pela instituição de saúde pelo facto de exercer as suas funções*" (nº3)

[21] Cf. Artigo 57.º, n.º 1, alínea d) do RGPD
[22] GT 29, Orientações sobre os EPDs, cit., 18.

Importa referir que as penalizações não são autorizadas de acordo com o RGPD no caso em que sejam impostas em resultado do exercício efetivo de funções do EPD. Assim, no caso em que o EPD possa considerar que um tratamento determinado é suscetível de levar a um elevado risco e aconselhar o responsável a realizar uma avaliação de impacto sobra Proteção de Dados. Embora, o RGPD não torna específico como e quando o EPD pode ser afastado ou substituído por outra pessoa.

A primeira de todas as obrigações do EPD está presente no número 2 do artigo 5.º do RGPD: "O responsável pelo tratamento é responsável pelo cumprimento do disposto no número 1 e tem de poder comprová-lo («responsabilidade»)."

1.6 Conflitos de interesses

A ausência de conflitos de interesses está diretamente ligada ao requisito de não dependência do EPD, embora este esteja autorizado a desempenhar outras tarefas, só podem ser cumpridas outras funções e atribuições se estas não originarem conflitos de interesses. Assim, o EPD não pode exercer um cargo dentro da organização que o conduza a determinar as finalidades e os meios de tratamento de dados pessoais.

Nas palavras de Paulo Mota Pinto[23], o conceito de interesses assume muitos significados, sendo este utlizado em contextos infindáveis. A sua transversalidade do conceito é igualmente, uma característica do mundo jurídico e da linguagem. Os vários contextos jurídicos em que este conceito pode ser utilizado correspondem à necessidade de separar as suas várias aceções para que se dê uma relevância científica e prática no momento do seu preenchimento.

Não obstante, existem conflitos sempre que a posição do EPD seja assumida pelo titular de uma posição de chefia, como diretor executivo, diretor de operações, entre outras. Isto porque o EPD tem como responsabilidade a verificação e adequação das atividades desenvolvidas por estes departamentos[24]. Os conflitos de interesses podem ainda existir no caso de funcionários menos graduados, importando assim, a

[23] Paulo mota Pinto, Interesse contratual negativo e interesses contratual positivo, i, Coimbra editora, Coimbra, 2008, 81, ss e 481, ss.
[24] GT 29, Orientações sobre os EPDs, cit., 19

averiguação antes de proceder à sua designação e existência ou não de conflitos de interesses[25].

Importa referir que ao optar-se por um prestador de serviços, os responsáveis pelo tratamento e os subcontratantes não podem designar um sujeito que assuma as outras posições ou atividades e, que sejam incompatíveis.

De acordo com o Regulamento (CE) 45/2001[26], o EPD é responsável por garantir que os titulares de dados sejam informados dos seus direitos e obrigações de acordo com o artigo 24º, nº 1, alínea a). E, de acordo com o mesmo artigo, nº 3, o EPD não deve ter conflitos de interesse relacionados com os deveres e outras funções oficiais.

Segundo o artigo 24º, nº 3, existe a presença de um conflito de interesses quando as funções de um EPD têm interesse distinto aos de proteção de dados pessoais dentro da instituição.

Por outro lado, a independência na prática não está definida atualmente de forma clara. Alguns países procuram garantir a independência funcional restringindo outras funções e responsabilidades que o EPD pode cumprir. Como exemplo, na Alemanha, o papel do EPD é considerado incompatível com um conjunto de outras funções e responsabilidades. Assim, o dono da empresa, os membros do conselho e o diretor administrativo, bem como os que possuem funções potencialmente conflituantes não podem assumir a função do EPD[27].

A finalidade do legislador Europeu segundo MAFALDA MIRANDA BARBOSA, é garantir que embora os dados passarem a ser utilizados com outro

[25] Bergt, Anotação ao artigo 37.º do RGPD em Kühling/Buchner, cit., rn. 40.
[26] Regulamento (CE) n.o 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).
[27] A Lei Federal de Proteção de Dados, conforme interpretada por uma resolução do Düsseldorfer Kreis

objetivo, as garantias de segurança que são disponibilizadas pelo RGPD ao titular dos dados se possam manter, não dependendo da ilicitude que tal possa implicar[28].

1.6.1 Transferência de dados pessoais para países terceiros

Tendo em conta que as transferências de dados pessoais é um elemento central das relações entre países, e principalmente nas relações comerciais, o RGPD reforçou as regras relacionadas com a transferência de dados pessoais para países terceiros (Comissão Europeia, 2015, p. 2).

De acordo com a 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, tal aplica-se também quando os dados são transferidos para um país que não seja membro da UE (país terceiro)"[29].

Ora, no seu memorando 56, a Diretiva reconheceu que os fluxos transfronteiriços de dados pessoais são importantes para o desenvolvimento do comércio internacional, embora estabeleceu no seu artigo 25º, que estas transferências de dados pessoais para outros países, só poderão ocorrer se estes países assegurarem um nível de proteção adequado. E, no seu memorando 57, determinou que as transferências de dados pessoais para países que não disponibilizem um nível de proteção adequado deve ser proibida e, em adição do memorando 60, as transferências só poderão ser realizadas no pleno respeito pelas disposições que sejam adotadas por cada um dos países europeus em termos da Diretiva.

Não obstante, o regulamento descreve a proibição geral de envio de dados pessoais para países que não façam parte da Comunidade Europeia[30] e que não garantam a proteção adequada, estabelecendo assim, no seu artigo 44º que qualquer tipo

[28] Mafalda Miranda Barbosa, Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil, RDCom, 15-mar.-2018, p.436 e ss

[29]Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/whatrules-apply-if-my-organisation-transfers-data-utside-eu_pt, consultado a 20/09/2020

[30] O Espaço Económico Europeu é constituído pelos 28 Estados-Membros da União Europeia, Islândia, Noruega e Liechtenstein.

de transferência de dados pessoais para um país terceiro só poderá ser realizada se forem cumpridas as condições que estão estabelecidas no capítulo V do RGPD.

A este aspeto, MARTINS[31] refere que, "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).

1.7 Funções do Encarregado da Proteção de Dados

A institucionalização do EPD une uma forma de desburocratização e descentralização da proteção de interesses dos titulares de dados pessoais, enquanto atribui aos responsáveis pelo tratamento de dados e aos seus subsequentes a responsabilidade de autorregularem as suas atividades, reduzindo assim a necessidade de uma intervenção constante por parte do supervisor[32]. A posição do EPD deve estar sempre enquadrada na funcionalização do RGPD e na proteção dos interesses dos titulares dos dados pessoais[33].

Não obstante de acordo com o artigo 39º, nº 1 existem quatro funções principais do EPD:

1) O EPD informa e aconselha o responsável pelo tratamento ou o subsequente, bem como os trabalhadores que tratem dos dados, relacionados com as suas obrigações, de acordo com o RGPD e legislação aplicável

2) Controla o cumprimento do RGPD e de toda a legislação associada, bem como das políticas das entidades designadoras relacionadas com a proteção dos dados pessoais, incluindo a repartição de responsabilidades, a

[31] 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

[32]Klug, Anotação ao artigo 37.º do RGPD em Gola, cit., rn. 1.

[33] Klug, Anotação ao artigo 37.º do RGPD em Gola, cit., rn. 2.

sensibilização e formação do pessoal implicado nas atividades de tratamento de dados

3) Presta aconselhamento, quando lhe seja solicitado relacionado com a avaliação do impacto sobre a proteção de dados e controla a sua realização de acordo com o artigo 35º

4) Atua como contacto com a autoridade de controlo sobre as questões relacionadas com o tratamento, consulta prévia de acordo com o artigo 36º, devendo mesmo assim, consultar a autoridade de controlo quando se justificar

O EPD deve realizar as suas funções de acordo com um conjunto de princípios, como é o caso da ***probidade***, ou seja, o EPD deve desempenhar todas as suas atividades com diligencia, lealdade, responsável, de forma honesta, tendo como base o seu conhecimento e perícia, ao serviço do responsável pelo tratamento de dados ou subcontratante. Assim, como consequência este profissional deve ser cuidadoso na utilização das normas, marcas, materiais ou recursos. Temos também o Princípio da ***imparcialidade***, ou seja, o EPD deve desempenhar as suas atividades com objetividade, independência, equidade, sem julgamentos prévios, com ausência de conflitos de interesses e, sem preconceitos e resistência à influência abusiva. No Princípio da ***objetividade***, ou seja, o EPD deve demonstrar um alto nível de objetividade e clareza na sua análise, avaliação e comunicação com o responsável de tratamento de dados ou com o subcontratante.

No princípio da i***ndependência***, o EPD deve definir e divulgar os meios para garantir a independência do profissional de proteção de dados. Ao mesmo tempo que se deve abster de interferir nas atividades que possam conduzir ao conflito de interesses.

Para além destes princípios, o EPD tem ainda como base outros princípios importantes na sua conduta de atividade. O princípio da licitude, lealdade e transparência, de acordo com o artigo 5º, nº 1, alínea a) do RGPD refere que os dados pessoais são “objeto de tratamento lícito, leal e transparente em relação aos titulares de

dados". Neste contexto, os dados pessoais terão que ser tratados licitamente, ou seja, "deverão ser tratados com base no consentimento do titular dos dados em causa"[34].

No que concerne ao princípio da ***lealdade,*** o tratamento de dados pessoais deve ser efetuado de forma leal, o mesmo significa, com a finalidade a que se destinam e não a outro, e assim fortalecer a ligação entre a organização e o titular de dados pessoais, pelo que este último ficará consciente de que os seus dados podem ser utilizados, compreendidos e salvaguardados pela entidade que os acolheu.

Do mesmo modo, o princípio da ***transparência*** está relacionado com a certeza imediata do titular de dados pessoais, e no que diz respeito à recolha, utilização e consulta, ou seja, este princípio "… diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhe dizem respeito que estão a ser tratados"[35].

No que diz respeito ao princípio da ***limitação das finalidades***, de acordo com o artigo 5º, nº 1, alínea a) e b) do RGPD, traduz que os dados pessoais são "recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1"[36].

O princípio da ***minimização dos dados*** de acordo com o artigo 5º, nº 1, alínea c) do RGPD refere que os dados pessoais são "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados."

[34] Considerando (40) do RGPD.
[35] Considerando (39), (58) e (59) do RGPD
[36] Considerando (39) do RGPD.

1.7.1 Controlo da conformidade com o RGPD

O fundamento legal para a adoção do RGPD está consagrado no artigo 16º, nº 2 do Tratado sobre o Funcionamento da União Europeia (TFUE), que refere "(…) 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 atos. (...)"[37].

Sendo o RGPD aplicável diretamente no que respeita à proteção de dados, os Estados-Membros devem atualizar as suas leis nacionais de proteção de dados existentes e alinharem-se com o Regulamento, conduzindo a disposições especificas[38]. Sobre este aspeto, ALEXANDRE SOUSA PINHEIRO[39] refere que "(...) não pensamos que o RGPD possa ser considerado como um texto paradigmaticamente unificador da matéria da proteção de dados no domínio da União Europeia. Esta conclusão é extraída pela abertura legislativa fornecida aos Estados-Membros, não pela atuação das autoridades de controlo cuja ação está sujeita ao procedimento do controlo da coerência."

De igual forma, nas palavras de HENRIQUES GORJÃO[40], o RGPD já tinha previsto uma série de regras em consonância com a proteção de dados em toda a União Europeia, e estabeleceu um ambiente de segurança jurídica através do qual os operadores económicos e os titulares dos dados podem beneficiar, o que contribuiu para a própria modernização da legislação existente na UE.

Uma das alterações do RGPD relativamente à legislação anterior em matéria de proteção da privacidade e de dados pessoais consiste no facto de conferir aos titulares de dados pessoais um conjunto de novos direitos.

---

[37] Neste sentido veja-se MAÑAS, José Luís Piñar, Antecedentes e processo de reforma sobre protección de datos personales en la Unión Europea in Regulamento General de Protección de Datos. Hacia un nuevo modelo europeo de protección de datos, 2016, p. 49.

[38] Cf., por todos, MACHADO, Jónatas E. M., Direito da União Europeia, 2010, p. 199-201, e HENRIQUES, Miguel Gorjão, Direito da União Europeia, 2014, p. 296.

[39] PINHEIRO, Alexandre Sousa, Comentário ao Regulamento Geral de Proteção de Dados, 2018, p. 21

[40] HENRIQUES, Miguel Gorjão, Direito da União Europeia, 2014, p. 296

De outro modo, o RGPD define um conjunto de direitos ao Titular dos Dados Pessoais, como o Direito de Acesso; Direito de Retificação e de ser notificado dessa retificação; Direito de Limitação; Direito ao apagamento dos dados ("direito ao esquecimento") e ser notificado desse apagamento; Direito de portabilidade dos dados; Direito de oposição ao tratamento e a decisões individuais automatizadas (definição de perfis) e Direito de Reclamação e de Acão.

Assim, o Direito de Acesso, consagrado no artigo 15º, diz-nos que o titular de dados pessoais tem o direito de aceder a todos os seus dados pessoais que existem, e também daqueles que foram recolhidos e registados em cada instituição. O direito de Retificação, enunciado no artigo 16º, descreve que o titular dos dados pessoais tem o direito de correção de todos os dados pessoais recolhidos por cada instituição. O Direito ao Apagamento, (esquecimento) consagrado no artigo 17º descreve que o titular de dados pessoais tem o direito de solicitar o apagamento de todos os seus dados pessoais existentes, recolhidos e registados em cada instituição com exceção dos que tenham que ser conservados por definição de prazo legal. O Direito à limitação do tratamento – artigo 18º, que institui que o titular de dados pessoais tem direito a limitar o tratamento dos seus dados pessoais solicitando o exercício da recolha dos dados estritamente necessários ao exercício da finalidade em causa, bem como a definição clara da finalidade a que o tratamento de dados se destina e o prazo de conservação dos mesmos;

Sendo que o Direito de portabilidade dos dados, que consagrado no artigo 20º, o titular de dados pessoais tem direito a receber os seus dados pessoais e a transmitir esses dados a outro responsável pelo tratamento, sempre que esses dados tenham sido fornecidos pelo seu titular a um responsável de tratamento com base no consentimento ou num contrato e se o tratamento de dados for realizado por meio automatizados.

O direito de oposição, descrito no artigo 21º, consagra que o titular de dados pessoais tem direito de se opor ao tratamento de dados incluindo a definição de perfis, se não tiver concedido consentimento para o efeito ou se o tratamento não decorrer, designadamente, de um contrato, de procedimentos judiciais ou defesa dos seus interesses vitais, entre outros (nº2 do artigo 9º).

Temos também o direito a não ficar sujeito a decisões individuais automatizadas, sendo que o direito está enunciado no artigo 22º, e diz-nos que o titular de dados pessoais tem o direito a não ficar sujeito a decisões tomadas com base no tratamento automatizado, incluindo a definição de perfis, se esse facto puder produzir efeitos que o venham a afetar na sua esfera jurídica ou outra.
Importa ainda referir que, de acordo com a perspetiva operacional, a exigência de comprovação da conformidade com o regulamento altera toda a forma de encarar o problema da proteção de dados nas organizações. Assim, até maio de 2018, a proteção de dados foi sempre regulada por um ponto de vista de hétero-regulação, ou seja, existia a necessidade de garantir a licitude do tratamento por meio dos princípios e condições de legitimidade, e que ocorria na fase inicial, através de meios definidos anteriormente pela autoridade de controlo.

Não obstante, a demonstração de conformidade com o regulamento e com as boas práticas respeitadas no tratamento de dados pessoais, são motivo de uma elevada relevância pois estão em conformidade. E, como tal, o RGPD fornece as ferramentas que podem ser importantes no auxílio desta tarefa da demonstração de conformidade, através do registo das atividades realizadas, marcas e selos, certificações, códigos de conduta[41].

1.7.2 Papel do EPD no âmbito da AIPD

Primeiramente importa referir que uma AIPD é um processo concebido para descrever o tratamento, avaliar a necessidade e a proporcionalidade deste tratamento, bem como ajudar na gestão dos riscos para os direitos e liberdades das pessoas singulares e relacionada com o tratamento de dados pessoais.

O Regulamento 2016/679 (RGPD)[42] está aplicável desde 25 de maio de 2018, e é o artigo 35º deste Regulamento que descreve o conceito de Avaliação de Impacto sobre a Proteção de Dados, de acordo com a Diretiva 2016/680[43].

[41]Artigo 40.° do RGPD - Secção 5 - Códigos de conduta e certificação
[42] Regulamento (UE) n.º 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).

Neste contexto, uma AIPD representa um processo concebido para descrever o tratamento, avaliar a necessidade e a proporcionalidade deste tratamento e ao mesmo tempo auxiliar na gestão dos riscos nos direitos e liberdades de pessoas singulares no tratamento de dados pessoais[44].

Importa ainda referir que de acordo com o RGPD, a não conformidade com os requisitos da AIPD, pode conduzir a sanções impostas pelas autoridades de controlo competentes. De igual modo, a não realização de uma AIPD no caso em que o tratamento esteja sujeito a ela (artigo 35.º, n.º 1 e nº 3 a 4), realizá-la de uma forma incorreta (artigo 35.º, n.º 2 e nº 7 a 9), ou não consultar a autoridade de controlo competente quando necessário (artigo 36.º, n.º 3, alínea e)), podendo em qualquer dos casos conduzir a uma coima de elevado valor.

Segundo a abordagem que se baseia no risco integrada no RGPD não se torna obrigatório a realização de uma AIPD em todas as operações de tratamento, embora exista a obrigação de realizá-la no caso em que o tratamento "for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (artigo 35.º, n.º 1).

De acordo com o artigo 70º, nº 1 alínea e) o Comité Europeu para a Proteção de Dados (CEPD) tem como habilitação emitir algumas diretrizes, recomendações e melhores práticas com o objetivo de incentivar a aplicação coerente do RGPD.

E, ainda, a AIPD pode ser igualmente útil na avaliação do impacto na proteção de dados de um produto tecnológico, como os programas informáticos sempre que estes estejam suscetíveis de serem utilizados por vários responsáveis pelo tratamento de dados que lança o respetivo produto. Neste caso, o responsável pelo tratamento de

---

[43] O artigo 27.º da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, também refere que é necessária uma avaliação de impacto na privacidade «[c]aso um tipo de tratamento [...] seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares»

[44] O RGPD não define formalmente o conceito de uma AIPD propriamente dita, mas, o seu conteúdo mínimo encontra-se especificado no artigo 35.º, n.º 7, da seguinte forma: o «a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;

dados que lança o produto está obrigado a realizar a sua própria AIPD em relação à implementação específica e com base nas informações desta.

Assim, a realização de uma AIPD torna-se obrigatória somente quando o tratamento for "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (artigo 35.º, n.º 1, ilustrado pelo artigo 35.º, n.º 3, e complementado pelo artigo 35.º, n.º 4). Com o objetivo de disponibilizar uma série de operações de tratamento que exigem uma AIPD relacionadas com o risco elevado e, tendo como base os elementos específicos dos artigos 35º, nº 1, e nº 3 alíneas a) a c), deve ser adotados os considerandos 71, 75 e 91, e as referências do RGPD com relação às operações de tratamento "suscetíveis de implicar elevado risco", de acordo com um conjunto de nove critérios:

1) A avaliação ou a classificação, bem como a definição de perfis e previsão, especialmente de "aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferência ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados" (considerandos 71 e 91). Importa referir que neste critério pode incluir uma instituição financeira que tenha controlo seletivo dos seus clientes de acordo com uma base de dados ao combate ao branqueamento de capitais e financiamento ao terrorismo e fraudes.

2) Decisões automatizadas que tenham efeitos jurídicos ou possam afetar de forma significativa, o tratamento relacionado coma pessoa singular (artigo 35º, nº3, alínea a)). Como exemplo, o tratamento que implique a exclusão ou a discriminação de pessoas.

3) O controlo sistémico, ou seja, o tratamento utilizado na observação, monitorização ou controlo de titulares dos dados, incluindo os dados recolhidos através de redes, ou em alguns casos "o controlo sistemático de zonas acessíveis ao público" (artigo 35º, nº 3, alínea c))[45]. Este critério é

[45] O Grupo de Trabalho do Artigo 29.º interpreta «sistemático» como significando um ou mais dos seguintes pontos (ver as orientações do Grupo de Trabalho do Artigo 29.º sobre o encarregado da proteção de dados 16/PT WP 243):
- que ocorre de acordo com um sistema;
- pré-determinado, organizado ou metódico;
- que acontece como parte de um plano geral de recolha de dados;
- realizado como parte de uma estratégia.

importante porque as pessoas podem não estar cientes de quem está a recolher os seus dados e, da forma como estão a ser tratados.

4) Os dados sensíveis ou dados de natureza altamente pessoais, inclui as categorias especiais de dados pessoais, de acordo com a definição integrada no artigo 9º, bem como os dados pessoais que se relacionam com as condenações penais e infrações. Como exemplo, um hospital geral que mantem os registos médicos dos doentes ou um investigador privado que mantem informações sobre os autores das infrações.

5) Os dados tratados em grande escala, ou seja, o RGPD não define de forma clara o que constitui a grande escala, embora o considerando 91 disponibiliza alguma orientação a este respeito. Especialmente, é através do artigo 29º que é recomendado alguns fatores neste caso concreto, ou seja, o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente; o volume de dados e/ou a diversidade de dados diferentes a tratar[46].

6) O estabelecimento de correspondências ou a combinação de um conjunto de dados, como exemplo, a origem em duas ou mais operações de tratamento de dados que são realizadas com vários objetivos distintos, ou por vários responsáveis pelo tratamento de dados.

7) Dados relacionados com os dados vulneráveis descritos no considerando 75, ou seja, o tratamento deste tipo de dados representa um critério devido ao grande desequilíbrio de poder existente entre os titulares dos dados e o EPD, o que significa que os indivíduos podem não ter a capacidade de consentir ou opor-se ao tratamento dos seus dados, ou de exercer os seus direitos, como exemplo as crianças ou segmentos mais vulneráveis como os doentes mentais e idosos

8) A utilização de soluções inovadoras ou a aplicação de novas soluções tecnológicas e/ou organizacionais, que combinem a utilização da impressão digital e o reconhecimento facial com a finalidade de melhorar o controlo do acesso físico (artigo 35º, nº 1, considerando 89 e 91).

O Grupo de Trabalho do Artigo 29.º interpreta «zona acessível ao público» como sendo qualquer local aberto a qualquer membro do público, por exemplo, uma praça, um centro comercial, uma rua, um mercado, uma estação de comboios ou uma biblioteca pública.

[46] Ver as orientações do Grupo de Trabalho do Artigo 29.º sobre o encarregado da proteção de dados 16/EN WP 243.

9) No caso em que o próprio tratamento impede os titulares de dados "de exercer um direito ou de utilizar um serviço ou um contrato" (artigo 22º e considerando 91). Neste caso, o exemplo pode ser quando um banco faz um controlo seletivos dos seus clientes a partir de uma base de dados de referências de crédito bancário com a finalidade de decidir a conceção ou não de um empréstimo.

1.7.3 Cooperação com a autoridade de controlo e função de ponto de contacto

De acordo com o consagrado no artigo 39º, nº 1, alíneas d) e e) o EPD "coopera com a autoridade de controlo" e serve de "ponto de contato com a autoridade de controlo sobre as questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto".

Ora, estas funções correspondem ao papel "facilitador" do EPD, tal como está referido nas orientações. Assim, o EPD serve de ponto de contato com o objetivo de facilitar o acesso da autoridade de controlo aos documentos e informações que sejam necessárias para o desempenho das funções descritas no artigo 57º, e igualmente para o exercício dos seus próprios poderes de investigação, de correção, consultivos e de autorização, de acordo com o descrito no artigo 58º.

Tem-se assim em linha de conta que o EPD se encontra vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União ou dos Estados-Membros (artigo 38º, nº 5), embora não o impeça de consultar a autoridade de controlo se necessário.

Com o objetivo de avaliar o atual grau de interação entre várias autoridades de proteção de dados, foi realizado um exercício no ano de 2015 entre o Centro Comum de Investigação (doravante CCI) da União Europeia em colaboração com a Direção-Geral da Justiça e dos Consumidores da Comissão Europeia e Autoridades de Proteção de

Dados de Sete Estados-Membros (França, Alemanha, Grécia, Irlanda, Itália, Polónia e Espanha)[47]. Este foi o primeiro exercício pan-europeu de violações de dados pessoais.

O tema da cooperação entre as diversas autoridades de proteção de dados é muito debatido, principalmente no que se relaciona com a competência da autoridade de controlo principal (artigo 56º, do RGPD), à cooperação entre a autoridade de controlo principal e as outras autoridades de controlo interessadas (artigo 60º do RGPD), ou à assistência mútua (artigo 61º do RGPD).

1.7.4 Abordagem baseada no risco

De acordo com artigo 39º, nº 2, exige-se ao EPD que tenha "em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento". Ou seja, estão implícitos o princípio geral e o bom senso, que se revela importante em muitos aspetos do trabalho quotidiano do EPD.

É exigido ao EPD que estabeleça prioridades nas suas atividades e centre os seus esforços nas principais questões relacionadas com o risco em matéria de proteção de dados, embora sem negligenciar o controlo da conformidade das operações de tratamento de dados que, nesse contexto trazem consigo algum tipo de risco.

Desde a década de 80 que a gestão de risco tem desempenhado um papel cada vez mais importante para garantir a conformidade das organizações com as leis de proteção de dados e os direitos fundamentais e liberdades dos indivíduos. Neste caso concreto, a gestão de risco está relacionada com processo de identificação sistemática, gerir e mitigar o impacto de uma operação de processamento de dados pessoais na organização e nas pessoas.

A abordagem baseada no risco, que foi prenunciada nos elementos da Diretiva de Proteção de Dados da UE e agora é totalmente aprovado pelo RGPD, que confirma essa tendência. Portanto, ao determinar como implementar a abordagem baseada em

[47] Cf. MALATRAS, Apostolos, et al., «Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities», in Computer Law & Security Review, volume 33, Issue 4, August 2017, Elsevier, p. 458-469, disponível em: https://www.sciencedirect.com/science/article/pii/S0267364917300808.

risco do RGPD e como identificar, gerir e mitigar riscos, é importante basear-se e levar em consideração as leis atuais, pesquisas e orientações sobre risco, avaliação de risco e as avaliações de impacto da proteção de dados (AIPD) no domínio da proteção de dados[48].

A abordagem baseada no risco é antes de mais nada uma ferramenta eficaz para garantir um alto nível de proteção dos direitos e liberdades dos indivíduos. Permite que todas as partes interessadas se dediquem aos seus recursos para as áreas onde os riscos e danos potenciais para os indivíduos são mais significativos e para reduzir ou eliminar esses riscos, criando melhores resultados e mais proteção eficaz para os indivíduos.

De outro modo, ao avaliar a probabilidade e a significância dos impactos (positivos ou negativos) e quaisquer danos potenciais a indivíduos de uma determinada atividade de processamento de dados pessoais, a avaliação de risco ajuda as organizações a conceber controlos eficazes e apropriados para a sua redução. Assim, esta abordagem tem como principal garantia que as organizações maximizem os benefícios potenciais da atividade de processamento de dados, enquanto diminui o impacto negativo da atividade de direitos e liberdades dos indivíduos.

Uma abordagem baseada em risco para a proteção de dados permite uma abordagem flexível e específica no contexto do seu cumprimento. Permite que as organizações possam priorizar as tarefas e utilizem os recursos de forma eficaz. Ora, esta abordagem é bastante relevante para as autoridades de proteção de dados que podem utilizar a gestão de risco para priorizar o cumprimento das suas funções de assessoria e fiscalização.

A abordagem baseada no risco torna possível que os EDP possam implementar os seus recursos de forma eficaz e consistente nas áreas onde exista maior probabilidade e gravidade de riscos e danos aos indivíduos.

[48] Nos últimos três anos, o Centro de Liderança em Políticas de Informação da Hunton & Williams LLP (CIPL) organizou uma série de workshops multinacionais e publicou três white papers sobre gestão de risco e seu papel na proteção de dados moderna eficaz. CIPL, uma abordagem baseada em risco para a privacidade: melhorando a eficácia na prática (2014), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1_a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf; ver também CIPL, The Role of Risk Gestão em Proteção de Dados (2014).

1.7.5 Papel do EPD na conservação do registo de atividades

Nos termos do artigo 30.º, n º1 e 2 do RGPD, é o responsável pelo tratamento dos dados ou o subcontratante, e não o EPD, que "conserva um registo de todas as atividades de tratamento sob a sua responsabilidade" ou "conserva um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento".

Na prática, os EPD criam, por norma, inventários e mantêm um registo das operações de tratamento com base nas informações que recebem dos vários departamentos na sua organização aos quais incumbe o tratamento de dados pessoais. Esta prática foi estabelecida ao abrigo de muitas disposições legislativas nacionais em vigor e em conformidade com as normas de proteção de dados aplicáveis às instituições.

O artigo 39.º, n.º 1 do RGPD, prevê uma lista das funções mínimas que devem incumbir ao EPD.

Por conseguinte, nada impede que o responsável pelo tratamento ou o subcontratante atribua ao EPD a função de conservar o registo das atividades de tratamento sob a responsabilidade do responsável pelo tratamento ou do subcontratante. Esse registo deve ser considerado um dos instrumentos que permitem ao EPD desempenhar as suas funções de controlo da conformidade e de prestação de informação e aconselhamento ao responsável pelo tratamento ou ao subcontratante.

Em qualquer caso, o registo de conservação obrigatória por força do artigo 30.º do RGPD deve igualmente ser encarado como instrumento que permite ao responsável pelo tratamento e à autoridade de controlo, a pedido destes, obter uma perspetiva geral de todas as atividades de tratamento de dados pessoais levadas a cabo por uma organização. Trata-se, portanto, de um requisito prévio da conformidade e, como tal, constitui uma medida de responsabilização eficaz.

1.8 Os subcontratantes no Regulamento de Proteção de Dados

Uma das principais novidades do novo Regulamento centra-se na responsabilização dos subcontratantes pelo tratamento de dados[49]. Como exemplo, refere-se a possibilidade de pedidos de indemnização contra o responsável pelo tratamento ou o subcontratante de forma direta, sem que tenha que existir uma ação de regresso em função do seu grau de responsabilidade.

Não obstante segundo o artigo 28º, nº 3, alínea f) do RGDP, o subcontratante encontra-se com a obrigação de assistir ao responsável pelo tratamento de dados com o objetivo de assegurar o cumprimento das obrigações relacionadas com as notificações de violações de dados pessoais à autoridade de controlo.

Igualmente, o considerando 82 descreveu que "a fim de comprovar a observância do presente regulamento, o responsável pelo tratamento ou o subcontratante deverá conservar registos de atividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento e subcontratantes deverão ser obrigados a cooperar com a autoridade de controlo e a facultar-lhe esses registos, a pedido, para fiscalização dessas operações de tratamento". Ou seja, o subcontratante tem como obrigação notificar o responsável pelo tratamento das violações de dados pessoais que tenham conhecimento, embora, a obrigação de notificar à autoridade competente é da responsabilidade do responsável de tratamento de dados, e não ao subcontratante, nos termos do n.º 1 do artigo 33.º do RGPD. A tabela seguinte demonstra as obrigações do subcontratante:

Obrigações do subcontratante	
Colaboração com a Autoridade de Controlo	O artigo 31.º do RGPD prevê a colaboração da CNPD com o responsável pelo tratamento e subcontratante e, em caso disso, com os seus representantes.

[49] Cf. Considerando 13 e artigo 79.º (Direito à ação judicial contra um responsável pelo tratamento ou um subcontratante) do RGPD.

	Coima: al. a) do n.º 4 do artigo 83.º do RGPD
Notificar o responsável pelo tratamento no caso de ocorrer uma violação dos dados	O subcontratante notifica o responsável pelo tratamento, e não a autoridade de controlo, quando tem conhecimento de uma violação de dados (n.º 2 do art. 33.º do RGPD). Coima: al. a) do n.º 4 do artigo 83.º do RGPD
Registo das atividades de tratamento e do Encarregado de Proteção de Dados	Aplicam-se, de igual modo, ao subcontratante como ao responsável pelo tratamento.

1.9 Avaliação dos principais impactos sobre a proteção de dados

A AIPD representa um processo que ocorre no caso em que exista um determinado tipo de tratamento, principalmente no uso das novas tecnologias, tendo em conta a sua natureza, âmbito, contexto e finalidade, perante um elevado risco para os direitos e liberdades das pessoas singulares.

É realizada pelo responsável pelo tratamento de dados, numa fase anterior do início da operação do tratamento (n.º 1 do art. 35.º do RGPD) e, inclui as medidas, garantias e procedimentos para reduzir os riscos, e ao mesmo tempo, assegurar o cumprimento do RGDP (considerando 90 do RGDP). A sua realização é efetuada da seguinte forma (n.º 7 do art. 35.º do RGPD):

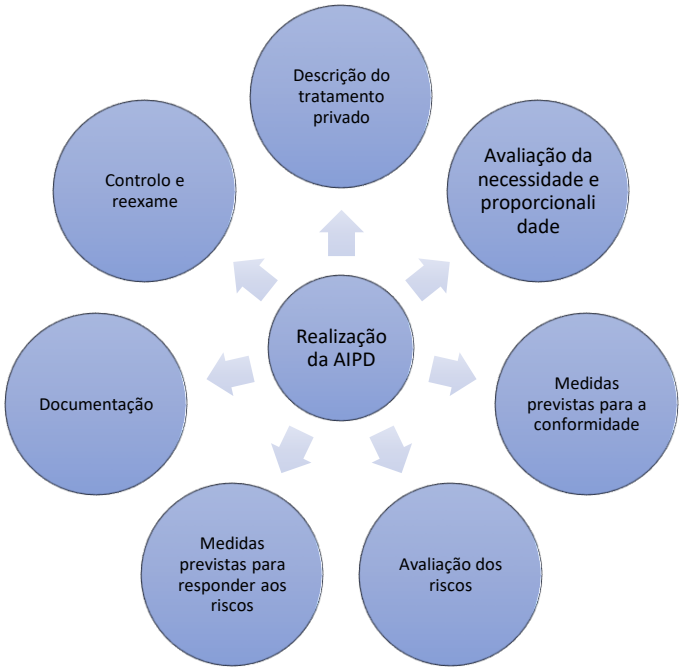

Figura 2 - A realização da AIPD

De acordo com a figura 1, observa-se que a AIPD é constituída de três fases distintas, a descritiva, que descreve as operações de tratamento previstas e a sua finalidade, a avaliativa, que é constituída de duas dimensões, a avaliação relacional entre as operações de tratamento e os objetivos associados ao princípio da proporcionalidade e avaliação dos riscos, e por fim, a fase decisória, que tem como base as medidas para reduzir os riscos[50].

Contrariamente, existem algumas situações em que não é necessário a realização de uma AIPD. Ou seja, após decorrida a avaliação, se esta determinar que o tratamento tem um elevado risco com ausência de medidas tomadas pelo responsável pelo tratamento, este não poderá atenuar o risco e, desta forma tem que consultar a autoridade de controlo antes de realizar o tratamento de dados pessoais (n.º 1 do art. 36.º e considerando 94 do RGPD)[51].

[50] PINHEIRO, Alexandre Sousa et al. – Cit. 42, p. 461.
[51] O G29 elenca um conjunto de situações em que não é obrigatório realizar uma AIPD, sendo todas aquelas que não apresentem um risco elevado para os direitos e liberdades das pessoas singulares. (Ver Grupo de Trabalho do Artigo 29.º - Cit. 43, p. 15).

1.10 A finalidade da proteção

O direito à proteção dos dados pessoais sugere a proteção de bens jurídicos, que de acordo com ALEXANDRE SOUSA PINHEIRO[52], a expressão "proteção de dados" («Datenschutz») não identifica o bem jurídico protegido, e embora adicione a expressão "pessoais" não transmite de forma clara qual o bem jurídico protegido no âmbito do Direito. Assim, o que a ordem jurídica protege é o direito a determinar a ação exercida sobre os dados pessoais e a sua finalidade[53]. Assim, a «proteção» («Schutz») respeita a pessoas, e não a «dados» («Daten»)[54].

Num entendimento próprio, o novo direito á proteção de dados pessoais, que se encontra consagrado no artigo 35º, da CRP é reconhecido por meio de um bem jurídico-penal que se designa por "autodeterminação informal ou informativa"[55], que corresponde à plena disponibilidade dos dados de índole pessoal em favor do seu titular, e impedindo que a pessoa se transforme em simples objeto de informações"[56].

Capítulo 2 - O Encarregado da Proteção de Dados, à Luz do Novo Regulamento Geral da Proteção de Dados

2.1 Porquê a necessidade de um novo enquadramento jurídico

O Regulamento Geral de proteção de Dados passou a ser aplicado de forma direta a partir de 25 de novembro de 2018, e substituiu a diretiva e lei de proteção de

---

[52] De acordo com PINHEIRO, Alexandre Sousa – Privacy e Protecção de Dados Pessoais…, op. cit., pág. 429

[53] Cfr. HOFFMANN-RIEM, Wolfgang – Informationelle Selbsbestimmung in der Informationgesellsschaft – Auf dem Wege zu einem neuen Konzept des Datenschutzes. AöR, n.º 123, 1998. Pág. 520.

[54] No mesmo sentido, cf. PINHEIRO, Alexandre Sousa – Privacy e Protecção de Dados Pessoais…, op. cit., pág. 803

[55] Assim denominado por inspiração germânica, cfr. CANOTILHO, J. J. Gomes; MOREIRA, Vital – Constituição da República Portuguesa Anotada. 4.ª Edição..., op. cit., pág. 551

[56] Em sentido convergente, ver QUEIROZ, Cristina – "A protecção constitucional da recolha…", op. cit., pág. 298; e ver SILVEIRA, Luís Lingnau da – "O direito à protecção de dados pessoais…", op. cit., pág. 209; e "Configuração constitucional…", op. cit., págs. 508-509. Nas palavras de PINHEIRO, Alexandre Sousa, in O RGPD aplica-se…, op. cit., pág. 9, a autodeterminação informacional ou informativa, protegida pelo direito à proteção de dados pessoais, está necessariamente associada ao princípio da finalidade e visa garantir que os titulares tenham direito a intervir sobre a informação pessoal que lhes respeita, nomeadamente através do conhecimento e consentimento no acesso, na recolha, no tratamento, no armazenamento, no uso ou na transmissão da informação pessoal, salvo quando a lei funcione como condição de legitimidade

dados pessoais. Este novo quadro legal trouxe algumas alterações marcantes que tiveram impacto na vida das organizações de acordo com a sua natureza, área de atividade, dimensão e tipo de tratamento de dados pessoais que possam realizar.

A necessidade de algumas mudanças no enquadramento jurídico deve-se à rápida evolução tecnológica e globalização que trouxeram consigo a criação de novos desafios em matéria de proteção de dados pessoais, exigindo assim um novo quadro de proteção mais sólido e coerente na UE.

Neste sentido, este novo Regulamento tem maior necessidade em obrigar a quem lida com os dados pessoais a ter um maior cuidado em relação ao passado, no tratamento desses dados. No caso das empresas, existe a necessidade de ter uma política de tratamento de dados pessoais em conformidade com o tipo de volume de dados que estas tratam, permitindo assim, regras mais céleres na obtenção, tratamento e destruição de dados, a existência de maior transparência para o utilizador, maior responsabilização de quem efetua o tratamento, evitar a utilização de dados pessoais sem autorização.

De acordo com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, no seu artigo 7º, "esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.".

Outro fator importante deve-se ao fato de que a Diretiva de 1995, sobre a proteção de dados surgiu antes da rápida ascensão das redes sociais e de outros serviços online, e como era uma Diretiva a sua forma de adoção variou de país para país. A finalidade do RGPD da UE é garantir que a legislação relacionada com a proteção de dados pessoais seja "adequada à finalidade" no atual quadro de conetividade e, ao

mesmo tempo para assegurar que todos estão a implementar o mesmo conjunto de regras[57].

Embora o RGPD tenha princípios, regras gerais, direitos e obrigações, que já fazem parte integrante da Diretiva e, da Lei da Proteção de Dados Pessoais (Lei n.º 67/98, de 26 de Outubro), na verdade introduziu alterações bastante importantes ao regime aplicável até esta altura, e onde se destacam o alargamento do âmbito da aplicação territorial, pois passa a ser aplicado apenas aos responsáveis pelo tratamento ou subcontratantes estabelecidos pela UE, e igualmente os responsáveis pelo tratamento ou subcontratantes não estabelecidos na União Europeia quando os tratamentos de dados que efetuam, estejam relacionados com a oferta de bens e serviços, que se dirigem aos residentes do território da União, bem como no controlo do seu comportamento[58].

2.2 As principais novidades do regulamento

Nas palavras de JOSÉ AUGUSTO SIMÕES[59], o novo regulamento de proteção de dados teve muitas alterações em relação ao anterior. Sendo que, na informação aos titulares de dados o RGDP obriga a informar os titulares dos dados sobre a base legal para o seu tratamento, o tempo de conservação e a transferência dos dados. E, por esta razão, torna-se necessário a existência de uma política de privacidade e textos que possam informar os titulares dos dados.

De igual modo, o RGDP obriga a garantir o exercício dos direitos dos titulares dos dados, sendo que, os pedidos de exercício destes direitos devem ser monitorizados e documentados com prazos de resposta máximos.

---

[57] Hewlett-Packard Company. (2018). O que são as regras vinculativas das empresas (BCR - Binding Corporate Rules) da HP. Disponível em http://www8.hp.com/pt/pt/bindingcorporate-rules.html

[58] Comissão Europeia. (2012). COM (2012) 11 final. Proposta de regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
Disponível em https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=COM:2012:0011:FIN

[59] JOSÉ AUGUSTO SIMÕES. Proteção de dados e o novo regulamento geral da União Europeia. Revista Portuguesa de Medicina Geral e Familiar. versão impressa ISSN 2182-5173. Rev Port Med Geral Fam vol.34 no.5 Lisboa out. 2018

Como o direito à portabilidade dos dados, à eliminação dos dados e à notificação de terceiros sobre a retificação, o apagamento ou a limitação de tratamento quando solicitados pelos terceiros.

No consentimento dos titulares dos dados, o RDPD obriga a controlar os contextos em que foi obtido o consentimento dos titulares, com base legal para o tratamento dos dados pessoais. A este aspeto, importa referir que o consentimento é necessário nalgumas situações em que surja um risco grave para a proteção dos dados, e por esta razão, considera adequado existir um nível mais elevado de controlo em relação aos dados pessoais. Está explicito no artigo 9º que o tratamento de categorias especiais de dados para países terceiros ou organizações internacionais quando não está presente as garantias adequadas no artigo 49º[60], e no artigo 22º, relacionado com as decisões individuais automatizadas[61].

Não obstante o RGDP tem previsto uma "declaração ou ato afirmativo inequívoco" como requisito principal de consentimento explicito de acordo com as regras. Neste contexto, o termo "explicito" corresponde à forma como o consentimento é manifestado pelo titular dos dados[62].

Outra das alterações do novo Regulamento de proteção de dados, relaciona-se com a sua natureza, ou seja, o RGDP define o conceito de dados sensíveis que estão sujeitos a determinadas condições para o seu tratamento, como o tratamento automatizado. E, igualmente é obrigatória a nomeação de um Encarregado de Proteção

[60] De acordo com o artigo 49.º, n.º 1, alínea a), do RGPD, o consentimento explícito pode afastar a proibição de transferir dados para países que não dispõem de níveis adequados de proteção de dados na sua legislação. Consultar também o documento de trabalho sobre uma interpretação comum do n.º 1 do artigo 26.º da Diretiva 95/46/CE de 24 de outubro de 1995 (WP 114), p. 11, em que o GT29 indica que o consentimento para transferências de dados que ocorram periódica ou repetidamente é inadequado.

[61] No artigo 22.º, o RGPD introduz disposições para proteger os titulares de dados contra decisões baseadas unicamente no tratamento automatizado, incluindo definição de perfis. As decisões tomadas com este fundamento são permitidas em determinadas condições jurídicas. O consentimento desempenha um papel importante neste mecanismo de proteção, dado que o artigo 22.º, n.º 2, alínea c), do RGPD deixa claro que o responsável pelo tratamento pode avançar com decisões automatizadas, incluindo definição de perfis, que possam afetar significativamente o indivíduo com o consentimento explícito do titular dos dados. O GT29 emitiu orientações distintas sobre esta questão: orientações do GT29 sobre decisões individuais automatizadas, atualmente apenas disponíveis na versão inglesa (Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679), de 3 de outubro de 2017, (WP251).

[62] Ver também o Parecer 15/2011 do GT29 sobre a definição de consentimento (WP 187), p. 25.

de Dados (DPO – Data Protection Officer). Neste contexto, o RGDP introduziu a figura do EPD com a responsabilidade de controlar os processos de segurança para garantir a proteção de dados numa organização.

O RGDP obriga à manutenção de um registo documentado de todas as atividades de tratamento de dados pessoais, sendo que as organizações estão obrigadas a demonstrar o cumprimento de todos os requisitos que decorram da aplicação do regulamento[63].

2.2.1 Aplicação territorial

Outra das alterações no novo Regulamento é o âmbito da aplicação territorial, no qual o RGDP aplica-se "ao tratamento dos dados pessoais, efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União"[64].

Neste contexto, o RGDP tendo em conta a sua dimensão de aplicação, engloba todas as organizações que façam parte da UE e fora desta, se o tratamento de dados pessoais tal como está descrito no artigo 3º, nº 1, RGDP. E, no nº 2 do mesmo artigo refere-se que o RGDP se aplica não só "ao contexto das atividades de um estabelecimento responsável pelo tratamento ou de um subcontratante", como igualmente, "ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante"[65].

No caso do tratamento de dados de titulares de residentes na UE, somente se aplica o RGDP se as atividades de tratamento estiverem relacionadas com a "oferta de bens e serviços a estes titulares de dados na União, independentemente da exigência de os titulares de dados procederem a um pagamento".

---

[63] Parlamento Europeu, Conselho Europeu. 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). JOUE. 2016;L(119):1-88.

[64] Art.º 3.º, n.º 1 do RGPD.

[65] Considerando (22), (23), (24) e (25) do RGPD.

O mesmo significa que, mesmo que a organização não esteja localizada territorialmente no espaço da União Europeia, estará sujeita ao RGDP, como as atividades que se relacionam com os sítios de internet. Assim, este alargamento ao nível de aplicação territorial está em conformidade com o tratamento para que este seja mais equilibrado entre os responsáveis pelo tratamento de dados dentro e fora da UE.

"O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecidos na União, 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; o controlo do seu comportamento, desde que esse comportamento tenha lugar na União"

2.2.2 Direito à privacidade

A privacidade é um direito fundamental dos cidadãos da UE. A noção do direito à privacidade no contexto dos dados é bem definida na Europa. Ao contrário de outras regiões onde as proteções de dados são mais fracas ou virtualmente inexistentes, manteve-se na vanguarda da questão. O sentimento público por proteções vigorosas de privacidade de dados é forte, um dos motivos é porque a UE mudou para modernizar e reforçar os regulamentos.

A privacidade de dados adquiriu um aspeto mais transnacional, embora não muito tempo atrás o controlador de dados, o titular dos dados e os meios utilizados para o seu processamento estivessem sempre localizados no país[66]. E, com o desenvolvimento do comércio internacional, as novas tecnologias e as novas estruturas corporativas das empresas multinacionais aumentaram a importância do processamento e transferência internacional de dados. Este novo ambiente sem fronteiras não dá muita credibilidade às leis de proteção de dados de âmbito territorial doméstico[67].

[66] Paul de Hert e Michal Czerniawski, Expandindo o escopo da proteção de dados europeia para além do território: Artigo 3 do Regulamento Geral de Proteção de Dados em seu contexto mais amplo , Lei Internacional de Privacidade de Dados, 2016, Vol. 6, No. 3.

[67] Merlin Gömann, O novo escopo territorial da lei de proteção de dados da UE: desconstruindo uma conquista revolucionária, Common Market Law Review, 54, pp. 567-590, 2017.

Num estudo atual, os conceitos de privacidade e intimidade da vida privada, a finalidade da tutela jurídica da privacidade é a de reservar ao sujeito, o círculo de acontecimentos e informações, que ele pretende guardar para si e subtrair, as experiências íntimas.

A importância da tutela da privacidade pode ser demonstrada através da constituição de um objetivo horizontal de ordem jurídica, de ser consagrada pela ordem jurídica no seu conjunto, ao nível constitucional, mas igualmente, pelo direito administrativo, direito penal e direito civil. Pode-se contextualizar que os instrumentos de tutela dos direitos do homem, ao nível internacional, centram-se essencialmente, na privacidade, protegendo-a deste modo, nos seus articulados, que corresponde à Declaração Universal dos Direitos do Homem, no artigo 8º, e com o Pacto Internacional sobre os Direitos Civis e Políticos (artigo 17º)[68.]

Ainda, ao nível internacional, as ordens jurídicas, a inclusão da proteção da privacidade ao nível constitucional, tem sido alvo de alguma polemica nos EUA, na Inglaterra, e na Alemanha, onde o direito à vida privada tem sido construído a partir do direito geral da personalidade consagrado nos artigos 1º e 2º da *Grundgesetz*.

A nível nacional, o direito à intimidade da vida privada e familiar está previsto no nº 1 do artigo 26º da CRP, com a mesma força jurídica que resulta da integração nos catálogos do direito, liberdade e garantias pessoais. No campo da legislação ordinária, igualmente, o código civil assegura no seu artigo 70º a tutela geral da personalidade, garante no artigo 80º o direito à reserva sobre a intimidade da vida privada. O Código Penal, prevê um conjunto de incriminações destinadas a proteger os bens jurídicos pessoais, entre os quais se descreve a reserva da vida privada e da intimidade, nomeadamente, nos crimes previstos nos artigos 192º, "Devassa da vida privada" e 193º "Devassa por meio de informática".

Os principais problemas da proteção da privacidade, modificaram-se de forma clara, na sociedade de risco e da informação, essencialmente, decorrente ao

[68] Para uma análise destes documentos internacionais, cfr. LEITE PINTO, *ob. cit.*, p. 84 ss. e DAVID FELDMAN, *ob. cit.*, p. 28.

desenvolvimento da informática e novas tecnologias[69], que facilitaram a recolha, tratamento, difusão, acesso e armazenamento de dados. As novas potencialidades da Internet, como uma "verdadeira autoestrada de informação". A qual tem vindo a expandir-se, alterou de forma significativa, a vida social no novo milénio. A informação pessoal assume a forma de *bits*, a sua vulnerabilidade ao abuso é evidente.

É pertinente referir que o Direito positivo, disponibiliza importantes indicações a este respeito, no artigo 35º da CRP, que garante "um conjunto de direitos fundamentais em matéria de defesa contra o tratamento informático de dados pessoais". Entre estes direitos, encontra-se o acesso, retificação e atualização dos dados informáticos, a proteção de dados pessoais (nº 2), foro íntimo (nº3), a proibição de acesso por terceiros (nº4) e o acesso livre às redes informáticas[70.]

Essencialmente, porque nos Estados de Direito Democráticos, como o Português, a afirmação dos valores da transparência, abertura, e democracidade da Administração Pública é efetuada de modo cada vez mais obvio, e representa as facilidades cada vez maiores, no acesso à informação. A razão mais representativa do aumento das possibilidades de conflito relaciona-se com o desenvolvimento das tecnologias informáticas, as quais facilitam a recolha, armazenamento e tratamento de dados pessoais[71.]

A alavanca do mundo sempre foi a informação, indistintamente de qual seja o meio para a transmitir, a época ou lugar onde estamos. A informação é sem dúvida a energia que move a sociedade, os indivíduos e as organizações. O que é, contudo, informação, como a podemos considerar? Existem várias definições, um dos conceitos existentes, Le Coadic (1996), refere que a informação é um conhecimento inscrito em diversas formas, desde escrita impressa ou numérica, oral ou audiovisual.

---

[69] Para COSTA ANDRADE (*Liberdade de Imprensa, cit.*, p. 17 s.) a sociedade do risco é "portadora de novas agressões, ameaças e perigos", multiplicando "exponencialmente as *superfícies expostas às intempéries* dos valores pessoais coenvolvidos".

[70] Cfr. GOMES CANOTILHO/VITAL MOREIRA, *ob. cit.*, p. 215 s.

[71] Relativamente ao "perigo real e efectivo que a acumulação informática de dados sobre as pessoas pode representar para a liberdade e os direitos dos cidadãos, em especial sobre a vida privada", *vide* FERNÁNDEZ ESTEBAN, *ob. cit.*, p. 128 ss. e PAULO MOTA PINTO, que oferece diversos exemplos de como "a *evolução técnica* veio fornecer meios incomparavelmente mais eficazes de violação da intimidade das pessoas" (cfr. *ob. cit.*, p. 511). Cfr. ainda FRANÇOIS RIGAUX, "La liberté de la vie privée", *cit.*, p. 556 (mostrando alguns dos perigos levantados pelos "bancos de dados").

A França foi o país pioneiro no sentido de tutelar os direitos à intimidade e vida privada, através do Código de Napoleão, no artigo 1382. O caso mais exemplar que ocorreu foi o caso da atriz Elisa Felix, reconhecida por Rachel, que foi fotografada pela sua família quando se encontrava morta, e esta imagem foi pintada num quadro. Assim, o promotor em defesa de Rachel, defendeu que somente a família pode, em nome da pessoa falecida, reproduzir os seus restos.

Ocorreu igualmente, na Alemanha e na Itália, países cuja jurisprudência é ampla em termos de direitos à vida privada e intimidade, e onde existe ainda a tutela constitucional destes direitos. Existem, pois algumas recomendações relevantes para o direito à intimidade e vida privada, nomeadamente, a Declaração Americana dos Direitos e Deveres do Homem, em 1948, que se contextualizou como a primeira declaração internacional de direitos que referencia o direito à vida privada. Igualmente, a Convenção Europeia dos Direitos Humanos, que foi assinada em 1950.

A intimidade representa algo mais profundo que a privacidade, caracteriza-se por um determinado espaço, considerado pelo individuo, como um espaço impenetrável, intransponível e que pertence única e exclusivamente à pessoa.

A privacidade apresenta como esfera da vida, nucleada na ausência do público, o mesmo significa que as relações sociais exteriores ao núcleo familiar, permanecem protegidas.

Posteriormente, no ano de 1890, dois advogados americanos publicaram no artigo "O direito à privacidade", instigando o reconhecimento do novo direito. Estes direitos passam então, a ser tutelados pouco a pouco, inicialmente, através da construção jurisprudencial e de seguida a sua integração nas Constituições.

O respeito pela vida desde que é jurídico, é reconhecido como norma jurídica. O direito à vida representa o mais importante direito de personalidade, e consagrado no artigo 24º da Constituição Portuguesa, que descreve que "*a vida humana é inviolável*" decorre de um direito inato que se adquire com o nascimento e, desta forma, é intransmissível e indisponível. Assim, do direito à vida, decorre a ilicitude do suicídio, do auxílio e da instigação ao suicídio e da eutanásia.

O direito à vida representa um direito ao respeito da vida perante os outros, é um direito de exigência de um comportamento positivo dos outros. Desta forma, não é um direito que é abordado na sua formulação típica. Não existe ainda um consenso sobre as condições de ilicitude do aborto, ou sobre o facto da ilicitude, decorrer da tutela do bem da vida.

A expressão "*Direito à vida privada e intimidade*" teve o seu início no final do século XIX. Numa fase anterior, os conflitos desta área eram substituídos pelos princípios gerais do direito, que serviam de fonte à formação da tutela a estes direitos. A proteção dos direitos à vida privada foi necessária, em consequência da evolução do homem e a busca pela sua dignidade e, ao mesmo tempo, que representa a luta contra a opressão e o arbítrio. É uma procura pela liberdade e positivação.

Foi em 1902, nos EUA do Norte que a Suprema Corte julgou o primeiro caso de violação do direito da vida privada, rejeitado por 4 votos. Embora a opinião pública colocou-se ao lado dos juízes vencidos e a Suprema Corte reconheceu o direito à intimidade.

Ao ser tutelado o bem jurídico da intimidade e da privacidade, existe a proteção do direito de personalidade que deve ser considerado como princípio da dignidade da pessoa humana. Deste modo, a primazia da tutela jurídica da vida privada é essencialmente, reservar ao individuo, o círculo de vivências, acontecimentos e informações que este pretende guardar de forma legítima. Está, pois, em causa o seu direito à privacidade.

Atualmente, a proteção da vida privada representa uma necessidade do homem e da sociedade, e sem exceção do significado do sentido relacional da reserva (Andrade, 1991)[72]. Numa época em que as relações com os outros e com a sociedade se efetua a vários níveis, é a própria sociedade a proteger os preceitos em que o homem se baseia. Não se podem, pois, deixar de considerar, as palavras e conceitos do comportamento

[72] Sobre a inserção – amplamente admitida pelas doutrinas e jurisprudências de vários países – do direito à intimidade da vida privada na categoria dos direitos de personalidade, em que está em causa a própria proteção da dignidade da pessoa humana, cfr., entre nós, COSTA ANDRADE, ob. ult cit., p. 13 e 29, acentuando o mesmo Autor noutro local ("Sobre a Reforma", cit., p. 437) como estes bens jurídicos pessoais (entre os quais inclui o direito à privacidade) são concretização de um direito ao livre desenvolvimento da personalidade

hermeticamente isolado. Na sociedade de comunicação, onde a troca e o acesso cada vez mais fáceis à informação devem assegurar a intimidade da pessoa.

No que está relacionado com as ordens jurídicas ao nível interno, a integração da proteção da privacidade ao nível constitucional, tem vindo a solicitar uma polémica elevada, especificamente, nos países desenvolvidos como os EUA, Inglaterra e Alemanha, constituído essencialmente, pelo Direito de Personalidade, descrito nos artigos 1º e 2º da Grundgesetz (Lei Fundamental da Republica Federal da Alemanha). Em Portugal, este tema tem sido discutido, consagrado na CRP, através do artigo 26º, detentora de uma elevada força jurídica, que resulta do catálogo dos direitos, liberdades e garantias pessoais de cada cidadão.

Ao nível da legislação, o Código Civil assegura a tutela geral da personalidade, no artigo 70º, e especificamente, garante o direito à reserva sobre a intimidade da vida privada no artigo 80º. O Código Penal, prevê, igualmente, um conjunto de incriminações que se destinam à proteção dos bens jurídicos pessoais, nomeadamente, a reserva da vida privada e da intimidade. Neste contexto, os crimes previstos nos artigos 192º constitui a "Devassa da vida privada" e o artigo 193º a "Devassa por meio da informática".

A regulação constitucional do direito à privacidade, especificamente, no que se relaciona com a integração da privacidade nos limites a observar no exercício do direito de acesso à vida privada, o direito administrativo revela uma apetência especial de regulação das questões de índole técnica neste domínio.

Na sociedade atual, os cidadãos são obrigados num conjunto de situações, a fornecer informações pessoais aos órgãos e agentes administrativos, porque necessitam deles, ou porque o poder da administração o justifica.

Os direitos à informação e à privacidade estão de forma contrária, isto porque, os Direitos democráticos, como o português, a abertura da democracia, a afirmação de determinados valores, é efetuada de forma mais clara.

As ofensas à privacidade constituem-se através de um conjunto de condutas, nomeadamente, a instalação de aparelhos eletrónicos como os microfones, para captar de forma furtiva, conversas ou imagens do interior de um domicílio. A existência de algumas destas hipóteses pode gerar um dano moral ou material que deve ser reparado pelo autor da ofensa à vítima (Diniz, 2011).

O direito à privacidade é tutelado essencialmente, pela Constituição Portuguesa e através do Código Civil, e preservado contra as agressões diretas ou indiretas ao longo do texto constitucional. Segundo Diniz (2011, p. 151), a proteção da vida privada

"Manifesta-se como a liberdade de expressão, inviolabilidade do domicílio, de correspondência e comunicação telefónica, liberdade de locomoção e associação e de exercício do trabalho; limitação do comportamento apenas imposta legalmente; relativa proibição da publicidade dos atos processuais; direito ao acesso do banco de dados etc. Repercute também no crime, visto que se pune a inviolabilidade de domicílio e correspondência".

O direito à vida privada é reconhecido pela Constituição da República no artigo 26º, nº 1 e igualmente, pelo código civil no artigo 80º como o direito fundamental e direito de personalidade. Este direito é essencialmente, intransmissível e irrenunciável[73].

Os direitos fundamentais são, na sua "essência", direitos do homem. Os direitos do homem têm pretensões de universalidade e de essencialidade: visam proteger bens que se consideram universais, e são válidos para todos os homens em todos os espaços e tempos, e bens que se consideram essenciais, (i.e., que tornam possível a prossecução de uma existência humana autónoma e condigna). (Por ex. Vida – artigo 24º da CRP;

[73] Sobre os direitos de personalidade, v. Carlos Alberto da MOTA PINTO, *Teoria geral do direito civil*, 3ª ed., Coimbra, 1985, p. 88, Rabindranath V. CAPELO DE SOUSA, *O direito geral de personalidade*, Coimbra, 1995, pp. 402 e ss., e Adriano de CUPIS, *Os direitos de personalidade*, trad. port. de A. Vera Jardim e M. Caeiro, Lisboa, 1961, pp. 45 e ss. Sobre a renúncia a direito fundamentais, v. José Joaquim GOMES CANOTILHO, *Direito constitucional e teoria da constituição*, 4ª ed., Coimbra, 2000, p. 453 – defendendo uma solução diferenciada que distingue "entre renúncia ao núcleo substancial do direito (constitucionalmente proibida)e limitação voluntária ao exercício (aceitável sob certas condições) de direitos" –, Jorge MIRANDA, *Manual de direito constitucional, tomo IV: Direitos fundamentais*, 3ª ed., Coimbra 2000, pp. 357-8, e Jorge REIS NOVAIS, "Renúncia a direitos fundamentais", in Jorge MIRANDA (org.), *Perspectivas constitucionais. Nos 20 anos da Constituição*, Coimbra, 1996, vol. I, pp. 263-335.

liberdade de consciência – artigo 41º; integridade física – artigo 25º; família e casamento – artigo 36º)[74].

Os direitos fundamentais, todos eles, qualquer que seja a sua estrutura – são direitos multifuncionais. Não cumprem só uma função. Não existem só para realizar os interesses ou as necessidades básicas dos seus titulares. Existem também para outra coisa: para revelar os valores fundamentais de uma comunidade política. A vida, por exemplo, não é apenas um direito subjetivo. É um valor fundante da comunidade política portuguesa. O mesmo se diga da liberdade de expressão, ou da liberdade de criação artística, ou do direito a uma habitação condigna[75].

Os princípios constitucionais representam normas de ordem jurídica e que legitimam o sistema isto porque, consagram valores culturalmente fundados na própria sociedade[76]. Deste modo, o princípio constitucional democrático é senão o princípio que estrutura judicialmente todo o regime político e com base no valor conatural ao homem da liberdade política de hoje[77].

Por um lado, a conceção teórica de Estado de Direito tem a missão de limitar o poder político no sentido de estabelecer o império do direito, ou seja, o "governo das leis e não dos homens". E, por outro, a conceção teórica de Estado Democrático procura um poder, uma ordem de domínio legitimada pelo povo e, na titularidade e exercício.

O princípio constitucional democrático renova as conceções e missões e estabelece para a democracia uma dimensão de legitimidade. Deste modo, a legitimidade está associada à prossecução concreta e ao mesmo tempo participativa, de fins e valores positivados. O Direito Liberal Formal é considerado como a dimensão principal do Estado de Direito e as técnicas de garantia dos direitos individuais, ou seja, o direito à vida.

---

[74] MIRANDA, Jorge. *Manual de Direito Constitucional*. Tomo IV, pp. 77- 106

[75] CANOTILHO, J.J. Gomes. *Direito Constitucional e Teoria da Constituição*, ob cit., pp. 393- 410
Por isso se diz que os direitos fundamentais, todos eles, têm uma dupla dimensão – e são por isso multifuncionais. Têm por um lado uma dimensão subjectiva – são direitos das pessoas, invocáveis em juízo. Mas têm também uma dimensão objetiva. Revelam os valores fundamentais que ordenam a comunidade política portuguesa.

[76] CUNHA, Paulo Ferreira da. *Res Pública: ensaios constitucionais*. Coimbra: Almedina, 1998.

[77] CANOTILHO, J. J. Gomes. (2003).*Direito Constitucional e Teoria da Constituição*. 7ª ed. Coimbra: Almedina.

2.3 Notificações de Violações de Dados Pessoais

Qualquer tipo de violação de dados está diretamente relacionado com a segurança da informação, pelo que internamente está associada a incidentes que por algum motivo comprometem a confidencialidade, a integridade ou a disponibilidade dos dados pessoais. Contudo, a proteção de dados pessoais apresenta um alcance distinto da segurança de informação.

Por esta razão, existem incidentes relacionados com a segurança de informação que não representam as violações de dados pessoais. Como exemplo, um acesso não autorizado por um hacker a dados estatísticos ou fictícios de um projeto em fase de teste, o qual não contém qualquer informação pessoal de indivíduos, embora se trate de uma falha de segurança da informação, mas não uma violação de dados pessoais. Embora, o contrário não se aplica, tendo em consideração que uma violação dos dados pessoais implica um incidente de segurança. E, assim, poder-se-á assumir que as violações de dados pessoais em três categorias: confidencialidade; integridade; e disponibilidade (Não obstante o GT29, no seu parecer 03/2014, devido à notificação de violação)[78].

Assim, a violação de confidencialidade ocorre quando existe uma divulgação ou acesso acidental não autorizado a dados pessoais, a violação de integridade quando existe uma alteração acidental ou não autorizada dos dados pessoais, e a violação da disponibilidade, quando existe uma perda de acesso ou a descrição acidental ou não autorizada de dados pessoais[79].

Uma violação que envolva a perda temporária de disponibilidade deve ser documentada de acordo com o artigo 33º, nº 5, que auxilia o responsável pelo tratamento e demonstrar a responsabilidade pelo controlo dos registos. No entanto, tendo em conta o contexto da violação, esta pode ou não exigir a notificação à autoridade de controlo e a comunicação às pessoas afetadas. De acordo com o artigo 33.º, o responsável pelo tratamento deverá proceder à notificação, a menos que a

[78] as orientações do GT29 sobre a aplicação e a fixação do valor das coimas, disponível em: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889
[79] Ver Parecer 03/2014.

violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.

Em qualquer tentativa de resolver uma violação, o responsável pelo tratamento deve primeiro ser capaz de reconhecer uma. O RGPD define «violação de dados pessoais» no artigo 4.º, n.º 12, 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».

Dito de outra forma, uma violação é um tipo de incidente de segurança, embora tal como consagrado no artigo 4º, nº 12, o RGDP só é aplicado no caso que exista uma violação de dados pessoais e, a consequência desta violação é que o EPD não poderá assegurar o cumprimento dos princípios relacionados com o tratamento de dados pessoais, de acordo com o estipulado no artigo 5º, do RGDP. Este aspeto identifica a diferença entre incidente de segurança e uma violação de dados pessoais, ou seja, enquanto todas as violações de dados pessoais são incidentes de segurança, nem todos os incidentes de segurança são necessariamente violações de dados pessoais[80].

De acordo com o descrito no considerando 86, o RGDP exige ao responsável pelo tratamento de dados que notifique a violação à autoridade de controlo respetiva, somente com exceção nos casos em que seja improvável que resulte em risco[81].

Não obstante os artigos 33º e 34º do RGDP definem uma das grandes novidades deste diploma legal, nomeadamente, a obrigação dos responsáveis pelo tratamento de dados notificarem a autoridade de controlo competente e, em alguns casos específicos, o titular dos dados afetado quando exista uma violação de dados pessoais. Esta obrigação representa um reflexo dos princípios da lealdade e transparência[82], integridade e

[80] Deve notar-se que um incidente de segurança não se limita a modelos de ameaça em que é efetuado um ataque a uma organização por parte de uma fonte externa, mas inclui incidentes decorrentes do tratamento interno que violam os princípios de segurança.
[81] o considerando 86.
[82] Cf. alínea a) do n.º 1 do artigo 5.º do RGPD.

confidencialidade[83] e da responsabilidade[84], que estão assim presentes no espírito do legislador europeu no momento da elaboração do RGDP.

Importa ainda referir que cabe ao EPD o ónus de reporte das violações de dados que tiver sido alvo às autoridades de controlo com competência de matéria de proteção de dados.

Ora, estas notificações têm como objetivo principal minimizar o impacto que decorre da violação dos dados pessoais e permitem uma resposta por parte das autoridades de controlo e dos indivíduos afetados. As notificações devem ocorrer de forma rápida após o conhecimento por parte dos responsáveis pelo tratamento e, nem todas as violações de dados terão de ser comunicadas às autoridades de controlo, nem aos titulares de dados afetados. Neste sentido, este dever de comunicar as violações de dados às autoridades de controlo não é original, ou seja, a Diretiva 2009/136/CE[85] e o Regulamento (UE) 611/2013[86] relacionados com as comunicações eletrónicas já tinham sido consagradas nesta obrigação.

Importa salientar que a inovação do RGDP na ampliação da obrigação de violações de dados pessoais a todos os responsáveis pelo tratamento e não somente aos operadores de serviços de comunicações publicamente disponíveis[87].

Assim, de acordo com o artigo 33º, nº 1 do RGDP os EPDs têm como obrigação notificar as violações de dados que estão sob a sua responsabilidade às autoridades de controlo com um prazo de 72 horas a partir do momento em que tenham tomado conhecimento das respetivas violações. Embora, esta obrigação somente diga respeito às

[83] Cf. alínea f) do n.º 1 do artigo 5.º do RGPD.
[84] Cf. n.º 2 do artigo 5.º do RGPD.

[85] Diretiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de Novembro de 2009 que altera a Diretiva/2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados e à proteção da privacidade no setor das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor, disponível em:
https://eurex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32009L0136&from=PT.
[86] Regulamento (EU) 611/2013 da Comissão, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho relativa à privacidade e às comunicações eletrónicas
[87] Cf. artigo 1.º da Regulamento (EU) n.º 611/2013, sobre o âmbito de aplicação do diploma.

violações de dados que sejam suscetíveis de provocar risco para os direitos e liberdades das pessoas singulares.

Tendo em conta o descrito no considerando 87 do RGDP, "há que verificar se foram aplicadas todas as medidas tecnológicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação de dados pessoais e para informar rapidamente a autoridade de controlo e o titular. Para comprovar que a notificação foi enviada sem demora injustificada importa ter especialmente em consideração a natureza e gravidade da violação dos dados pessoais, assim como as respetivas consequências e efeitos adversos para os titulares dos dados. Essa notificação poderá resultar numa intervenção da autoridade de controlo em conformidade com as suas funções e competências, definidas pelo presente regulamento"[88].

Do mesmo modo, o Grupo de Trabalho do Artigo 29º (GT29), considera que o novo requisito de notificação tem diversos benefícios, pois os responsáveis pelo tratamento de dados ao notificarem à autoridade de controlo, podem obter aconselhamento sobre as pessoas singulares afetadas que devem ser informadas. A comunicação de uma violação permite ao responsável pelo tratamento de dados prestar informação sobre os riscos decorrentes da violação e as principais medidas que estas pessoas devem ter para se protegerem das suas consequências.

Qualquer plano de resposta a uma violação dos dados pessoais deve centrar-se na proteção de pessoas e dos seus dados pessoais. E, como consequência a notificação da violação deve ser observada principalmente como um instrumento de reforço da conformidade relativo à proteção de dados pessoais, e a não comunicação de uma violação pode significar de acordo com o artigo 83º, é aplicável a uma sanção ao responsável pelo tratamento.

2.3.1 Notificação de Dados Pessoais no Âmbito do RGDP

O RGDP possui algumas disposições relacionadas sobre quando uma violação deve ser notificada e a quem, bem como sobre a informação a ser prestada. Assim, a informação necessária para a notificação de violação deve ser fornecida por fases. No

[88] Relativamente às competências das autoridades de controlo nesta matéria, veja-se o artigo 51.º e ss. do RGPD.

seu parecer 03/2014[89], relacionado com a notificação da violação de dados pessoais, o GT29 disponibilizou orientações específicas aos EPDs para auxiliar na decisão de notificar os titulares de dados em caso de violação, o qual teve em conta a obrigação dos fornecedores ao abrigo da Diretiva 2002/58/CE, e disponibilizou exemplos de vários setores no contexto do projeto de RGDP, bem como as boas práticas para todos os EPDs.

Um dos novos requisitos do RGDP é que por meio da adoção de medidas técnicas e organizativas apropriadas os dados pessoais são tratados com o objetivo de assegurar a segurança adequada dos dados pessoais, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental[90]. Como resultado, o RGDP requer que os EPDs e os subcontratantes possam aplicar as medidas técnicas e organizativas adequadas com a finalidade de assegurar um nível de segurança apropriado ao risco que os dados pessoais impõem[91].

Neste contexto, deve-se ter em consideração as técnicas mais avançadas, os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades de tratamento de dados, e o risco decorrente do tratamento, que pode ser variável. Para além de que, o RGDP exige que sejam adotadas as medidas tecnológicas de proteção e de organização para apurar a ocorrência de uma violação de forma imediata, e assim está representada a obrigação de notificação[92].

2.3.2 Prazo para a notificação

O EPD tem como obrigatoriedade notificar a violação dos dados pessoais que tenha sofrido à autoridade de controlo competente sempre que possível nas 72 horas seguintes ao momento em que tenha tido conhecimento da mesma (artigo 33º, nº 1, RGDP). Ou seja, de acordo com o artigo 33º, é pertinente definir qual o momento em que o EPD tenha "tido conhecimento", da violação dos dados pessoais e a partir daí estabelecer o prazo de 72 horas.

---

[89] Ver o Parecer 03/2014 relativo à notificação da violação de dados pessoais http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/files/2014/wp213_en.pdf

[90] Ver artigo 5.º, n.º 1, alínea f) e artigo 32.º.

[91] Artigo 32.º; ver igualmente o considerando 83.

[92] Ver considerando 87

No que concerne a este aspeto o Grupo do Artigo 29, atual Comité Europeu para a Proteção de dados, consagra que o EPD toma conhecimento da violação de dados pessoais na altura em que tiver um grau de certeza razoável de que ocorreu um incidente que afetou a proteção de dados pessoais[93].

Importa ainda referir que o prazo que é concebido ao EPD são de 72 horas após a tomada de conhecimento com a pretensão de fornecer a possibilidade de avaliação de risco para os titulares dos dados e proporcionar uma resposta adequada à violação. Assim, mesmo que o EPD tenha uma perceção não clara das implicações da violação, principalmente pela força de avaliação do impacto sobre a proteção de dados (AIPD) realizada de forma prévia, a avaliação dos danos e as circunstâncias concretas terá de ser considerada objeto de uma nova avaliação, de acordo com a violação de dados pessoais observada.

Neste contexto, terá como resultado que a AIPD é pertinente prever abstratamente os riscos de um tratamento de dados específico, enquanto adota um conjunto de medidas de segurança em conformidade, embora não dispense uma análise mais meticulosa do impacto real de uma violação de dados pessoais após esta ocorrer.

De acordo com o legislador, este prazo de 72 horas pode ser considerado curto para a tomada de medidas apropriadas, entende-se que a existência anterior de um plano operacional de resposta pode ser uma boa prática para facilitar a execução dos mecanismos internos.

Mesmo que o responsável e o subcontratante tenham a obrigação de implementar as medidas técnicas e organizativas que sejam necessárias para a proteção dos dados pessoais, devem articular entre si um plano estratégico de resposta face a esta situação[94].

[93] Cf. EDPB Guidelines on Personal data breach notification under Regulation 2016/679, de 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018:
http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827 p. 10 e ss.
[94] Cf. n.º 1 do artigo 32.º do RGPD.

2.4 Responsabilidade do EPD no Direito Comparado

2.4.1 França

A primeira legislação adotada na França em relação à proteção dos dados pessoais era a Lei nº 78-17 de 6 de janeiro de 1978. Embora com o surgimento da internet, a Lei nº 78-17 não foi alterada por 25 anos. A primeira alteração foi adotada apenas a 6 de agosto de 2004, com o objetivo de transpor a Diretiva 95/46 CE[95].

Nesta alteração, os Estados-Membros tiveram três anos para implementar as modificações à lei. A França demorou quase nove anos porque precisava de uma reforma de longo alcance da Lei nº 78-17[96] que se focou no setor público. Assim, o NDPA é a segunda reforma mais importante desta Lei. No entanto, na altura da redação, o NDPA ainda não entrou em vigor porque 60 senadores o encaminharam ao Conselho Constitucional, e argumentou-se que não estava em conformidade com a Lei Constitucional Francesa.

O Projeto de Lei só foi proposto pelo Governo a 23 de dezembro de 2017[97], após a consulta do Conselho d'Etat e a Autoridade Francesa de Proteção de Dados (Commission Nationale de l'Informatique et des Libertés, CNIL)[98].

Este atraso foi devido às eleições presidenciais e legislativas francesas que ocorreram em junho de 2017. Contrariamente, do que ocorreu na Alemanha, o governo francês estava no comando quando o RGPD foi adotado. No entanto, alguns trabalhos ex-parlamentares facilitaram a adoção do NDPA. Primeiramente, a proteção de dados e o próximo RGPD foi o núcleo da adoção da Lei da República Digital[99]. Esta lei

[95] Diretiva 95/46 CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 sobre a proteção de indivíduos em relação ao tratamento de dados pessoais e a livre circulação de tais dados, JO L 281/0031

[96] Lei nº 78-17 de 6 de janeiro de 1978 relativa ao processamento de dados, arquivos e liberdades; uma versão em inglês, mas não atualizada está disponível em https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf

[97] Projeto de lei n ° 490 relativo à proteção de dados pessoais, aprovado em 13 de dezembro de 2017

[98] Declaração da CNIL, 30 de novembro de 2017 (avis de la CNIL Délibération n ° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n ° 78-17 du janvier 1978) https://www.cnil.fr/sites/default/files/atoms/files/projet_davis_cnil.pdf

[99] Lei n ° 2016-1321 de 7 de outubro de 2016 para uma república digital, https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000031589829&type=general&legislature=1

introduziu antecipadamente alguns direitos de notícias para o titular dos dados[100], uma ação coletiva em proteção de dados e o maior poder de fiscalização da CNIL.

Na França, os principais regulamentos relacionados com os dados pessoais são a Lei nº 78-17 sobre a Tecnologia da Informação, Arquivos de Dados e Liberdades Civis, de 6 de janeiro de 1978, conforme emenda pela Lei nº 2018-493 de 20 de junho de 2018 sobre Proteção de Dados Pessoais, que integra algumas disposições do Regulamento da UE 679/2016 relacionadas com a proteção de dados de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação destes dados que entrou em vigor a 25 de maio de 2018.

Ao nível nacional, é tomada a posição sobre algumas cláusulas iniciais do RGDP e implementa a Diretiva 2016/680 sobre a proteçao de pessoas em relação ao tratamento de dados pessoais pelas autoridades competentes para fins de prevenção, investigação, deteção ou repressão de infrações criminais ou a execução de penalidades criminais, e no livre movimentação de tais dados.

Há um conjunto de leis e regulamentos relacionados com a proteção de dados pessoais que regulam setores específicos, incluindo o Código Postal e das Comunicações Eletrónicas[101]; o código do consumidor [102]; o Código de Saúde Pública[103] (sobre o processamento de dados de saúde); bem como o Código de propriedade[104] (sobre a retenção de dados pessoais contidos em arquivos públicos). Estas disposições não foram alteradas após a entrada em vigor do RGPD.

De igual modo, as regras nacionais que foram adotadas para as quais o RGPD possibilita que os Estados-membros legislem e aplicam-se a titulares de dados que residam em França, mesmo que o controlador de dados não esteja estabelecido em

[100] ou seja, o direito de ser esquecido pelos menores
[101] (artigos L.34 e seguintes e artigos R.10 e seguintes)
[102] (artigos L.223-1 e seguintes) (sobre telemarketing),
[103] (Artigos L.1110-4 e segs, L.1111-8 e segs, L.1115-1 e seguintes, L.1122-1 e seguintes, L.1435-6, L.1460-1 et seq, R.1111-1 et seq)
[104] (Artigo L.212-3)

França, com exceção, do processamento relacionado com a liberdade de expressão e informação quando a lei aplicável é a do estado-membro da UE[105].

A lei francesa introduziu igualmente um novo artigo 5-1 para o DFPA que aplica a legislação francesa adotada com base no RGPD amplo e nas cláusulas de abertura quando o individuo resida em França, incluindo o controlador de dados não estabelecido em França[106].

O RGPD requer que controladores e processadores de dados apontem um oficial de proteção de dados (DPO) em certas circunstâncias (Artigo 37 (1), GDPR; Nota Prática, Responsáveis pela proteção de dados sob o RGPD e DPA 2018 (w-010-3427)). O RGPD permite que os estados-membros possam exigir nomeações DPO em situações adicionais (Artigo 37 (4), GDPR). A lei francesa RGPD não exige a nomeação de um DPO sob circunstâncias adicionais ou alterar os requisitos ou as obrigações aplicáveis aos DPOs segundo o GDPR.

2.4.2 Alemanha

A Alemanha ajustou a estrutura legal alemã ao RGPD aprovando a nova Lei de Proteção de Dados Federal Alemã (Bundesdatenschutzgesetz - 'BDSG'). O BDSG foi publicado oficialmente em 5 de julho de 2017 e entrou em vigor em conjunto com o RGPDem 25 de maio de 2018. O objetivo do BDSG é especialmente fazer uso das inúmeras cláusulas de abertura ao abrigo do GDPR, que permite aos Estados-Membros especificar ou mesmo restringir os requisitos de processamento de dados ao abrigo do GDPR.

Além do BDSG, existe uma série de regras de proteção de dados em leis específicas da área, por exemplo, aquelas que regulam o comércio financeiro ou do setor de energia. Muitas dessas leis foram adaptadas ao RGPD pelo Second Data Protection Ato de adaptação e implementação da UE (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU - ‘2. DSAnpUG-EU’), que geralmente entrou em vigor em 26 de novembro de 2019. No entanto, algumas leis particularmente relevantes permaneceram até agora inalteradas, principalmente a Lei de Telemedia

[105] (Artigo 5-1, DPA).
[106] Artigo 10, Lei francesa GDPR).

(Telemediengesetz - ‘TMG’), levantando questões sobre a aplicabilidade continuada das regras de proteção de dados nele contidas

A Alemanha não tem uma autoridade central de proteção de dados ('DPA'), mas as várias autoridades diferentes para cada um dos 16 estados alemães (Länder) que são responsáveis por garantir que as leis e regulamentos de proteção de dados sejam cumpridos. Além disso, o Comissário Federal Alemão para Proteção de Dados e Liberdade de Informação (Bundesbeauftragte für Datenschutz und Informationsfreiheit - ‘BfDI’) é a Autoridade de Proteção de Dados para fornecedores de serviços de telecomunicações e representa a Alemanha no Conselho Europeu de Proteção de Dados. Para garantir que todas as autoridades tenham a mesma abordagem, foi estabelecido um comité composto por membros de todas as Autoridades - a 'Conferência de Proteção de Dados' (Datenschutzkonferenz 'DSK'). O mecanismo de coordenação entre as autoridades alemãs espelha a consistência do mecanismo sob o RGPD.

O BDSG fornece regras especiais relativas ao processamento para fins relacionados ao emprego na Seç. 26 BDSG. O legislador alemão fez um uso muito amplo da cláusula inicial do art. 88 (1) RGPDe basicamente estabeleceu um regime específico de proteção de dados de funcionários. Estas novas regras refletem as atuais regras de privacidade dos funcionários alemães que também têm como consequência a aplicação de um conjunto de jurisprudência do Tribunal Federal do Trabalho Alemão (Bundesarbeitsgericht - ‘BAG’).

Os dados pessoais dos funcionários só podem ser processados no contexto de emprego (deixando de lado alguns casos muito especiais no âmbito do BDSG quando se trata da avaliação da capacidade de trabalho do funcionário e outro tratamento de dados de categorias especiais, bem como troca de dados com as obras do conselho) nos seguintes casos:

1) O processamento é necessário para as decisões de contratação ou, após a contratação, para a efetivação ou rescisão do contrato de trabalho[107] (o BAG interpreta a disposição anterior de forma mais ampla do que Art. 6 (1) (b) RGPD

[107] (Seção 26 (1) frase 1 BDSG)

2) Os dados pessoais dos funcionários podem ser processados para detetar crimes apenas se houver uma razão documentada para acreditar que o titular dos dados cometeu tal crime enquanto estava empregado, o processamento de tais dados é necessário para investigar a ofensa e não seja superado pelo interesse legítimo do titular dos dados em não processar os dados e, em particular, o tipo e a extensão não são desproporcionais à razão (Seção 26 (1) sentença 2 BDSG)[108].

2.4.3 Estados Unidos

A primeira legislação dos EUA abordou especificamente as consequências prejudiciais de dados pessoais realizadas em bancos de dados computorizados foi o Fair Credit Reporting Act de 1970[109], uma prática comum no discurso jurídico dos Estados Unidos. A FCRA foi aprovada para reformar a indústria de crédito ao consumidor, impondo limites à partilha de dados e tornando mais fácil para os indivíduos corrigir erros.

Os Estados Unidos carecem de uma lei federal única e abrangente que regule a colheita e o uso de informações pessoais. Em vez disso, o governo abordou a privacidade e a segurança regulamentando apenas em certos setores e tipos de informações confidenciais (por exemplo, saúde e finanças), criando proteções sobrepostas e contraditórias.

O RGPD, que entrou em vigor em 25 de maio de 2018, é uma das leis de proteção de dados mais abrangentes do mundo até o momento. Na ausência de uma abrangente lei federal de privacidade nos EUA, a CCPA é considerada uma das leis de privacidade legislativas mais importantes no desenvolvimento no país. Tal como o RGPD, o impacto do CCPA deve ser global, dado o status da Califórnia como a quinta maior economia global. A CCPA entrou em vigor no dia 1 de janeiro de 2020, mas certas disposições da CCPA exigem que as organizações forneçam aos consumidores com informações sobre o período de 12 meses anteriores e, portanto, atividades para cumprir a CCPA podem ser necessárias antes da data efetiva

[108] O processamento é realizado com base em contrato de conselho de empresa que atende aos requisitos do art. 88 pára. 2 RGPD(Seção 26 (4) BDSG

[109] Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006).
Available at: https://www.law.cornell.edu/uscode/text/15/168

O Artigo 4 (1) do RGPD esclarece que o titular dos dados é “uma pessoa física identificada ou identificável.” Artigo 3 e os considerandos 2, 14 e 24 estabelecem que o titular dos dados pode ser qualquer indivíduo cujos dados pessoais são processados, e não exigem especificamente que o titular dos dados tenha residência na UE ou cidadania, ou está localizado dentro ou fora da UE.

O CCPA aplica-se a empresas que fazem negócios na Califórnia e, embora não seja explicitamente mencionado, o CCPA parece ser aplicável a uma empresa estabelecida fora da Califórnia se ela colher ou vender informações pessoais de consumidores da Califórnia enquanto conduz negócios no território.

Ao contrário do RGPD, o CCPA fornece vários carve-outs específicos de seu escopo de aplicação, como informações médicas e informações protegidas de saúde. A CCPA também exclui informações pessoais a transferência de dados para terceiros no contexto de uma fusão (da definição de “venda”). No entanto, a lei ainda permite o direito de *opt-out* se a entidade resultante usar estas informações de forma materialmente inconsistente com “as promessas feitas no momento da colheita.

"Controladores" sob o RGPD têm similaridade com "empresas" sob a CCPA, já que ambos são responsáveis por cumprir com as obrigações ao abrigo das respetivas leis. Algumas das obrigações do RGPD, no entanto, também se aplicam a "processadores", que são entidades que processam dados pessoais em nome de controladores e sob a direção destes[110].

2.4.4 Reino Unido

O objeto da Diretiva Europeia de Proteção de Dados, implementada no Reino Unido pela DPA, é estabelecer que "os Estados-Membros devem proteger os direitos e liberdades fundamentais das pessoas físicas, e, em particular, seu direito à privacidade no que diz respeito ao processamento de dados pessoais ”[111].

'Dados pessoais' são definidos no Artigo 2 da Diretiva por referência a informações que se relacionam a uma identificação Individual. A diretiva prevê, no seu

[110] CCPA, Sections 1798.105, 1798.140, 1798.145, 1798.155
[111] As defined in European Directive Article 2 (c)

artigo 3.º, que se aplica apenas ao processamento de dados pessoais, quando o processamento é total ou parcial por meios automáticos, ou onde é o processamento não automatizado de dados pessoais que fazem parte de um 'sistema de arquivo".

A DPA repete a essência da definição da Diretiva de 'Dados pessoais', mas aborda a definição na ordem inversa à Diretiva. O DPA primeiro considera a natureza do processamento para determinar se as informações em questão são "dados" (ou processado por meios automáticos ou processamento não automatizado dentro um sistema de arquivo) e, em segundo lugar, considera se os "dados" são 'Dados pessoais' no que se refere a um indivíduo identificável.

O DPA apresenta mais dois tipos de processamento manual de informações que, se as informações se referem a um individuo identificável, envolverá o processamento de "dados pessoais". Estas categorias adicionais de processamento são introduzidas no DPA na definição de 'dados' e preocupação, nomeadamente, o processamento de informações como parte de um "registo acessível"[112] e, o processamento de informações registadas mantidas por uma autoridade pública (referidos como dados de 'categoria' e ', uma vez que se enquadram no parágrafo (e) da definição de "dados" da seção 1 (1) do DPA).

O Reino Unido tem fortes padrões domésticos de proteção de dados pessoais, definidos na Lei de Proteção de Dados (DPA) de 1998. A nova Lei de Proteção de Dados do Reino Unido, que será revogada e substituiu o DPA 1998, foi anunciado num discurso da rainha[113]. Fortaleceu igualmente, os padrões do Reino Unido, garantindo que estejam atualizados para a era moderna, e implementou o novo quadro de proteção de dados da UE no direito interno.

O Data Protection Act 2018 é a implementação do Regulamento Geral de Proteção de Dados (RGPD) no Reino Unido. Todos os responsáveis pela utilização de dados pessoais têm de seguir regras estritas denominadas "princípios de proteção de dados". Eles devem certificar-se de que as informações são:

[112] Accessible record' is defined in section 1(1)(d) and section 68 DPA.
[113] Maxmillian Schrems v Data Protection Commissioner (C-362/14), Grand Chamber, 6 October 2015.

- usadas de forma justa, legal e transparente;
- usadas para fins específicos e explícitos;
- usadas de uma forma adequada, relevante e limitada apenas ao necessário;
- precisos e, quando necessário, mantidas atualizadas;
- mantido por não mais do que o necessário;
- tratada de uma forma que garanta a segurança adequada, incluindo a proteção contra o processamento, acesso, perda, destruição ou dano ilegal ou não autorizado.

2.4.5 Espanha

A proteção de pessoas físicas em relação ao tratamento de dados pessoais é um direito fundamental protegido pelo artigo 18.4 da Constituição Espanhola. Desta forma, a Constituição Espanhola foi pioneira no reconhecimento do direito fundamental à proteção de dados pessoais, quando estipulado que "a lei deve limitar o uso da informática para garantir a honra e privacidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos". Assim, ecoou o trabalho realizado desde o final dos anos 1960 no Conselho da Europa e as poucas disposições legais adotadas nos países vizinhos[114].

O Tribunal Constitucional indicou na sua Sentença 94/1998, de 4 de maio, que estamos perante um direito fundamental à proteção de dados, pelo qual é garantido à pessoa o controlo sobre seus dados, quaisquer dados pessoais e o seu uso e destino, para evitar o tráfico ilícito do mesmo ou prejudicial à dignidade e direitos do afetado; desta forma, o direito à proteção de dados é configurado como uma faculdade do cidadão de se opor à utilização de certos dados pessoais para fins diversos do que justificou a sua obtenção.

Por sua vez, no Julgamento 292/2000, de 30 de novembro, considerou-se que é um direito autónomo e independente que consiste em um poder de disposição e controle

[114] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Jefatura del Estado. «BOE» núm. 294, de 6 de diciembre de 2018 Referencia: BOE-A-2018-16673

sobre os dados pessoais que capacita a pessoa que decide quais desses dados fornecer a um terceiro, seja ele o Estado ou um particular, ou que terceiros podem colher, e que também permite que o indivíduo saiba quem é o proprietário desses dados pessoais e com que finalidade, podendo se opor a tal posse ou uso.

Mais especificamente, a Constituição Espanhola estabelece o seguinte no artigo 18: "O direito à honra, privacidade pessoal e familiar e de imagem própria ", acrescentando no artigo 4 que" a lei limitará o uso de computadores para garantir a honra e a privacidade pessoal e familiar dos cidadãos e o exercício pleno dos seus direitos".

A proteção de indivíduos com relação ao processamento automatizado de dados de caráter pessoal foi inicialmente desenvolvida pela Lei Orgânica 5/1992, de outubro. Antes da aprovação deste texto legal, a Espanha tinha assinado a 28 de janeiro de 1982, a Convenção da Comunidade sobre o assunto, aprovada e ratificada, para a sua entrada em vigor a 1 de outubro de 1985.

A citada Lei Orgânica 5/92 foi revogada e substituída pela Lei Orgânica de Proteção de Dados Pessoais, que adaptou legislação interna às diretrizes dos Regulamentos da União Europeia e, especificamente, a Diretiva Comunitária 1995/46, de 24 de outubro, do Parlamento Europeu e do Conselho, sobre a proteção de pessoas singulares no tratamento de dados pessoais e na livre circulação destes dados. Da mesma forma, devemos ter em mente que a Carta dos Direitos Fundamentais da UE reconhecem-no a nível comunitário como um direito fundamental (artigo 8º)[115].

No sistema Jurídico, o marco regulatório neste caso, é composto pelos seguintes padrões: Regulamento (UE) 2016/679 do Parlamento Conselho e Conselho de 27 de abril de 2016 (Proteção Geral de Dados),

O artigo 1º do RGPD indica a proteção dos direitos e liberdades como objeto de direitos fundamentais das pessoas singulares e, em particular, o seu direito à proteção de

[115] Lei Orgânica de Proteção de Dados (agora também sobre "Garantias de direitos digitais") su trabajo: «De la libertad informática a la constitucionalización de nuevos
derechos digitales (1978-2018)», Revista de Derecho Político, 100, UNED (septiembre-diciembre de 2017), pp. 639-669.

dados pessoais. Acrescenta também que a livre circulação de dados pessoais na União não pode ser restringida ou proibida por motivos relacionados à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais[116].

2.5 Os novos impactos do RGDP no tratamento de dados pessoais

2.5.1 A ilicitude

A ilicitude é designada como a anti juridicidade e a outra forma de ilegalidade, é a divergência ou a oposição entre o fato humano e o ordenamento jurídico pelo seu conjunto que conduz à lesão de um bem jurídico, ou a negação/violação de certos valores jurídico-criminais[117].

De acordo com Figueiredo Dias a ilicitude somente seria extinguida em nome do exercício de um direito, ou seja, um entendimento que, de acordo com a doutrina, encontra acolhimento legal no artigo 44º, nº 4 do CP, através do qual "justificam o fato: os que praticarem o fato no exercício de um direito ou no cumprimento de uma obrigação se tiverem procedido com negligencia devida"[118].

De acordo com a análise do direito ao recurso à via judicial atribuído aos titulares dos dados pessoais, este direito tem como base dois pressupostos, a existência de uma violação dos direitos dos titulares de dados e a violação destes direitos que resulte de um tratamento de dados pessoais efetuado ao "arrepio" do Regulamento.

Tal como já referido, observa-se que uma violação dos direitos dos titulares de dados, resulta de uma violação ao RGDP, e é igualmente necessário que esta violação ocorra de um tratamento de dados pessoais efetuado em violação ao RGDP, com incumprimento[119].

---

[116] Ver: RODRÍGUEZ ÁLVAREZ, L.: «Artículo 18.4 CE», Comentarios a la Constitución de 1978. Libro Homenaje al Profesor Luís López Guerra, Valencia, Tirant lo Blanch, 2018.

[117] SILVA, Germano Marques da Direito Penal Português, Volume II, 2.ª Edição, Editorial Verbo, Lisboa, 2005, p. 22; SIMAS SANTOS, Manuel et LEAL-HENRIQUES, Manuel, Noções de Direito Penal, 4.ª Edição, Rei dos Livros, Porto, 2011, pp. 18 ss

[118] DIAS, Jorge de Figueiredo; MONTEIRO, Jorge Sinde. Responsabilidade Médica…, p. 53.

[119] Entre outros, vd. Oliveira, Princípios de Direito, 617 e seg

O artigo 82º do RGDP, que descreve o direito de indemnização, alude à produção dos dados materiais ou imateriais, decorrentes de uma violação do regulamento. E, para que seja possível a ilicitude, deve ser verificado uma desconformidade relativa ao regime legal constante do RGDP, e assim optar-se por uma interpretação mais ampla do conceito de ilicitude.

O ato lesivo cuja prática é da responsabilidade do responsável pelo tratamento de dados ou subcontratante, pode violar qualquer um dos princípios legais do RGDP, e não se limita a uma ilicitude relacionada com os fundamentos para o tratamento de dados[120].

Importa salientar que, no caso de um dos requisitos de que depende o direito à indemnização esteja preenchido, o requisito da ilicitude estará preenchido igualmente, isto porque uma violação ao direito dos titulares de dados unifica uma violação ao RGDP, e que por consequência na sua ilicitude[121].

No entanto, a dignidade humana impõe o respeito pela vida privada, pelo que, "ainda que o RGPD sujeite as restantes dimensões da vida privada ao regime dos dados abrangidos pelo artigo 6.º, esse regime tem de ser interpretado em conformidade com os artigos 26.º, n.º 1, e 35.º, n.º 3, da CRP, e com o artigo 8.º da Convenção Europeia dos Direitos do Homem e o artigo 7.º da Carta dos Direitos Fundamentais, garantindo sempre o resultado da proteção efetiva da vida privada". Tal significa que, na avaliação da ilicitude do tratamento, deverá ser refletido se não foi "exposta desnecessariamente ou de modo insuportável a vida privada dos titulares ou se existiu um risco sério de resultado discriminatório para os mesmos"[122].

2.5.2 A culpa

A culpa representa o fundamento e o limite do direito de punir num Estado de Direito democrático (nullum crimen sine culpa). Este princípio é expresso na doutrina onde está mencionado "a determinação da medida da pena, dentro dos limites definidos

[120] Cf. resulta do artigo 6.º do RGPD.
[121] a respeito dos conceitos de dolo e de negligência, Oliveira, Princípios de Direito, 428 e segs.
[122] Vide Parecer n.º 20/2018, op. cit, ibid.

na lei, é feita em função da culpa do agente", sendo que esta culpa é semelhante aquela em que a pena seja gradual[123].

A culpabilidade é o juízo de censura jurídica do agente, por ter cometido o ilícito e não ter agido de acordo com o direito, pelo que se pressupõe para a formulação deste juízo de valor que o indivíduo atue segundo a consciência ética e liberdade na sua tomada de decisão, excluindo-se os inimputáveis pois estes não conseguem realizar este tipo de censura[124].

De acordo com o Professor Germano Marques da Silva[125], "a imputabilidade é a imputação em potência como a imputação é a imputabilidade em ato". A imputabilidade é a possibilidade de se poder imputar a alguém um facto mediante as suas capacidades. Assim, a inimputabilidade pode-se dar por razões de idade ou por anomalia psíquica

A culpa pode assim, ser observada através de um plano objetivo ou subjetivo, sendo objetivo quando se atribui a uma pessoa um ato ilícito pelo qual aquela é de forma objetiva responsável, e subjetiva quando se verifique os pressupostos para imputar a uma pessoa em particular a responsabilidade do ato[126].

O responsável pelo tratamento de dados ou o subcontratante ficam isentos de culpabilidade, de acordo com o artigo 82º, nº 3, do RGDP, no caso em provém que não são responsáveis pelo acontecimento que deu origem aos danos, ou seja, que ambos não tenham atuado com dolo ou negligencia[127]. Neste caso específico, estamos perante uma causa de exclusão de culpabilidade onde o responsável de tratamento de dados ou o subcontratante não originaram, de forma dolosa ou negligenciada, a situação de violação.

---

[123] FERREIRA, Manuel Cavaleiro de, Lições de Direito Penal, Parte Geral I , Reimpressão da 4.ªedição, Almedina, Coimbra, 2010, p. 89

[124] FIGUEIREDO DIAS, Jorge de, Direito Penal – Parte Geral, Tomo I, 2.ª edição, Coimbra Editora, Coimbra, 2007, pp.82 ss; SIMAS SANTOS, Manuel et LEAL-HENRIQUES, Manuel, Noções de Direito Penal, 4.ª Edição, Rei dos Livros, Porto, 2011, pp. 81 ss.

[125] SILVA, Germano Marques, Direito Penal Português, Volume II, 2.ª Edição, Editorial Verbo, Lisboa, 2005, p. 163.

[126] SIMAS SANTOS, Manuel et LEAL-HENRIQUES, Manuel, Noções de Direito Penal, 4.ª Edição, Rei dos Livros, Porto, 2011, pp. 81 ss.

[127] a respeito dos conceitos de dolo e de negligência, Oliveira, Princípios de Direito, 428 e segs.

A este aspeto, estão associados os princípios relativos ao tratamento de dados pessoais, máxime, o princípio da integralidade e confidencialidade, através dos quais são tratados os dados pessoais para garantir segurança contra a destruição ou danificação acidental, adotando-se, para o efeito as medidas técnicas ou organizativas adequadas.

E a adoção destas medidas técnicas e organizativas deve incluir a pseudonimização e a cifragem dos dados pessoais, ou seja, a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; e um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento[128]. Sublinha Sinde Monteiro que "a culpa tem agora de se referir apenas à própria violação da norma e já não à violação dos bens jurídicos"[129].

As informações pseudonimizadas ainda são uma forma de dados pessoais, mas o uso de pseudonimização é encorajado, por exemplo, como um fator a ser considerado ao determinar se o processamento é "incompatível" com os fins para os quais os dados pessoais foram colhidos e processados originalmente; e está incluído como um exemplo de uma técnica que pode satisfazer os requisitos para implementar "privacidade desde o design e por inadimplência" (obrigações de governança de dados);

2.6 Mudança de paradigma do novo Regulamento

O RGPD trouxe várias mudanças que terão impacto na vida das empresas e das entidades públicas e para as quais as mesmas terão de se adaptar. Por esse motivo, o RGPD estabelece um período de dois anos para que as organizações se possam adaptar no sentido de cumprir com as novas obrigações a que estão sujeitas.

[128] Nos termos do disposto no n.º 2 do artigo 32.º do RGPD, "Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

[129] Sinde MONTEIRO, Responsabilidade por conselhos, recomendações ou informações, Almedina, Coimbra, 1989, 239.

A mudança de paradigma relaciona-se com a legislação vigente sobre a proteção de dados, isto porque já não são necessárias as notificações à CNPD, e passa a ser da responsabilidade do responsável pelo tratamento de dados pessoais, ou seja, no caso das organizações que tratam dos dados, para implementar os mecanismos de cumprimentos dos mesmos.

Nas palavras de ALESSANDRA SILVEIRA[130], a separação dos regimes nacionais existentes, que resultaram de diversas transposições da Diretiva 95/46/CE, era considerada uma das principais causas, com base na uniformidade jurídica, justificaram a necessidade de reforma.

De referir que, tendo em conta a rápida evolução tecnológica, a UE adotou a nova legislação a 4 de maio de 2016, para adaptação das regras de proteção de dados à era digital. A este aspeto, o RGDP considerou como paradigma a tecnologia disponivel para a realização do tratamento de dados pessoais e, assim poder conciliar a utilização de soluções tecnológicas, o futuro desenvolvimento e os riscos associados, com base na defesa dos direitos e liberdades das pessoas[131].

Não obstante a referida reforma tem como base alguns pilares como as normas coerentes, procedimentos mais simplificados, ações coordenadas, participação dos utilizadores, informações mais eficazes e poderes coercivos reforçados[132]. Embora, esta reforma não estabeleceu uma rutura absoluta entre o sistema de proteção de dados descritos na Diretiva 95/46/CE e o sistema do RGDP.

Tendo em conta a necessidade de garantir a livre circulação de dados pessoais num mercado sem fronteiras, o RGDP foi pensado para a proteção dos cidadãos, em

[130] De acordo com SILVEIRA, Alessandra; FROUFE, Pedro – Do mercado interno à cidadania…, op. cit., pág. 9

[131] De acordo com o Parecer n.º 20/2018, de 2 de maio de 2018, Processo n.º 6275/2018, da Comissão Nacional de Proteção de Dados (C.N.P.D.). [Consulta em 05 de outubro de 2020]. Disponível para consulta em: http://bit.ly/2GrYSjQ. Pág. 2

[132] Cfr. o GRUPO DE TRABALHO DO ART. 29.º DA DIRETIVA 95/46/CE PARA A PROTEÇÃO DE DADOS – Diretrizes de aplicação e fixação de coimas para efeitos do Regulamento 2016/679, 17/PT, WP 253, adotadas em 3 de outubro de 2017. [Consulta em 04/10/2020]. Disponível para consulta em: http://bit.ly/2VRYiCx. Pág. 4.

prol do tratamento dos dados pessoais numa escala ampla, por grandes empresas e serviços de informação[133].

Nas palavras de JOSÉ LOBO MOUTINHO[134], no direito de proteção de dados pessoais, foi conferida a dignidade constitucional e, a tutela constitucional ao titular de dados pessoais, pelo legislador constitucional português, integrados no Capítulo I, do Título II, destinado aos «direitos, liberdades e garantias», através do art. 35.º, na versão originária da C.R.P., aprovada em 2 de abril de 1976[135].

De acordo com o descrito no artigo 35º, da CRP o legislador constitucional teve como pretensão referir-se à "utilização da informática" e, reconhecer a importância do tratamento de forma automatizada dos dados pessoais[136]. E, o que se propôs no mesmo artigo, nº 1 através do qual se descreve que "todos os cidadãos têm o direito de acesso aos dados informatizados que lhe digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei", foi aprovado por unanimidade.

Assim, o novo texto do nº 1, artigo 35º, CRP, não registou alterações significativas em relação à redação anterior, salvo na parte final em que foi adotada uma

---

[133] Em conformidade, veja-se GABRIEL, João – Atlas, mostra alto o mundo no seu ombro – Aplicabilidade extraterritorial do
Regulamento Geral de Proteção de Dados. Vida Judiciária. Porto, Portugal: Vida Económica. N.º 207, maio-junho de 2018, pág. 26

[134] No mesmo sentido, cf. MOUTINHO, José Lobo – Legislador português precisa-se. Algumas notas sobre o regime sancionatório no Regulamento Geral Sobre a Proteção de Dados (Regulamento (UE) 2016/679) – Em Foco: Inteligência Artificial. Revista Fórum de Proteção de Dados. Portugal: Comissão Nacional de Proteção de Dados. N.º 4, julho de 2017, pág. 43.

[135] Apesar de já existirem textos essenciais em matéria de proteção de dados, o texto constitucional português de 1976 foi pioneiro na previsão da proteção de dados como «direito» – ainda que tão-somente de forma indireta (i.e., a partir da interpretação dos diversos números do artigo) –, o que o torna bastante inovador. A versão originária da C.R.P. continha uma disposição normativa – o art. 35.º – sob a epígrafe «utilização da informática», não fazendo referência, em qualquer dos seus números, à «proteção de dados» ou ao «direito à proteção de dados». Atenta a redação do art. 35.º na versão originária – "1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização. 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.

[136] SILVEIRA, Luís Lingnau da – "Configuração constitucional…", op. cit., pág. 506.

fórmula mais ampla, ou seja, "nos termos da lei", em lugar da anterior, mais restritiva ("sem prejuízo do disposto na lei sobre o segredo de Estado e segredo de justiça")[137].

Nas palavras de JOAQUIM SEABRA[138], no nº 2, do artigo 35º, 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 proteção, designadamente através de entidade administrativa independente".

A entrada em vigor do RGDP a 25 de maio de 2016, e com a obrigatoriedade da sua aplicação a partir de 25 maio 2018, teve algumas dificuldades face a atual redação do artigo 35º, da CRP e, a referencia à lei em seis dos sete números deste artigo, não deveria manter-se com exceção que se associe o qualificativo "europeia"[139].

Outra especificidade do novo regulamento refere-se aos casos de não aplicabilidade da proibição de tratamento de dados pessoais do artigo 9º, nº 1, do RGDP, que são substancialmente distintos dos previstos no art. 35.º, n.º 3, da C.R.P., que se limitam ao "consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis". Ou seja, já existia conflito com as situações de não aplicabilidade da proibição de tratamento de dados pessoais, do artigo 8º, nº 1 da Diretiva 95/46/CE[140].

Nas palavras de ALEXANDRE SOUSA PINHEIRO[141], o direito à proteção de dados pessoais fundou-se doutrina e jurisprudencialmente no princípio da dignidade da pessoa humana, e por esta razão deve ser entendido como uma especificidade do

[137] Segundo LOPES, Joaquim de Seabra – O artigo…, op. cit., pág. 37. É de referir, neste contexto, que esta fórmula mais ampla foi consagrada para melhor adaptar o art. 35.º, n.º 1, da C.R.P. ao art. 13.º, n.º 1, da Diretiva 95/46/CE, o qual previa a possibilidade de concretização de mais algumas restrições ao direito de acesso, designadamente: no caso de medidas necessárias em matéria de segurança do Estado, defesa, segurança pública, prevenção, investigação, deteção e repressão de infrações penais e de violações da deontologia das profissões regulamentadas, de um interesse económico ou financeiro importante de um Estado-Membro ou da União Europeia, de missões de controlo, de inspeção ou de regulamentação associadas, ainda que ocasionalmente, ao exercício da autoridade pública, ou ainda de proteção da própria pessoa titular dos dados ou dos direitos e liberdades de outrem. Ibidem, pág. 37.

[138] LOPES, Joaquim de Seabra – O artigo…, op. cit., pág. 38

[139] ibidem, pag.43

[140] Cf. LOPES, Joaquim de Seabra – O artigo..., op. cit., pág. 43

[141] In Privacy e Protecção de Dados Pessoais…, op. cit., pág. 778

disposto no artigo 1º, da CRP, ao consagrar a dignidade humana como um "valor fundamental", bem como, o descrito no artigo 2º, da CRP, relacionado com a proteção e garantia do respeito e efetivação dos diretos e liberdades fundamentais.

A este aspeto, relaciona-se com dois direitos fundamentais, como o «direito ao livre desenvolvimento da personalidade» e o «direito à reserva da intimidade da vida privada e familiar», previstos no art. 26.º, n.º 1, da CRP.

A tutela dos direitos fundamentais e máxime de direitos, liberdades e garantias faz-se essencialmente, contra os atos dos poderes públicos, e que traduzem o exercício de funções próprias do Estado, seja o nível legislativo, executivo e judicial[142].

Da mesma forma, os direitos, Liberdades e garantias são objetivos de concretização e imperativos de respeito exigíveis às entidades públicas, e a todas as entidades investidas em poderes de autoridade pública, sob forma privada (artigo 18.º, nº 1, 2ª parte, CRP).

Segundo Vieira de Andrade, estes direitos "visam a imposição judicial, em regra dirigida à Administração, da adoção de comportamentos (em sentido amplo, em que se englobam ações e omissões, operações materiais ou simples atos jurídicos), e também, no caso de intimação para proteção de direitos, liberdades e garantias, para a prática de atos administrativos". De facto, é um imperativo de urgência na resolução de determinada situação que leva a que estes processos, que normalmente seguiriam a forma de ação administrativa comum ou ação administrativa especial (no caso de condenação à prática de ato administrativo), corram numa tramitação especial simplificada.

E, ainda, segundo o Código de Processo nos Tribunais Administrativos no título VI, capítulo II, secção II, trata a "intimação para a proteção dos direitos, liberdades e garantias" e, de igual forma, o artigo 109º, nº 1, Código de Processo nos Tribunais Administrativos, consagra que a "*a intimação para proteção de direitos, liberdades e*

[142] Partindo da bipartição clássica entre direitos, liberdades e garantias e direitos económicos, sociais e culturais que a nossa Constituição acolhe, nota-se que a tutela jurisdicional incide sobre os primeiros, em razão da não exequibilidade imediata dos segundos (dada a interdependência entre a concretização dos direitos económicos, sociais e culturais e os condicionalismos económico-financeiros).

garantias pode ser requerida quando a célere emissão de uma decisão de mérito que imponha à Administração a adoção de uma conduta positiva ou negativa se revele indispensável para assegurar o exercício, em tempo útil, de um direito, liberdade ou garantia, por não ser possível ou suficiente, nas circunstâncias do caso, o decretamento provisório de uma providência cautelar, segundo o disposto no artigo 131º".

O primeiro pressuposto que surge no artigo 109/1 Código de Processo nos Tribunais Administrativos diz respeito à urgência da pronúncia de uma decisão de mérito, que discipline de forma definitiva uma determinada situação, de forma a evitar a lesão ou inutilização de um direito. Sem esta urgência, que resulta da absoluta necessidade de tutelar um direito que é alvo de uma ofensa ou que está na iminência de ser ofendido, deve haver lugar a uma ação administrativa comum ou especial – os meios normais de defesa de direitos fundamentais. A referida urgência tem um carácter relativo, na medida em que depende dos concretos vetores factuais em causa, dobrados por um critério composto que compreende considerações temporais de "iminência" e juízos de valor. Como tal, está em causa uma ponderação de existência de perigo de lesão séria ou lesão iminente dos direitos do particular, ponderação que determinará, ou não, a absoluta necessidade de recorrência a uma tutela urgente definitiva.

Deste modo, a legitimidade ativa atribui-se aos direitos, liberdades e garantias enquanto titulares de posições jurídicas subjetivas. Segundo Vieira de Andrade, existe a possibilidade de se recorrer a ação popular, exemplo em matéria de ambiente, desde que estejam em causa algumas dimensões subjetivas e não somente os interesses de fruição de bens coletivos e, que corresponda a disponibilidade legítima dos direitos dos titulares. Por seu turno, Carla Amado Gomes segue a orientação em contrário e exclui a admissibilidade desta ação[143].

Quanto à legitimidade passiva, ela pertence à pessoa coletiva ou Ministério responsável, devendo, sempre que possível, identificar-se a autoridade concretamente competente para que esta possa ser diretamente citada e intimada[144].

[143]ANDRADE, José Carlos Vieira de. (2009). *A Justiça Administrativa (Lições*). 10ªedição. Almedina; Coimbra. P. 275 ss.;

[144] GOMES, Carla Amado. *Intimação para protecção de direitos, liberdades e garantias*. Revista do Ministério Público. Ano 26; Nº104; 1005;

Por outro lado, não há direitos, liberdades e garantias que sejam ilimitados, isto é, os direitos são limitados logo ao nível do sistema social, são limitados porque constituem partes de um subsistema normativo, são limitados pela interatividade entre as respetivas normas de garantia e são limitados porque não há possibilidade de realizar simultaneamente todos os direitos de todos os titulares[145].

Não são limitados na sua dimensão subjetiva, porque os preceitos constitucionais não remetem para o arbítrio do titular a determinação do âmbito e do grau de satisfação do respetivo interesse. Também não o são enquanto valores constitucionais, visto que a comunidade não se limita a reconhecer o valor da liberdade: liga os direitos a uma ideia de responsabilidade social e integra-os no conjunto dos valores comunitários.

Por fim, temos de ter em conta que os direitos fundamentais, podem sofrer inúmeras formas de compressão e múltiplas modalidades de afetação[146], sendo que os limites impostos ao exercício dos direitos fundamentais se encontram relacionados com conflitos práticos entre valores legitimamente consagrados.

A natureza dos direitos de personalidade e o facto de serem inatos e essenciais à realização da pessoa, tem como resultado as características que os singularizam, nomeadamente, a intransmissibilidade, a indisponibilidade, irrenunciabilidade, inexpropriabilidade, imprescritibilidade e vitaliciedade[147]. A sua integração na Constituição teve como consequência, a existência de maior visibilidade, não subsumiu nos direitos fundamentais[148].

Assim, na perspetiva do direito constitucional existe um conjunto de direitos fundamentais[149] e na perspetiva de direito civil, estes constituem o conjunto de direitos inatos da pessoa.

---

[145] *Idem*, p. 118. O autor denomina este como o postulado da relatividade.

[146] *Idem*, p. 118. O autor denomina este como o postulado da mobilidade

[147] VASCONCELOS, Pedro Pais de. Direito de Personalidade. Coimbra: Almedina, 2006, p.30

[148] CANOTILHO, J. J. Gomes. Civilização do Direito Constitucional ou Constitucionalização do Direito Civil A eficácia dos direitos fundamentais na ordem jurídico-civil no contexto do direito pós-moderno.

[149] Os direitos fundamentais do Homem, representam situações que são reconhecidas juridicamente, sem as quais o homem é incapaz de alcançar a sua própria realização e desenvolvimento.

Os direitos fundamentais[150] são designados de direitos que dizem respeito ao conceito de pessoa, com os seus direitos básicos, ou através das relações com o Estado, como direitos essenciais do cidadão. É visível, a sua relação com as filosofias políticas, sociais e económicas. Os direitos fundamentais são direitos naturais e originários, provêm da ordem jurídica através da Constituição de Weimar.

A estrutura dos direitos fundamentais, como direitos subjetivos, expetativos, de interesse jurídico, resulta da formulação das normas constitucionais. Ao nível da disposição central sobre os direitos fundamentais, o artigo 8º descreve um conjunto de direitos do individuo em sociedade, direitos de liberdade, direito à vida (nº1), e integridade moral (nº2).

No Direito Constitucional Português a regulação dos direitos fundamentais é contextualizada através de algumas perspetivas funcionais, dando um importante campo de utilidade prática, para: Esclarecer o conteúdo e o objeto dos direitos fundamentais, acomodar o respetivo exercício tornando-o efetivo, prevenir situações de abuso de exercício e, enquanto estabelece os seus limites internos e evita situações de colisão com outros direitos.

Desta forma, a regulação dos direitos fundamentais é da responsabilidade do próprio texto constitucional. A intervenção ao nível normativo e constitucional dos direitos fundamentais, cumpre diferenciar entre as intervenções legislativas que atuam no plano das leis reforçadas.

No contexto de sociedade, a conduta social é uma organização que pela sua complexidade, se pode dividir noutras ordens normativas como na ordem moral, religiosa, jurídica, etc.

---

[150] Citem-se, entre tantos, PAOLO BARILE, Ilsogetto privato nella Costituzione Italiana, Pádua, 1953; a obra colectiva Die Grundrechte, Berlim, 1954-1966; PHILIPPE BRAUD, La notion de liberté en droit public français, Paris, 1968; THOMAS M. FRANCK, Comparative Constitutional Process — Cases and Materials — Fundamental Rights in the Common Law Nations, Londres, 1968; CASTAN TOBEÑAS, Los derechos del hombre, Madrid, 1969. Em Portugal, o único estudo dogmático dos direitos fundamentais é o de MIGUEL GALVÃO TELES, Direito Constitucional Português — Sumários Desenvolvidos, policopiados, 1969-70, págs. 108 e seguintes.

É pois pertinente que os termos de consagração dos direitos fundamentais representem a intervenção normativa seguinte, a qual pode assumir duas configurações[151]: a Regulamentação dos direitos fundamentais, pois quando a intervenção normativa não se assume como necessária, e a Concretização dos direitos fundamentais, isto porque, quando a intervenção normativa permite o exercício e delimitação dos contornos. Assim sendo, os direitos da personalidade são essencialmente constituídos por três elementos: psíquicos, físicos e morais, protegendo a convivência do ser humano em sociedade, e igualmente, os aspetos internos da personalidade. Estes direitos de personalidade não apresentam conteúdo económico, e não são descartáveis[152].

Este direito de proteção de dados pessoais reveste a natureza de ser um "direito complexo", constituído por um conjunto de direitos distintos em matéria de defesa dos cidadãos, como o direito de acesso, o direito de retificação, o direito de atualização, o direito à informação, o direito à proibição de tratamento de dados sensíveis, o direito à não difusão dos dados, o direito à proibição do número nacional único e o direito de acesso às redes informáticas de uso público[153].

Segundo citação feita por José Alexandrino os limites são normas que, de forma duradoura, excluem diretamente âmbitos ou efeitos de proteção ou que são fundamento suscetível de afetar as possibilidades de realização de normas jusfundamentais[154].

Isto significa que os limites tanto podem ser impostos de forma direta como indiretamente. Os limites não derivam apenas de situações de conflito entre os diferentes valores que representam as diversas facetas e dignidade humana, mas também

[151] JORGE BACELAR GOUVEIA: Os direitos fundamentais atípicos, Lisboa, 1995; O estado de exceção no Direito Constitucional – entre a eficiência e a normatividade das estruturas de defesa extraordinária da Constituição, I e II, Coimbra, 1998; Estudos de Direito Público, I, Cascais, 2000

[152] ALVAREZ, Tomás Prieto. La dignidade de la persona. Cizur Menor (Navarra).Espanha: Thomson-Civitas, 2005.

[153] Nos mesmos termos, ver PINHEIRO, Alexandre Sousa – Privacy e Protecção de Dados Pessoais…, op. cit., págs. 771 e 827

[154] *Idem*, p.122.

de situações de imposições legais próprias da vida em sociedade: a ordem pública, a ética ou moral social, a autoridade do Estado, a segurança nacional entre outros[155].

Segundo Alexandrino as situações quando qualificadas como limites dos direitos fundamentais podem assumir duas "feições básicas": ou correspondem a fronteiras que assinalam normativamente âmbitos não concluídos no objeto ou no conteúdo do direito ou correspondem a normas constitucionais que constituem fundamento para operações de delimitação do direito ou para posteriores restrições.[156]

Os limites impostos ao exercício dos direitos fundamentais podem consistir na imposição de regras ou princípios, podem ser normas gerais ou individuais, normas constitucionais ou infraconstitucionais, podem ser limites constitucionais diretos ou indiretos e podem estar referidos a cláusulas explícitas ou a uma cláusula implícita.

Na verdade, estes limites ou limitações constitucionais dos direitos fundamentais, podem partir desde logo através de imposições legislativas, quando o preceito constitucional não tenha previsto qualquer restrição para um determinado direito ou se torne necessário ir além das restrições legislativas e também naquelas hipóteses em que a CRP preveja direitos ou valores que são estruturalmente incompatíveis.

Estes limites surgem igualmente nos casos concretos ao nível da aplicação do direito, nomeadamente nos Tribunais. Aqui, por vezes é necessário conciliar preceitos constitucionais diretamente aplicáveis que numa situação de fato conflituem entre si.

Por fim há ainda situações em que os limites são impostos a apenas algumas categorias de cidadãos e restrições legislativas que visem a "proteção dos cidadãos contra si próprios"[157]

---

[155] Vide neste sentido JOSÉ CARLOS VIEIRA DE ANDRADE, Os direitos fundamentais na Constituição Portuguesa de 1976, 2ªedição, Almedina, Novembro de 2001 275 e 276

[156] Vide neste sentido JOSÉ CARLOS VIEIRA DE ANDRADE, Os direitos fundamentais na Constituição Portuguesa de 1976, 2ªedição, Almedina, Novembro de 2001pag. 121

[157] ANDRADE, José Carlos Vieira de. *Os direitos fundamentais na Constituição Portuguesa de 1976*. 2ªedição, Almedina, novembro de 2001, p. 278.

O artigo 37º nº 1 da CRP impõe um limite ao exercício de expressão, determinando que "todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, pela imagem ou por qualquer outro meio (…). Isto é, limita o exercício deste direito ao próprio pensamento de cada um. Um outro limite que deriva diretamente da lei é o que é imposto relativamente ao direito de manifestação e de reunião. Determina o artigo 45º da CRP que "os cidadãos têm o direito de se reunir, pacificamente e sem armas (…) ". Ou seja, impõe o limite do exercício deste direito ao fato de ser exercício de forma pacífica e sem armas. Estes são limites diretamente impostos pela lei constitucional. Já de forma indireta a CRP impõe limites relacionados por exemplo com a dignidade da pessoa humana (art.º 1.º), com o princípio da democracia económica, social e cultural (art.º 2.º), princípio da igualdade (art.º 13.º), a normalidade constitucional e a garantia da capacidade funcional do Estado (art.º 19.º).

2.7 A qualificação jurídica das infrações previstas no RGPD

Ao nível nacional, a definição de crime e de contraordenação, com base no critério conceitual-formal e nominal, a prática de um fato declarado passível de pena através da Lei e do artigo 1º, nº 1, do Código Penal e da prática de um fato que corresponda a um tipo legal que termine numa coima de acordo com o artigo 1º, do Regime Geral das Contra Ordenações, conclui-se que no caso do artigo 83º do RGPD estamos perante as contraordenações. Pelo fato de que, é utilizada neste artigo, a expressão "coima" para classificar a ameaça de infrações.

Não obstante no artigo 84º, nº 1, do RGPD[158], existe uma sanção especial, pelo fato de que o conceito utilizado de "sanção"[159] não permite enquadrar de forma imediata todas as infrações a que corresponde os conceitos de crime ou de contraordenação. Embora, a compreensão do que está em causa tem necessariamente de passar por uma leitura associada dos artigos 58º, 83º e 84º do RGPD.

[158] Sendo certo que certas contraordenações podem não implicar a aplicação de uma coima, como sucede no art. 15.º, n.º 2, da Lei n.º 30/2000, de 29 de novembro, que aprova o regime jurídico do consumo de estupefacientes, nos termos do qual "[a]os consumidores toxicodependentes são aplicáveis sanções não pecuniárias". Sobre este tema vide VILELA, Alexandra – O Direito de Mera Ordenação Social: Entre a Ideia de "Recorrência" e a de "Erosão" do Direito Penal Clássico. Coimbra, Portugal: Coimbra Editora, 2013. Págs. 369-371.

[159] Espanha, França e Inglaterra consideram que se trata de infrações e multas administrativas

Assim, no artigo 83º, nº 4, 5 e 6, estão consagrados os atos suscetíveis de conduzir à aplicação de uma coima, ou seja, as próprias obrigações do responsável pelo tratamento e do subcontratante de acordo com os artigos 8º, 11º, 25º a 39º e 42º e 43º, de igual forma, as obrigações do organismo de certificação nos termos dos artigos 42º e 43º, as obrigações do organismo da supervisão de acordo com o artigo 41º, nº 4, os princípios básicos do tratamento, incluindo as condições de consentimento de acordo com os artigos 5º, 6º, 7º e 9º. Bem como, as transferências de dados pessoais para um país terceiro ou uma organização internacional de acordo com os artigos 44º a 49º.

No artigo 84º está descrito que, "os Estados-Membros estabelecem as regras relativas às outras sanções aplicáveis em caso de violação do disposto no presente regulamento, nomeadamente às violações que não são sujeitas a coimas nos termos do artigo 7983.º, e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas"[160].

Estes aspetos identificam uma indefinição, porque algumas vezes podem conduzir a discrepâncias no tratamento jurídico das mesmas situações de acordo com o Estado-Membro em causa, necessárias para adequar aos diversos ordenamentos jurídicos nacionais.

Num entendimento mais pormenorizado o objetivo do artigo 84º não está presente noutro artigo deste ato legislativo, mas sim nos considerandos particularmente o considerando 148 e 149, sendo que a epigrafe do reforço da execução das regras do RGPD, introduz a obrigação da imposição de "sanções incluindo as coimas, por violação do presente regulamento, além da substituição das medidas adequadas que venham a ser impostas pela autoridade de controlo de acordo com presente regulamento".

E no considerando 149 refere que os "Estados-Membros deverão poder definir as normas relativas às sanções penais aplicáveis por violação do presente regulamento,

[160] Na redação portuguesa do RGPD menciona-se o artigo 7983.º. Estamos perante um lapso não corrigido na 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, de 23 de maio de 2018. A versão inglesa, francesa, espanhola e alemã, para citar algumas, em lugar do (suposto) artigo 7983.º, remetem para o artigo 83.º do RGPD.

inclusive por violação das normas nacionais adotadas em conformidade com o presente regulamento".

Para além destes pressupostos, o considerando 152 determina que "Sempre que o presente regulamento não harmonize sanções administrativas, ou se necessário noutros casos, por exemplo, em caso de infrações graves às disposições do presente regulamento, os Estados-Membros deverão criar um sistema que preveja sanções efetivas, proporcionadas e dissuasivas. A natureza das sanções, penal ou administrativa, deverá ser determinada pelo direito do Estado-Membro".

Assim, mesmo que a expressão "sanções" não esteja presente no artigo 83º, este refere-se materialmente à área penal e contraordenacional. Deve-se salientar ainda que, na versão do RGPD português as duas expressões são utilizadas de forma intercambiável como se fossem semelhantes e que pode dar origem a alguma confusão. Neste caso, as expressões "sanções administrativas" e "coimas", são de grande importância para o panorama jurídico pelo fato de que a última expressão condiz com o domínio jurídico específico distinto do direito administrativo.

2.7.1 Os recetores das sanções

É através do artigo 83º do RGPD que está diferenciado o valor das coimas de acordo com seja aplicado numa organização ou particularmente. Não obstante no presente artigo, nº 4, a coima é limitada para um máximo de 10 milhões de euros, ou no caso da empresa a 2% do seu volume de negócios anual. Nos nº 5 e 6. O limite máximo da coima aumenta para 20 milhões de euros e 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado[161].

O considerando 150 teve como pretensão atenuar as possíveis dificuldades hermenêuticas, e referiu que "sempre que forem impostas coimas a empresas, estas deverão ser entendidas como empresas nos termos dos artigos 101.º e 102.º do Tratado

[161] Mário Ferreira Monte, Lineamentos de Direito das Contraordenações (Braga: AEDUM, 2014), 49–50.

sobre o Funcionamento da União Europeia para esse efeito". Embora o RGPD português beneficia de uma definição mais clara dos recetores de coimas[162].

O regulamento requer sempre uma avaliação de cada caso ao nível individual[163], ou seja, o artigo 83º, nº 2 representa a base para esta avaliação. Refere que "ao decidir sobre a aplicação de uma coima e sobre o montante da coima em cada caso individual, é tido em devida consideração o seguinte". Assim, em conformidade com o que antecede e de acordo com o considerando 148[164], a autoridade de controlo tem a responsabilidade da escolha das medidas mais adequadas.

No caso do referido no artigo 83º, nº 4 a 6, esta escolha tem como consideração todas as medidas corretivas, ou seja, implica a imposição da coima apropriada, conjugada com a medida corretiva de acordo com o artigo 58º, nº 2, ou de forma autónoma. As coimas são assim, consideradas como um instrumento fundamental utilizado pelas autoridades de controlo em determinadas circunstâncias. Neste caso concreto, as autoridades de controlo são estimuladas a adotar uma abordagem

[162] Pedro Miguel Freitas. Regulamento Geral de Proteção de Dados: uma visão portuguesa sobre o regime sancionatório. UNIO - EU LAW JOURNAL. Vol. 4, No. 2, julho 2018

[163] Para além da aplicação dos critérios constantes do artigo 83.º, existem outras disposições que reforçam a base desta abordagem, nomeadamente:
- Considerando 141 – «[a] investigação decorrente de uma reclamação deverá ser realizada, sob reserva de controlo jurisdicional, na medida adequada ao caso específico.»
- Considerando 129 – «[o]s poderes das autoridades de controlo deverão ser exercidos em conformidade com as garantias processuais adequadas previstas no direito da União e do Estado-Membro, com imparcialidade, com equidade e num prazo razoável. Em particular, cada medida deverá ser adequada, necessária e proporcionada a fim de garantir a conformidade com o presente regulamento, tendo em conta as circunstâncias de cada caso concreto [...].»
- Artigo 57.º, n.º 1, alínea f) – «tratar as reclamações apresentadas por qualquer titular de dados, ou organismo, organização ou associação nos termos do artigo 80.º, e investigar, na medida do necessário, o conteúdo da reclamação [...].»

[164] «A fim de reforçar a execução das regras do presente regulamento, deverão ser impostas sanções, incluindo coimas, por violação do presente regulamento, para além, ou em substituição, das medidas adequadas que venham a ser impostas pela autoridade de controlo nos termos do presente regulamento. Em caso de infração menor, ou se o montante da coima suscetível de ser imposta constituir um encargo desproporcionado para uma pessoa singular, pode ser feita uma repreensão em vez de ser aplicada uma coima. Importa, porém, ter em devida conta a natureza, gravidade e duração da infração, o seu caráter doloso, as medidas tomadas para atenuar os danos sofridos, o grau de responsabilidade ou eventuais infrações anteriores, 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, o cumprimento de um código de conduta ou quaisquer outros fatores agravantes ou atenuantes. A imposição de sanções, incluindo coimas, deverá estar sujeita às garantias processuais adequadas em conformidade com os princípios gerais do direito da União e a Carta, incluindo a proteção jurídica eficaz e um processo equitativo.»

equilibrada em relação à utilização das medidas corretivas, com a finalidade de assegurar a resposta à infração cometida, que seja efetiva, dissuasiva e proporcionada. O objetivo principal é não tornar as coimas como o último recurso.

O Comité Europeu para a Proteção de Dados (CEPD) quando está em conformidade com artigo 65º do RGPD lança uma decisão vinculada relacionada com os litígios entre as autoridades no que se refere, especialmente na determinação da existência de violação. E, nos casos em que se esteja presente de uma objeção pertinente que possa suscitar a conformidade da medida corretiva com o RGPD, a decisão do CEPD praticará os princípios da efetividade, proporcionalidade e dissuasão na decisão da autoridade. E, posteriormente, são apresentadas as orientações do CEPD relacionadas com a aplicação do artigo 65º, do regulamento.

2.7.2 Critérios de avaliação

O artigo 83º, nº 2, prevê um conjunto de critérios que as autoridades de controlo têm o dever de utilizar na avaliação da imposição de uma determinada coima, bem como do seu montante. Assim, trata-se uma avaliação individual que tem em conta cada caso, de acordo com o artigo 83º, nº 7[165].

Não obstante as conclusões que foram alcançadas na primeira fase de avaliação podem ser utilizadas na segunda, relacionada com o montante da coima, e por isso torna-se desnecessária uma nova avaliação com base nos mesmos critérios.

Importa referir que na natureza, a gravidade e a duração da infração, quase todas as obrigações dos responsáveis pelo tratamento de dados e os seus subcontratantes de acordo com o regulamento estão categorizadas segundo a sua natureza, no artigo 83º, nº 4 a 6. Assim, no estabelecimento dos dois montantes máximos distintos para as coimas, o regulamente determina que existem algumas disposições cuja violação pode ser mais grave do que a de outras. Embora, a autoridade de controlo, com base na avaliação dos fatos e, à luz dos critérios gerais consagrados no artigo 83º, nº 2 pode decidir que se está

[165] A avaliação da sanção a aplicar poderá ocorrer em separado, após a determinação da existência de infração por força de normas processuais nacionais decorrentes dos requisitos constitucionais de alguns países. Por conseguinte, tal pode limitar, nesses países, o conteúdo e o nível de detalhe de um projeto de decisão emitido pela autoridade de controlo principal.

perante uma necessidade adicional ou reduzida de reação através de uma medida corretiva que corresponde a uma coima. E, neste caso, será aplicado o sistema de limiares do regulamento (artigo 83º, nº 4 a 6) com o objetivo de identificação da coima máxima que pode ser imposta com base na sua natureza.

Dito de outra forma, o considerando 148 insere o conceito de "infrações menores", que podem constituir as violações de uma ou várias normas descritas no artigo 83º, nº 4 ou 5 do regulamento. Embora, a avaliação dos critérios que estão inseridos no artigo 83º, nº 2, pode conduzir a autoridade de controlo a entender que a violação não constitui um risco significativo para os direitos dos titulares dos dados, e que não afeta ainda, a essência desta obrigação. Neste contexto, a coima pode ser apenas substituída por uma repreensão.

O considerando 148 não institui a obrigação da autoridade de controlo a substituir de forma invariável a coima por uma repreensão em caso de se tratar de uma infração menor, mas apenas como uma probabilidade na sequência da avaliação específica de todas as circunstâncias do caso.

O próprio regulamento não atribui às infrações distintas um valor específico, mas sim um limite, que pode corresponder a um grau de gravidade menor de uma violação das obrigações enunciadas no artigo 83º, nº 4, relacionadas com o nº 5 do mesmo artigo. A reação efetiva, proporcionada e dissuasiva a uma violação do artigo 83.º, n.º 5, dependerá, contudo, das circunstâncias do caso.

Assim, as violações que já tenham sido objeto de uma ordem emitida pela autoridade de controlo, em que o responsável pelo tratamento ou o subcontratante não tiveram cumprido (artigo 83º, nº 6)[166], as disposições do direito nacional podem ter impacto forte nesta avaliação[167].

[166] A aplicação do artigo 83.º, n.º 6, deve forçosamente ter em conta o direito processual nacional. O direito nacional determina o modo de emissão e notificação das ordens, assim como o momento a partir do qual produzem efeitos, e se existe, ou não, um período de tolerância para fins de cumprimento. Deve ser tido em consideração, entre outros, o efeito de um recurso sobre o caráter executivo da ordem.

[167] As disposições legais em matéria de prescrição podem levar a que uma ordem emitida pela autoridade de controlo deixe de ser tida em consideração em virtude do período decorrido desde a emissão da mesma. Em alguns países existem normas que determinam que, decorrido o prazo de prescrição da

A natureza da infração, bem como "o âmbito ou o objetivo do tratamento de dados em causa, e o número de titulares dos dados afetados e o nível de danos por eles sofridos", poderão revelar a gravidade da infração.

O cerne da questão corresponde ao facto de que a ocorrência de diversas infrações diferentes que são cometidas em conjunto em qualquer caso específico, significa que a autoridade de controlo poderá aplicar as coimas de forma mais efetiva, proporcionada e dissuasiva, no limite aplicável à infração mais grave. E, assim, se tratar de uma infração nos termos dos artigos 8º e 12º, a autoridade de controlo pode aplicar as medidas corretivas que fazem parte do artigo 83º, nº 5.

O número de titulares de dados deve ser avaliado, com a finalidade de identificar se trata de um evento isolado ou se identifica uma violação sistémica, ou falta de rotinas adequadas. Na fase anterior não está implicado que os eventos isolados não sejam alvo de medidas, isto porque podem afetar um número elevado de titulares de dados. Importa referir que, a relevância deste número de titulares está relacionada com o número de inscritos na base de dados, o número de utilizadores de um serviço, o número de clientes ou a população do país, conforme o caso.

Neste contexto, o objetivo do tratamento de dados deve ser igualmente avaliado, o parecer G29 relacionado com a "limitação da finalidade"[168], analisou os dois elementos centrais de base deste princípio de proteção de dados, como a especificação da finalidade e utilização compatível. Ao ser efetuada a avaliação da finalidade do tratamento de dados de acordo com o artigo 83º, nº 2, as autoridades de controlo devem analisar em que medida este tratamento respeita os dois princípios chave[169].

---

ordem, não pode ser imposta qualquer coima pelo seu incumprimento nos termos do artigo 83.º, n.º 6. Incumbirá às autoridades de controlo de cada país determinar os efeitos nacionais de uma situação deste tipo.

[168] WP 203, Parecer 03/2013 sobre a limitação da finalidade, disponível em: http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf .

[169] Cf. também WP 217, Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento nos termos do artigo 7.º, pág. 24, no que se refere à questão: «O que torna um interesse 'legítimo' ou 'ilegítimo'?»

No caso em que os titulares de dados tenham sofrido danos, o seu nível tem de ser tomado em conta, podendo o tratamento de dados gerar riscos para os direitos e liberdades das pessoas, de acordo com o considerando 75, que descreve que:

"O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial: quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos significativos de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou dados relativos à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados".

De uma forma geral, a "intenção" corresponde ao conhecimento como vontade em relação às características da violação, e a "negligência" refere que não há intenção de provocar a infração, mesmo no caso em que o responsável pelo tratamento e o subcontratante tenham violado o dever de diligência exigido na lei. É reconhecido que as violações intencionais que correspondem ao incumprimento da lei são consideradas mais graves do que as negligentes e, por esta razão, mais suscetíveis de justificar a aplicação de uma coima.

A jurisprudência e a prática relativas ao domínio da proteção de dados no âmbito da aplicação do regulamento fornecem elementos claros na apreciação da intencionalidade da violação. Como exemplo, a massificação das situações em diversas

localidades, possibilita a liberdade de circulação de pessoas e bens, e permite aos indivíduos obter, manter e gerir rendimentos à margem dos sistemas fiscais dos estados de residência.

No acórdão com o processo nº 00001/17. BCPRT do Tribunal Central Administrativo Norte, de 14/07/2017, a entidade veio invocar incompetência do TCAN para decidir, em primeira instância o presente litígio fundamentando a sua posição na decisão na jurisprudência tirada no Acórdão do TCA Sul proc. n.º 04827/09 de 07-05-2009, que refere: a competência para conhecer dos recursos contenciosos de anulação dos atos da Comissão Nacional da Proteção de Dados, a par da competência para conhecer de todos os outros recursos dessa natureza, a que se referia o artigo 40º, al. b) do anterior Estatutos dos Tribunais Administrativos e Fiscais.

"De acordo com o artigo 23º, n.º 3, da Lei de Proteção de Dados Pessoais (LPDP) aprovada pela Lei nº 67/98, de 26 de outubro "3 - No exercício das suas funções, a CNPD profere decisões com força obrigatória, passíveis de reclamação e de recurso para o Tribunal Central Administrativo". Ou seja, quando da transposição para a ordem jurídica interna da Diretiva n.º 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, através da Lei 67/98, de 26 de Outubro, ficou consagrado que das decisões da Comissão Nacional de Proteção de Dados cabia recurso para o Tribunal Central Administrativo"[170].

Por outro lado, os responsáveis pelo tratamento de dados e os subcontratantes são obrigados a aplicar as medidas técnicas e organizativas que possam garantir um nível de segurança apropriado ao risco inerente, e realizar as avaliações do impacto em matéria de proteção de dados, bem como reduzir os riscos para os direitos e liberdades das pessoas decorrentes do tratamento de dados pessoais. Embora, sempre que estejam presentes uma violação e a ocorrência de danos do titular dos dados, a parte responsável deve esforçar-se por limitar as consequências da respetiva violação.

[170] acórdão com o processo nº 00001/17. BCPRT do Tribunal Central Administrativo Norte, de 14/07/2017, disponível em: http://www.dgsi.pt/jtcn.nsf/89d1c0288c2dd49c802575c8003279c7/2d62be6b1ae49e55802581d1003a1f44?OpenDocument&Highlight=0,Protec%C3%A7%C3%A3o,dados,pessoais

No âmbito do controlo da Diretiva 95/46/CE e na sua experiência reguladora das autoridades de controlo, pode ser apropriado a conceção de um determinado grau de flexibilidade aos responsáveis pelo tratamento de dados, bem como ao subcontratante que assumem a responsabilidade pela correção ou limitação dos efeitos dos seus próprios atos. Como exemplo, através do contato com outros responsáveis pelo tratamento dos dados que estivessem envolvidos numa parte ou totalmente no tratamento e, na partilha indevida de dados para terceiros.

A este aspeto, o RGPD introduziu um nível mais elevado de responsabilidade do responsável pelo tratamento de dados em comparação com a Diretiva 95/46/CE, relacionada com a proteção de dados. Assim, o grau de responsabilidade do responsável pelo tratamento ou o subcontratante avaliado com a finalidade de aplicação das medidas corretivas adequadas, pode incluir um conjunto de aspetos, ou seja, o responsável pelo tratamento aplica medidas técnicas e organizativas que se relacionem com os princípios da proteção de dados desde a conceção e por defeito (artigo 25º), e aplica um nível adequado de segurança (artigo 32º).

De igual modo, o grau de cooperação com a autoridade de controlo com o objetivo de recuperar a infração e atenuar os seus efeitos negativos, o artigo 83º, nº 2, estabelece que o grau de cooperação pode ter em atenção a "devida consideração" no caso em que decida impor uma coima e, ao mesmo tempo, determinar o seu montante.

2.8 A emergência da regulação do risco no tratamento da proteção de dados

A Diretiva de Proteção de Dados da UE 95/46/CE exige que as medidas de segurança devem "garantir um nível de segurança adequado aos riscos representados pelo processamento e natureza dos dados a serem protegidos" (artigo 17º) e, que as operações de processamento suscetíveis de apresentar riscos específicos para os direitos e liberdades dos titulares dos dados sejam sujeitos a uma verificação pelos Estados-Membros (artigo 12º).

De igual forma, os dados pessoais podem ser processados quando "necessário para os fins do interesse legítimo perseguido pelo controlador ou pelo terceiro parte ou partes a quem os dados são divulgados, exceto onde tais interesses são anulados pelos interesses dos direitos e liberdades fundamentais dos titulares dos dados" (artigo 7º).

O RGPD foca-se essencialmente na gestão de riscos, e o texto que emergiu do Parlamento Europeu determina a necessidade de "o controlador ou o processador deve avaliar os riscos inerentes ao processamento e implementar as medidas para reduzir os riscos"[171]. O projeto de regulamento exige assim, que os controladores de dados demonstrem conformidade com este, tendo em consideração os "riscos para os direitos e liberdades do titular de dados"[172].

Nas diversas circunstâncias, o controlador tem a obrigação de "realizar uma análise de risco do impacto potencial do processamento de dados pretendido sobre os direitos e liberdades dos titulares dos dados, avaliando se as suas operações de processamento têm probabilidade de apresentar riscos específicos"[173].

Existem ainda, outros exemplos recentes relacionados com o novo destaque dado à gestão de riscos, ou seja, no ano de 2013, o Conselho de Ministros da OCDE reviu as diretrizes que regem a proteção da privacidade e os fluxos transfronteiriços de dados pessoais, adotadas pela primeira vez em 1980, e para implementar uma abordagem baseada no risco[174].

Ou seja, no memorando explicativo, os redatores observaram a "importância da avaliação de risco no desenvolvimento de políticas e salvaguardas para proteger a privacidade". E, a este aspeto, tem existido uma série de relatórios do governo sobre a gestão de riscos na proteção de dados[175].

The *French Commission Nationale de l'informatique et des Liberte´s* (CNIL) liderou o caminho com a sua Metodologia para Gestão de Risco de Privacidade, revista

[171] Article 29 Data Protection Working Party, Opinion 03/2014 on Personal Data Breach Notification, 693/14/EN WP 213 (2014), 4.
[172] Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN, WP218 (2014), 2.
[173] European Parliament Resolution of 12 March 2014 on the 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, P7 TA (2014)0212, 12 March 2014, } 66.
[174] Organization for Economic Co-operation and Development, Supplementary Explanatory memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013), 30.
[175] Organization for Economic Co-operation and Development, OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, C(80)58/FINAL, as amended by C92013)79 (2013), 12.

mais recentemente em 2012, que "descreve um método de gestão dos riscos que o processamento de dados pessoais pode gerar para os indivíduos"[176].

A Comissão Federal de Comércio dos EUA em 2012 publicou um relatório que recomendou que as empresas devem "implementar mecanismos de responsabilidade e conduzir avaliações de ricos de privacidade para garantir que as questões de privacidade sejam abordadas por todos"[177].

Posteriormente, no ano de 2013, o Gabinete do Comissário de Informação do Reino Unido publicou um relatório exaustivo sobre avaliação de impacto de privacidade e Gestão de Riscos. Preparado por Trilateral Research & Consultoria[178], o relatório reflete um esforço para promover um melhor 'ajuste' entre o PIA (Avaliação de impacto de privacidade) e os "padrões de gestão de risco e metodologias"[179].

A ICO (Information Comissioner's office) publicou um Código de Conduta abrangente da PIA em fevereiro de 2014, que fornece às organizações a orientação passo a passo sobre como conduzir a PIA e aconselha-os a considerar a privacidade e riscos relacionados para os indivíduos.

Por fim, o CNIL refere que "usar um método de gestão de risco é a maneira mais segura para garantir a objetividade e relevância das escolhas a fazer ao configurar um tratamento de dados pessoais".

A gestão de risco pode priorizar o investimento de recursos escassos em proteger a privacidade e fazer cumprir as obrigações de privacidade, pode identificar sérios riscos à privacidade e nas medidas para reduzi-los. Não obstante a regulamentação da gestão de risco deve evitar as avaliações de risco desnecessárias ou duplicadas. O regulamento de proteção de dados prevê que "avaliação única deve ser suficiente para

[176] Commission Nationale de l'informatique et des Liberte´s, Methodology for Privacy Risk Management (2012), 4.
[177] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change (2012), 30.
[178] Trilateral Research & Consulting, Privacy Impact Assessment and Risk Management (2013), 15–16
[179] National Institute of Standards and Technology, NIST Privacy Engineering Objectives and Risk Model Discussion Draft (2014), 3.

abordar um conjunto de operações de processamento semelhantes que apresentam riscos semelhantes"[180].

É importante que os instrumentos de gestão de risco de proteção de dados correspondam às metodologias e programas de gestão de risco já existentes, para que seja permitido benefícios da experiência desenvolvida noutras áreas, como aproveitamento dos recursos já utilizados.

2.9 O Encarregado de Proteção de Dados na Administração Pública

O RGPD consagra no seu artigo 37º, nº 1, a nomeação obrigatória de um EPD para as autoridades e organismos públicos, não incluindo os tribunais e na sua função jurisdicional. Assim, de acordo com o mesmo artigo, nº 3, está em causa um organismo público o qual só poderá existir um unido EPD, para várias dessas autoridades e organismos, tendo em conta a respetiva estrutura organizacional e dimensão".

De igual modo, no artigo 37º, do RGPD está traçado o perfil do EPD que deve conter conhecimentos especializados de direito, principalmente no que se relaciona com a proteção de dados, e de acordo com o artigo 39º, na capacidade para o desempenho das funções que estão confiadas.

De acordo com o considerando 7 do RGPD existe a referência à necessidade de reforçar a segurança jurídica e prática para as autoridades públicas para as pessoas singulares e operadores económicos[181].

2.10 A responsabilidade civil que decorre da violação do RGPD

De acordo com o artigo 79.º e Considerandos 145 e 147, do RGPD, permite-se que todos os titulares dos dados tenham o direito de recorrer à via judicial no caso em que estes considerem ter existido uma violação dos direitos que lhes assistem de acordo com o regulamento, e que essa violação resulte do tratamento dos seus dados pessoais efetuados em violação do regulamento.

---

[180] Draft EU General Data Protection Regulation (unofficial consolidated version after LIBE Committee vote), at art 33, } 1.

[181] CALVÃO, Filipa – " O modelo de supervisão de tratamentos de dados pessoais na União Europeia: Da atual Diretiva ao futuro Regulamento", Revista Fórum de Proteção de Dados, n.º 1, julho de 2015, p. 42

Este meio de tutela dos direitos dos titulares de dados pessoais não inclui o recurso a outros meios legalmente previstos[182], pois está estabelecido no artigo 82º, do RGPD[183] que qualquer pessoa que tenha sofrido danos, materiais ou imateriais devido a uma violação do regulamento, tenha o direito de receber uma indemnização do responsável pelo tratamento ou pelo subcontratante pelos danos sofridos.

Importa por isso, referir que a responsabilidade do responsável do tratamento de dados ocorre no caso em que este esteja envolvido no tratamento de dados, e a responsabilidade do subcontratado só terá lugar nos casos em que este cumpra as obrigações que decorrem do regulamento[184], ou no caso em que não tiver seguido as instruções licitas que foram fornecidas pelo responsável pelo tratamento.

Por outro lado, sempre que estejam envolvidos mais do que um responsável pelo tratamento civilmente responsáveis de acordo com o regulamento ocorre a regra da solidariedade. Nas palavras de JOSÉ PROENÇA[185], o regime da solidariedade que resulta dos termos do RGPD determina, no âmbito das obrigações, uma inversão de regra da parciaridade ou conjunção, presente no Código Civil Português, na área que cada devedor responde pelas suas obrigações. E, que se intitula a solidariedade quando existe a vontade das partes[186].

Importa referir que nas palavras de NUNO PINTO OLIVEIRA[187], a solidariedade passiva, no âmbito da teoria geral das obrigações tem como consequência

---

[182] Conforme resulta do corpo da norma, "sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, nomeadamente o direito de apresentar relação a uma autoridade de controlo". No mesmo sentido, vd. Alexandre Sousa Pinheiro et. al., Comentário ao Regulamento Geral de Proteção de Dados (Coimbra, Almedina, 2018), 629, "o direito de ação, judicial […] não preclude o recurso às vias administrativas, maxime a reclamação perante uma autoridade de controlo […], nem é prejudicado pelo facto de estas terem sido utilizadas"

[183] 3Cfr. Considerando 146 do RGPD

[184] Deve-se entender as obrigações do RGPD que lhe são especificamente dirigidas, nos termos do artigo 28.º

[185] Cfr. José Carlos Brandão Proença, Lições de Cumprimento e Não Cumprimento das Obrigações (Coimbra: Coimbra Editora, 2011), 105.

[186] Cfr. artigo 513.º do Código Civil. Neste sentido, vd. Nuno Manuel Pinto Oliveira, Princípios de Direito dos Contratos (Coimbra: Coimbra Editora, 2011), 72, "[e]m regra – se a lei ou o negócio jurídico nada disserem – a obrigações é parciária; excecionalmente – se a lei ou o negócio jurídico o disserem – a obrigação plural é solidária."

[187] Cfr. Oliveira, Princípios de Direito, 70 e segs.; e ainda Proença, Lições de Cumprimento, 109. Visto que o estudo em causa deslinda-se pela análise da responsabilidade civil aplicada em caso de violação dos princípios constantes no RGPD, faz-se necessário ressaltar que a posição tradicional do credor, no âmbito

a possibilidade de o credor exigir, judicial ou extrajudicialmente, a prestação integral ou parcial de cada um dos devedores solidários.

Pode-se referir que o Direito das Obrigações corresponde ao Direito dos particulares. É através do artigo 405º do Código Civil que está descrito esta liberdade contratual, sendo o conteúdo da prestação, dentro dos limites impostos por lei. Existe, no entanto, uma vinculação à juridicidade. Qualquer obrigação, de fonte contratual ou legal, tem de ser cumprida pela parte devedora, para que a obrigação se extinga. Surgem, em alguns casos, litígios quando o credor considera incumprido a sua pretensão contra o devedor.

De acordo com o que está referido no artigo 762º, do nº 1 do Código Civil, o devedor cumpre a obrigação quando realiza a prestação a que está vinculado. O cumprimento das obrigações obedece a três princípios gerais que se referenciam na lei, através do princípio da pontualidade, integralidade e boa-fé.

O princípio da pontualidade está consagrado no artigo 406º, nº 1 do Código Civil, que determina que o contrato deve ser cumprido pontualmente, e só pode modificar-se ou extinguir-se por mútuo consentimento dos contraentes ou nos casos admitidos por lei. O princípio da pontualidade resulta da irrelevância da situação económica do devedor, e por esta razão, o devedor não pode com este fundamento, solicitar a redução da sua prestação ou obtenção de outro benefício[188].

O princípio da integralidade está expresso no artigo 763º, nº 1 do CC e descreve que o devedor deve realizar a prestação de uma só vez, ainda que se trate de prestação divisível. Se o devedor oferecer somente uma parte da prestação, o credor pode recusar o seu recebimento sem incorrer em mora. A própria lei admite que o credor decida exigir somente uma parte da prestação.

---

direito civil, é aqui compreendida como sendo o titular do direito violado, ao passo que a posição do devedor, corresponde ao responsável pelo tratamento ou subcontratado civilmente responsáveis nos termos do regulamento, que têm ao seu encargo a incumbência de zelar pela proteção e não disponibilização dos dados em causa

[188] Manuel A. Domingues de Andrade, Teoria Geral das Obrigações, com a colaboração de Rui de Alarcão, Coimbra 1966

No caso do princípio da boa-fé, pode-se salientar que está expresso no artigo 762º, nº 2 do CC. O que resulta que, para se considerar o verificado, o cumprimento da obrigação não é suficiente a realização da prestação devida em termos formais, sendo antes necessário o respeito dos ditames de boa-fé, seja por parte de quem executa ou por parte de quem exige a obrigação. São parte destes deveres, o dever da proteção, informação e lealdade[189].

[189] Luís Manuel Teles de Menezes Leitão, Direito das obrigações, volume II, Transmissão e extinção das obrigações, não cumprimento e garantias de crédito, 3.a edição, Coimbra 2005

Conclusão

Temos então que o Encarregado da Proteção de Dados é uma figura central no Novo Regulamento Geral da Proteção de Dados.

O EPD auxilia o responsável pelo tratamento ou o subcontratante em todas as questões relacionadas com a proteção de dados pessoais. O EPD deve, concretamente: informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os seus trabalhadores, sobre as respetivas obrigações nos termos da lei da proteção de dados; controlar o cumprimento, por parte da organização, de toda a legislação relacionada com a proteção de dados, nomeadamente em auditorias, atividades de sensibilização e formação do pessoal implicado nas operações de tratamento; prestar aconselhamento sempre que tenha sido realizada uma AIPD e controlar a sua realização; atuar como ponto de contacto para pedidos de pessoas relativamente ao tratamento dos seus dados pessoais e ao exercício dos seus direitos; cooperar com as Autoridades da Proteção de Dados e atuar como ponto de contacto das mesmas sobre questões relacionadas com o tratamento.

A organização tem de envolver o EPD nas suas atividades em tempo útil. O EPD não deve receber instruções do responsável pelo tratamento nem do subcontratante relativamente ao exercício das suas funções. O EPD responde diretamente perante o nível mais elevado de administração da organização.

As organizações devem, deste modo, confirmar se é ou não obrigatório nomear um EPD, e caso não seja obrigatório, devem na mesma ponderar a contratação de um EPD, mesmo que seja a título de prestação de serviços, com o objetivo de respeitar escrupulosamente o RGPD.

A figura do Encarregado da Proteção de Dados (EPD) aparece, com uma enorme relevância, no novo Regulamento Geral da Proteção de Dados (RGPD). Os EPD, que terão de ser designados, em algumas situações, pelos responsáveis de dados e subcontratantes, têm funções centrais neste novo quadro normativo, na perspetiva de facilitar cumprimento do RGPD.

Embora o EPD apenas seja obrigatório em algumas situações, as organizações podem sempre nomear um EPD a título voluntário.

A figura do EPD não é nova, pois embora a Diretiva 95/46/CE não se obriga, em nenhum momento, à designação de um EPD, diversas organizações dos Estado-Membros vieram a contratar estes profissionais, de forma a contribuir para a salvaguarda dos dados pessoais dos cidadãos.

O RGPD deixa bem explicito que o EPD não é o responsável em caso de incumprimento do Regulamento, sendo sempre os responsáveis de tratamento ou os subcontratantes que têm o ónus de assegurar e comprovar que o tratamento é realizado, conforme podemos constatar com o disposto no artigo 24.º, n.º1 do RGPD.

A importância da tutela da privacidade pode ser demonstrada através da constituição de um objetivo horizontal de ordem jurídica, de ser consagrada pela ordem jurídica no seu conjunto, ao nível constitucional, mas igualmente, pelo direito administrativo, direito penal e direito civil. Pode-se contextualizar que os instrumentos de tutela dos direitos do homem, ao nível internacional, centram-se essencialmente, na privacidade, protegendo-a deste modo, nos seus articulados, que corresponde à Declaração Universal dos Direitos do Homem, no artigo 8º, e com o Pacto Internacional sobre os Direitos Civis e Políticos (artigo 17º)[190.]

[190] Para uma análise destes documentos internacionais, cfr. LEITE PINTO, *ob. cit.*, p. 84 ss. e DAVID FELDMAN, *ob. cit.*, p. 28.

Bibliografia Citada

ALVAREZ, Tomás Prieto. La dignidade de la persona. Cizur Menor (Navarra). Espanha: Thomson-Civitas, 2005.

ANDRADE, José Carlos Vieira de. (2009). A Justiça Administrativa (Lições). 10ªedição. Almedina; Coimbra. P. 275 ss.

ANDRADE, José Carlos Vieira de. Os direitos fundamentais na Constituição Portuguesa de 1976. 2ªedição, Almedina, novembro de 2001, p. 278.

BERGT, Anotação ao artigo 37.º do RGPD em Kühling/Buchner, cit., rn. 40.

CALVÃO, Filipa – "O modelo de supervisão de tratamentos de dados pessoais na União Europeia: Da atual Diretiva ao futuro Regulamento", Revista Fórum de Proteção de Dados, n.º 1, julho de 2015, p. 42

CANOTILHO, J. J. Gomes; MOREIRA, Vital – Constituição da República Portuguesa Anotada. 4.ª Edição..., op. cit., pág. 551

CANOTILHO, J.J. Gomes. Direito Constitucional e Teoria da Constituição, ob cit., pp. 393- 410

CANOTILHO, J. J. Gomes. Civilização do Direito Constitucional ou Constitucionalização do Direito Civil A eficácia dos direitos fundamentais na ordem jurídico-civil no contexto do direito pós-moderno.

CATARINA Santos Botelho, A Tutela Directa dos Direitos Fundamentais… cit., p. 151, e ULLI F. H. RÜHL, op. cit., p. 157.

COSTA ANDRADE (Liberdade de Imprensa, cit., p. 17 s.) a sociedade do risco é "portadora de novas agressões, ameaças e perigos", multiplicando "exponencialmente as superfícies expostas às intempéries dos valores pessoais coenvolvidos".

CUNHA, Paulo Ferreira da. Res Pública: ensaios constitucionais. Coimbra: Almedina, 1998.

DIAS, Jorge de Figueiredo; MONTEIRO, Jorge Sinde. Responsabilidade Médica…, p. 53.

FERREIRA, Manuel Cavaleiro de, Lições de Direito Penal, Parte Geral I , Reimpressão da 4.ªedição, Almedina, Coimbra, 2010, p. 89

FIGUEIREDO DIAS, Jorge de, Direito Penal – Parte Geral, Tomo I, 2.ª edição, Coimbra Editora, Coimbra, 2007, pp.82 ss;

FRANÇOIS RIGAUX, "La liberté de la vie privée", cit., p. 556 (mostrando alguns dos perigos levantados pelos "bancos de dados").

GABRIEL, João – Atlas, mostra alto o mundo no seu ombro – Aplicabilidade extraterritorial do Regulamento Geral de Proteção de Dados. Vida Judiciária. Porto, Portugal: vida Económica. N.º 207, maio-junho de 2018, pág. 26

GOMES, Carla Amado. Intimação para protecção de direitos, liberdades e garantias. Revista do Ministério Público. Ano 26; Nº104; 1005;

JORGE MIRANDA, Ideias para uma revisão constitucional… cit. p. 15.

JOSÉ AUGUSTO SIMÕES. Proteção de dados e o novo regulamento geral da União Europeia. Revista Portuguesa de Medicina Geral e Familiar. versão impressa ISSN 2182-5173. Rev Port Med Geral Fam vol.34 no.5 Lisboa out. 2018

JOSÉ CARLOS VIEIRA DE ANDRADE, Os direitos fundamentais na Constituição Portuguesa de 1976, 2ªedição, Almedina, Novembro de 2001 275 e 276

José Carlos Brandão Proença, Lições de Cumprimento e Não Cumprimento das Obrigações (Coimbra: Coimbra Editora, 2011), 105

HeBerlein, Anotação ao artigo 37.º do RGPD em Ehmann/Selmayr, cit., rn. 41.

HENRIQUES, Miguel Gorjão, Direito da União Europeia, 2014, p. 296

HOFFMANN-RIEM, Wolfgang – Informationelle Selbsbestimmung in der Informationgesellsschaft – Auf dem Wege zu einem neuen Konzept des Datenschutzes. AöR, n.º 123, 1998. Pág. 520.

Hewlett-Packard Company. (2018). O que são as regras vinculativas das empresas (BCR - Binding Corporate Rules) da HP. Disponível em http://www8.hp.com/pt/pt/bindingcorporate-rules.html

Jorge REIS NOVAIS, "Renúncia a direitos fundamentais", in Jorge MIRANDA (org.), Perspectivas constitucionais. Nos 20 anos da Constituição, Coimbra, 1996, vol. I, pp. 263-335.

JORGE BACELAR GOUVEIA: Os direitos fundamentais atípicos, Lisboa, 1995; O estado de exceção no Direito Constitucional – entre a eficiência e a normatividade das estruturas de defesa extraordinária da Constituição, I e II, Coimbra, 1998; Estudos de Direito Público, I, Cascais, 2000

Klug, Anotação ao artigo 37.º do RGPD em Gola, cit., rn. 1.

LEITE PINTO, ob. cit., p. 84 ss. e DAVID FELDMAN, ob. cit., p. 28.

Luís Manuel Teles de Menezes Leitão, Direito das obrigações, volume II, Transmissão e extinção das obrigações, não cumprimento e garantias de crédito, 3.a edição, Coimbra 2005

Mafalda Miranda Barbosa, Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil, RDCom, 15-mar.-2018, p.436 e ss

Maxmillian Schrems v Data Protection Commissioner (C-362/14), Grand Chamber, 6 October 2015.

MACHADO, Jónatas E. M., Direito da União Europeia, 2010, p. 199-201, e HENRIQUES, Miguel Gorjão, Direito da União Europeia, 2014, p. 296.

MAÑAS, José Luís Piñar, Antecedentes e processo de reforma sobre protección de datos personales en la Unión Europea in Regulamento General de Protección de Datos. Hacia un nuevo modelo europeo de protección de datos, 2016, p. 49.

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

Merlin Gömann, O novo escopo territorial da lei de proteção de dados da UE: desconstruindo uma conquista revolucionária, Common Market Law Review, 54, pp. 567-590, 2017.

Manuel A. Domingues de Andrade, Teoria Geral das Obrigações, com a colaboração de Rui de Alarcão, Coimbra 1966

MALATRAS, Apostolos, et al., «Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities», in Computer Law & Security Review, volume 33, Issue 4, August 2017, Elsevier, p. 458-469, disponível em: https://www.sciencedirect.com/science/article/pii/S0267364917300808.

MOUTINHO, José Lobo – Legislador português precisa-se. Algumas notas sobre o regime sancionatório no Regulamento Geral Sobre a Proteção de Dados (Regulamento (UE) 2016/679) – Em Foco: Inteligência Artificial. Revista Fórum de Proteção de Dados. Portugal: Comissão Nacional de Proteção de Dados. N.º 4, julho de 2017, pág. 43.

Mário Ferreira Monte, Lineamentos de Direito das Contraordenações (Braga: AEDUM, 2014), 49–50.

Nuno Manuel Pinto Oliveira, Princípios de Direito dos Contratos (Coimbra: Coimbra Editora, 2011), 72,

PAOLO BARILE, Ilsogetto privato nella Costituzione Italiana, Pádua, 1953; a obra colectiva Die Grundrechte, Berlim, 1954-1966;

PHILIPPE BRAUD, La notion de liberté en droit public français, Paris, 1968;;

QUEIROZ, Cristina – "A protecção constitucional da recolha…", op. cit., pág. 298;

Paulo mota Pinto, Interesse contratual negativo e interesses contratual positivo, i, Coimbra editora, Coimbra, 2008, 81, ss e 481, ss.

Paul de Hert e Michal Czerniawski, Expandindo o escopo da proteção de dados europeia para além do território: Artigo 3 do Regulamento Geral de Proteção de Dados em seu contexto mais amplo, Lei Internacional de Privacidade de Dados, 2016, Vol. 6, No. 3

Pedro Miguel Freitas. Regulamento Geral de Proteção de Dados: uma visão portuguesa sobre o regime sancionatório. UNIO - EU LAW JOURNAL. Vol. 4, No. 2, julho 2018

PINHEIRO, Alexandre Sousa, Comentário ao Regulamento Geral de Proteção de Dados, 2018, p. 21

RODRÍGUEZ ÁLVAREZ, L.: «Artículo 18.4 CE», Comentarios a la Constitución de 1978. Libro Homenaje al Profesor Luís López Guerra, Valencia, Tirant lo Blanch, 2018.

SILVEIRA, Luís Lingnau da – "O direito à protecção de dados pessoais…", op. cit., pág. 209

SILVA, Germano Marques da, Direito Penal Português, Volume II, 2.ª Edição, Editorial Verbo, Lisboa, 2005, p. 22;

SIMAS SANTOS, Manuel et LEAL-HENRIQUES, Manuel, Noções de Direito Penal, 4.ª Edição, Rei dos Livros, Porto, 2011, pp. 81 ss.

Sinde MONTEIRO, Responsabilidade por conselhos, recomendações ou informações, Almedina, Coimbra, 1989, 239

THOMAS M. FRANCK, Comparative Constitutional Process — Cases and Materials — Fundamental Rights in the Common Law Nations, Londres, 1968

SILVEIRA, Alessandra; FROUFE, Pedro – Do mercado interno à cidadania…, op. cit., pág. 9

VASCONCELOS, Pedro Pais de. Direito de Personalidade. Coimbra: Almedina, 2006, p.30

VILELA, Alexandra – O Direito de Mera Ordenação Social: Entre a Ideia de "Recorrência" e a de "Erosão" do Direito Penal Clássico. Coimbra, Portugal: Coimbra Editora, 2013. Págs. 369-371.

Documentos legislativos

Acórdão com o processo nº 00001/17. BCPRT do Tribunal Central Administrativo Norte, de 14/07/2017, disponível em: http://www.dgsi.pt/jtcn.nsf/89d1c0288c2dd49c802575c8003279c7/2d62be6b1ae49e55802581d1003a1f44?OpenDocument&Highlight=0,Protec%C3%A7%C3%A3o,dados,pessoais

Artigo 27.º da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016,

CCPA, Sections 1798.105, 1798.140, 1798.145, 1798.155

Commission Nationale de l'informatique et des Liberte´s, Methodology for Privacy Risk Management (2012), 4.

Comissão Europeia. (2012). COM (2012) 11 final. Proposta de regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=COM:2012:0011:FIN

Declaração da CNIL, 30 de novembro de 2017 (avis de la CNIL Délibération n ° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n ° 78-17 du janvier 1978) https://www.cnil.fr/sites/default/files/atoms/files/projet_davis_cnil.pdf

Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)

Diretiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de Novembro de 2009

Diretiva 2002/58/CE relativa ao tratamento de dados e à proteção da privacidade no setor das comunicações eletrónicas

Draft EU General Data Protection Regulation (unofficial consolidated version after LIBE Committee vote), at art 33, } 1.

EDPB Guidelines on Personal data breach notification under Regulation 2016/679, de 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827 p. 10 e ss.

European Parliament Resolution of 12 March 2014 on the 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, P7 TA (2014)0212, 12 March 2014, } 66.

Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change (2012), 30.

Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006).

Available at: https://www.law.cornell.edu/uscode/text/15/168

GRUPO DE TRABALHO DO ART. 29.º DA DIRETIVA 95/46/CE PARA A PROTEÇÃO DE DADOS – Diretrizes de aplicação e fixação de coimas para efeitos do Regulamento 2016/679, 17/PT, WP 253, adotadas em 3 de outubro de 2017. [Consulta em 04/10/2020]. Disponível para consulta em: http://bit.ly/2VRYiCx. Pág. 4.

Grupo de Trabalho do Artigo 29.º sobre o encarregado da proteção de dados 16/EN WP 243.

Lei n.º 67/98, de 26 de outubro

Lei nº 78-17 de 6 de janeiro de 1978 relativa ao processamento de dados, arquivos e liberdades; uma versão em inglês, mas não atualizada está disponível em https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Jefatura del Estado. «BOE» núm. 294, de 6 de diciembre de 2018 Referencia: BOE-A-2018-16673

Lei n ° 2016-1321 de 7 de outubro de 2016 para uma república digital, https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000031589829&type=general&legislature=1

A Lei Federal de Proteção de Dados, conforme interpretada por uma resolução do Düsseldorfer Kreis

Lei n.º 58/2019, Diário da República n.º 151/2019, Série I de 2019-08-08, Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

National Institute of Standards and Technology, NIST Privacy Engineering Objectives and Risk Model Discussion Draft (2014), 3.

Organization for Economic Co-operation and Development, Supplementary Explanatory memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013), 30

Parecer 15/2011 do GT29 sobre a definição de consentimento (WP 187), p. 25.

Parecer 03/2014 relativo à notificação da violação de dados pessoais http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/files/2014/wp213_en.pdf

Parecer n.º 20/2018, op. cit, ibid.

Parecer 03/2013 sobre a limitação da finalidade, disponível em: http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Parlamento Europeu, Conselho Europeu. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016

Projeto de lei n ° 490 relativo à proteção de dados pessoais, aprovado em 13 de dezembro de 2017

Regulamento (CE) n.o 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

Regulamento (CE) n.º 2006/2004 relativo à cooperação entre autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor, disponível em:

https://eurex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32009L0136&from=PT

Regulamento (EU) n.º 611/2013, sobre o âmbito de aplicação do diploma.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016,

WP 217, Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento nos termos do artigo 7.º, pág. 24, no que se refere à questão: «O que torna um interesse 'legítimo' ou 'ilegítimo'?»

Trilateral Research & Consulting, Privacy Impact Assessment and Risk Management (2013), 15–16.