Oliveira, Sara Filipa Carneiro de

Regime da proteção de dados pessoais nas empresas : impacto e adaptações à nova realidade

http://hdl.handle.net/11067/6440

Metadados

Data de Publicação 2021

Resumo A escolha deste tema visa abordar a importância da proteção de dados e analisar este novo paradigma, este tema surge no âmbito do novo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho aprovado a 27 de abril de 2016, mais conhecido como Regulamento Geral sobre a Proteção de Dados. Desta forma, a proteção de dados pessoais ganhou uma crescente importância no contexto atual, isto porque a informação é cada vez mais um bem fundamental e por isso mesmo tem de ser devidamente protegida, ...

The choice of this theme aims to address the importance of data protection and analyze this new paradigm, this theme comes under the new Regulation (EU) 2016/679 of the European Parliament and of the Council approved on April 27, 2016, better known as Regulation General on Data Protection. In this way, the protection of personal data has gained increasing importance in the current context, this because information is increasingly a fundamental asset and therefore it must be properly protected, ...

Palavras Chave Direito, Protecção de Dados - Direito e Legislação - Empresas, Responsabilidade civil

Tipo masterThesis

Revisão de Pares Não

Coleções [ULP-FD] Dissertações

UNIVERSIDADE LUSÍADA DO PORTO

REGIME DA PROTEÇÃO DE DADOS PESSOAIS NAS EMPRESAS:
IMPACTO E ADAPTAÇÕES À NOVA REALIDADE

Sara Filipa Carneiro de Oliveira

Orientador: Professor Doutor Alberto Ribeiro de Almeida

Dissertação para obtenção do Grau de Mestre

Porto, 2021.

UNIVERSIDADE LUSÍADA DO PORTO

REGIME DA PROTEÇÃO DE DADOS PESSOAIS NAS EMPRESAS:
IMPACTO E ADAPTAÇÕES À NOVA REALIDADE

Sara Filipa Carneiro de Oliveira

Orientador: Professor Doutor Alberto Ribeiro de Almeida

Dissertação para obtenção do Grau de Mestre

Porto, 2021.

Agradecimentos

A realização da presente dissertação de mestrado contou com importantes apoios e incentivos sem as quais isto não se teria tornado uma realidade e ao qual estou eternamente grata.

Ao ilustre professor Doutor Alberto Ribeiro de Almeida pela sua orientação, total apoio, disponibilidade, pelo saber que transmitiu críticas, opiniões. Pela sua simpatia e entusiasmo com que demonstrou com este trabalho, e por todo o seu incentivo. Foi sem dúvida a chave para o sucesso deste trabalho.

A todos os bibliotecários da Universidade Lusíada Porto, por me ajudarem a reunir a bibliografia que precisava, e por toda motivação que sempre me deram.

Aos meus colegas de curso de Direito que embora em diferentes instituições também acompanham e vivem este momento, e acima de tudo pela vossa amizade.

Aos advogados da Santos, Maia, Marques & Moreira, Sociedade de Advogados, R.L, em especial ao Dr. Pedro Moreira meu patrono, um muito obrigada pelo carinho, paciência e por me acompanharem nesta jornada e na minha etapa como Advogada Estagiária.

À minha irmã Patrícia, que sempre me apoiou, desde o dia que lhe disse que voltaria a estudar e frequentar um curso superior, tão grata por isso.

Aos meus pais, que vivem com orgulho e paixão todos os meus passos, que acreditam que o meu percurso ainda é muito longo.

E por fim, Simão Ferreira, a pessoa que mais do que eu, acredita em mim, aquele que me arranca um sorriso mesmo nos momentos mais difíceis.

O meu muito Obrigada!

Índice

Lista de Abreviaturas, Acrónimos e Siglas

Ac.	Acórdão
ACI	Autoridade de Controlo Independente
ADFUE	Agência dos Direitos Fundamentais da União Europeia
AEPD	Autoridade Independente Europeia para a Proteção de Dados
AIPD	Avaliações de Impacto sobre a Proteção de Dados
Al.	Alínea
Art.	Artigo
Arts.	Artigos
Cap.	Capítulo
CC	Código Civil
CCom	Código Comercial
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CE	Comissão Europeia
CEPD	Comité Europeu para a Proteção de Dados
Cfr.	Conforme
CNPD	Comissão Nacional de Proteção de Dados
CRP	Constituição da República Portuguesa
D95	Diretiva 95/46/CE
DPIA	Data Protection Impact Assesments
ELSJ	Espaço de Liberdade Segurança e Justiça
EPD	Encarregado de Proteção de Dados
GT29	Grupo de Trabalho do Artigo 29.º para a Proteção de Dados
LPDP	Lei de Proteção de Dados Pessoais
n.º	Número
p.	Página
P.ex.	Por exemplo
pp.	Páginas

RGCO	Regime Geral das Contra Ordenações
RGPD	Regulamento Geral de Proteção de Dados
TCE	Tratado da Comunidade Europeia
TFUE	Tratado de Funcionamento da União Europeia
TJUE	Tribunal de Justiça da União Europeia
UE	União Europeia
vide	Veja-se em

Resumo

A escolha deste tema visa abordar a importância da proteção de dados e analisar este novo paradigma, este tema surge no âmbito do novo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho aprovado a 27 de abril de 2016, mais conhecido como Regulamento Geral sobre a Proteção de Dados.

Desta forma, a proteção de dados pessoais ganhou uma crescente importância no contexto atual, isto porque a informação é cada vez mais um bem fundamental e por isso mesmo tem de ser devidamente protegida, pois uma simples divulgação de dados pessoais pode causar danos irreversíveis na esfera jurídica dos titulares.

Para garantir um quadro jurídico mais completo e sólido no que concerne à proteção dos dados pessoais na União Europeia procedeu-se à revogação da Diretiva 95/46/CE pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Este diploma cria um regime jurídico uniforme para todos os Estados-Membros, procurando assim evitar diferentes graus de proteção dos direitos dos cidadãos europeus. A introdução deste novo regime traduz-se, num desafio para os particulares e para as várias entidades envolvidas na sua aplicação, nomeadamente para as empresas.

No âmbito normativo, é evidenciado uma exaustividade da regulação europeia que, na verdade, deixa pouca margem de complementaridade da legislação nacional, querendo com isto alcançar uma mais harmonização dos diferentes regimes nacionais.

O legislador europeu, no âmbito de aplicação do RGPD, demonstra a preocupação em assegurar uma execução normativa adequada, instituindo mecanismos e procedimentos organizacionais com o objetivo específico de o garantir. Deste modo, da perspetiva organizacional, o RGPD obriga a uma mudança das autoridades de controlo dos diferentes Estados-Membro, e, por conseguinte, afeta em alguma medida os agentes económicos.

É seguramente dos temas mais atuais no mundo jurídico, e é neste contexto que surge o interesse de trabalhar e pesquisar sobre esta "nova" realidade.

Abstract

The choice of this theme aims to address the importance of data protection and analyze this new paradigm, this theme comes under the new Regulation (EU) 2016/679 of the European Parliament and of the Council approved on April 27, 2016, better known as Regulation General on Data Protection.

In this way, the protection of personal data has gained increasing importance in the current context, this because information is increasingly a fundamental asset and therefore it must be properly protected, as a simple disclosure of personal data can cause irreversible damage in the sphere legal status of the holders.

To ensure a more complete and solid legal framework with regard to the protection of personal data in the European Union, Directive 95/46/EC was repealed by Regulation (EU) 2016/679 of the European Parliament and of the Council. This diploma creates a uniform legal regime for all Member States, thus seeking to avoid different degrees of protection of the rights of European citizens. The introduction of this new regime is a challenge for individuals and for the various entities involved in its application, namely for companies.

In the normative scope, an exhaustiveness of the European regulation is evidenced, which, in fact, leaves little room for complementarity of the national legislation, wanting with this to reach a more harmonization of the different national regimes.

The European legislator, within the scope of application of the RGPD, demonstrates the concern to ensure an adequate normative execution, instituting organizational mechanisms and procedures with the specific objective of guaranteeing it. Thus, from an organizational perspective, the RGPD requires a change in the supervisory authorities of the different Member States, and, therefore, affects to some extent the economic agents.

It is certainly one of the most current issues in the legal world, and it is in this context that the interest in working and researching this “new” reality arises.

Palavras-Chave

RGPD

Regulamento UE

Tratamento de dados

Responsabilidade pela proteção dos dados.

Introdução

A 27 de Abril de 2016 foi aprovado no Parlamento Europeu, com 95% dos votos a favor, o novo Regulamento Geral de Proteção de Dados (RGPD), após aproximadamente 5 anos de negociações e 4.000 adendas (Gomes R. 2017, p. 1).

O Regulamento (EU) 2016/679 do Parlamento Europeu e o Conselho, entrou em vigor a 25 de maio de 2018, conhecido como RGPD (Regulamento Geral sobre a Proteção de Dados), sendo o seu âmbito de aplicação relativo à proteção das pessoas singulares no que concerne ao tratamento de dados pessoais e à livre circulação dos mesmos. Em Portugal, substitui a Lei 67/98, que transpõe para a ordem jurídica portuguesa a anterior Diretiva 95/46/CE.

A União Europeia, veio reforçar a legislação de proteção de dados pessoais, após mais de duas décadas desde a Diretiva 95/46/CE, adotando assim o atual regulamento que apresenta como objetivo principal cooperar para a realização de um espaço de liberdade e segurança, um espaço para o progresso económico e social, consolidação das economias a nível de mercado interno e principalmente para o bem-estar das pessoas singulares.

Implementar um regime de proteção de dados vem alterar profundamente as organizações empresariais. Este regulamento obriga a profundas alterações na forma como habitualmente trabalham com os dados pessoais que possuem, nomeadamente no que diz respeito a procedimentos internos, recolha dos dados pessoais e das ferramentas utilizadas no processamento destes dados, dando ao titular um maior controlo sobre os mesmos.

Uma das alterações que este regulamento traz é precisamente uma revisão à definição de dados pessoais, define novas regras para o tratamento dos dados pessoais, direitos dos titulares dos dados, obrigações para as organizações que tratam os dados e medidas de contraordenação para o seu incumprimento.

O presente regulamento reflete a vontade do Parlamento Europeu e do Conselho da União Europeia de implementar *um quadro de proteção de dados sólido e coerente, apoiada por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno* (Magalhães & Pereira, 2018).

Com o atual regulamento não se pretende apenas prever um conjunto de regras de proteção de dados para toda a União Europeia, pretende-se garantir segurança aos titulares de dados e ainda proporcionar um panorama de cumprimento modernizado com base na responsabilidade em matéria de proteção de dados na Europa.

Este trabalho encontra-se dividido em sete partes, donde começo na primeira parte por fazer uma contextualização europeia e nacional, passando pela análise de diversos diplomas que já regulavam a matéria de proteção de dados.

Na segunda parte, abordarei os princípios que norteiam o RGPD, passando para a terceira parte que falarei dos direitos dos titulares dos dados pessoais, fazendo uma análise detalhada de cada um deles.

Na quarta parte, e não menos importante, vou abordar o âmbito da responsabilidade que por sua vez tem conexão com a quinta e sexta parte, que abordo os temas das sanções e da tutela judicial.

Veja-se que até aqui há um fio condutor deste trabalho em paralelo com a disposição normativa do RGPD.

Por último, entramos na sétima parte desta dissertação, ao qual lanço aqui a pergunta que nos propusemos a responder: com o RGPD que impacto existiu no seio das empresas e concomitantemente o que fizeram para se adaptarem à nova realidade.

Capítulo I – Enquadramento Geral

1.1.A origem do Regime geral de Proteção de Dados: contextualização Europeia e Nacional

A UE como união económica e política é um espaço de livre circulação de pessoas e bens entre os Estados-Membros e como tal deve assegurar os direitos fundamentais constantes da Carta dos Direitos Fundamentais da União Europeia (CDFUE). Muitas das medidas de segurança criadas pela UE, passam pela coleta, utilização e troca de dados pessoais, e daí surge a necessidade de salvaguardar os indivíduos sempre que os seus dados pessoais são tratados.

A proteção das pessoas singulares em relação ao tratamento de dados pessoais é um direito fundamental. A Carta dos Direitos Fundamentais da União Europeia (Carta) através do seu artigo 8.º n.º1 e o Tratado sobre o Funcionamento da União Europeia (TFUE) no artigo 16.º nº 1, define que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito (Parlamento Europeu, 2016a).

Conforme resulta da Diretiva da (UE) 2016/680 do Parlamento Europeu e do Conselho, os principais instrumentos legislativos em matéria de proteção de dados para melhor contextualizar é o TFUE nomeadamente no art.º 16.º [1] bem como na CDFUE, art.º 8.º [2], o artigo 16.º do TFUE prevê que o Parlamento e o Conselho definem as normas referentes à proteção das pessoas singulares no que concerne ao tratamento de dados pessoais pelas instituições, órgãos e agências da União, assim como pelos Estados-Membros na prática de atividades relativas à aplicação do direito da União.

Em dezembro de 2009, o Conselho Europeu aprovou, no seguimento dos programas de Tampere (de outubro de 1999) e Haia (de novembro de 2004), o programa

[1] Artigo 16.º (ex-artigo 286.º TCE)
1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes.

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

plurianual no Espaço de Liberdade Segurança e Justiça (ELSJ) para o período 2010-2014 conhecido por Programa de Estocolmo. Nas suas conclusões, o Conselho Europeu definiu as orientações estratégicas para o planeamento legislativo e operacional para os próximos anos no quadro do ELSJ, em conformidade com o artigo 68.º do TFUE. Um dos principais objetivos deste programa consiste em proteger melhor os dados pessoais na UE (Parlamento Europeu, 2020).

De mencionar a Convenção 108/1981 do Conselho da Europa que foi o primeiro instrumento internacional juridicamente vinculativo adotado para a proteção das pessoas singulares no que respeita ao tratamento automatizado de dados pessoais (Parlamento Europeu, 2020).

Por sua vez, a Diretiva 95/46/CE (D95) do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, imponha aos Estados-Membro a garantia dos direitos e liberdades das pessoas singulares no respeitante ao tratamento dos dados pessoais, designadamente, o seu direito à privacidade com o objetivo de garantir a livre circulação de dados pessoais na Comunidade Europeia.[3] Estes eram os documentos legais, em vigor, relativos à proteção de dados pessoais a nível europeu (Parlamento Europeu, 2002).

A Diretiva 2002/58/CE, alterada em 2009, no que concerne ao direito da privacidade, define regras por forma a garantir a segurança não só no que ao tratamento de dados pessoais diz respeito, como à notificação da violação de dados pessoais e à confidencialidade das comunicações. Não obstante a isso, proíbe, nos casos que o titular dos dados não tenha dado o seu consentimento, comunicações não solicitadas (Parlamento Europeu, 2002).

Relativa à conservação de dados, a Diretiva 2006/24/CE, é aplicável aos dados de tráfego e aos dados de localização relativos quer a pessoas singulares como a pessoas coletivas, e ainda aos dados conexos necessários para identificar o utilizador registado ou o assinante. Não sendo aplicável ao conteúdo das comunicações eletrónicas, assim com as informações consultadas através de uma plataforma de comunicações eletrónicas[4] (Parlamento Europeu, 2006).

Por sua vez, o regulamento (CE) n.º 45/2001 é relativo ao tratamento de dados pessoais por instituições e órgãos comunitários (Parlamento Europeu, 2001).

---

[3] O regulamento 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) (sublinhado nosso), conforme supramencionado no parágrafo 2º da introdução.

[4] Artigo 1º nº2 "Objeto e âmbito de aplicação".

Também de referir, o Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (GT29) que emite recomendações e pareceres. É um órgão independente sobre proteção de dados e privacidade sendo constituído por representantes das autoridades nacionais dos Estados-Membros da UE.[5]

Em Portugal, paralelamente à legislação europeia, a proteção de dados pessoais encontra-se vertida na Constituição da República Portuguesa e demais legislação, como um direito fundamental, sendo que a violação dos dados pessoais é passível de ser punida como crime ou contraordenação no sistema jurídico português.

Portugal confere dignidade constitucional à proteção de dados pessoais, logo na CRP aprovada em 2 de abril de 1976, que foi sucessivamente atualizada, ampliada e reforçada pelas leis de revisão de 1982 e 1989, e por fim, na revisão constitucional de 1997 dedicou um artigo à matéria da proteção de dados pessoais, nomeadamente o seu art.º 35º.[6]

Como refere Catarina Sarmento e Castro *longe de ser um mero direito contra as intrusões do Estado ou de outros indivíduos, que devem abster-se de proceder a tratamento dos seus dados pessoais, é um direito a decidir até onde vai a sombra que deseja que paire sobre as informações que lhe respeitam, construindo-se como uma liberdade, como um poder de determinar o uso dos seus dados pessoais. Para a mesma autora, o direito à autodeterminação informativa é um verdadeiro direito fundamental com conteúdos próprios* e não uma mera garantia do direito à reserva da intimidade da vida privada (Castro, 2004, pp. 11-12).

Na aceção de Canotilho e Moreira (2014) essa proteção concretiza-se em três direitos, designadamente, *o direito de acesso aos registos informáticos para conhecimento dos seus dados pessoais deles constantes, direito ao sigilo em relação a terceiros dos dados pessoais informatizados e direito à sua não interconexão, direito à proibição de tratamento informático de certos tipos de dados pessoais, sendo que a proibição do número nacional único funciona como garantia daqueles direitos,*

[5] Este grupo de trabalho foi instituído ao abrigo do artigo 29.º da Diretiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições encontram-se descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.

[6] Artigo 35.º da CRP "Utilização Informática".

1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização.
2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.
3. É proibida a atribuição de um número nacional único aos cidadãos.

dificultando o tratamento informático de dados pessoais e a sua interconexão, que seria facilitada com um identificador comum.

Não obstante de se tratar de um regulamento de União Europeia, o RGPD apresenta um conjunto alargado de normas que exige a intervenção do legislador nacional. Portanto, Portugal teve que adotar as soluções mais adequadas para a proteção dos direitos dos titulares de dados pessoais tendo em consideração da competitividade das empresas portuguesas no quadro da União Europeia (Proposta de Lei n.º 120/XIII, 2018).

Por conseguinte, a Diretiva 95/46/CE é revogada, como também da legislação nacional, a Lei n.º 67/98, de 26 de outubro (LPDP), pelo que Portugal teve de preparar e elaborar uma proposta de lei de execução do RGPD, em consequência surgiu a Proposta de Lei 120/XIII.

Embora a proposta de lei fosse aprovada pelo Conselho de Ministros e reencaminhada à Assembleia da República, a mesma não foi aprovada, ao qual mereceu um parecer n.º 20/2018, de 2 de maio de 2018, da Comissão Nacional de Proteção de Dados, que teceu duras críticas, apontando imprecisões na reprodução de normas do RGPD e normas que se contradizem.[7]

[7] No parecer n.º 20/2018 a CNPD invoca, entre outros, o desrespeito pelo direito da União Europeia na medida em que "a presente proposta pretende reproduzir em alguns artigos parte do articulado do RGPD. É esse, designadamente, o caso do artigo 2.º (âmbito de aplicação), do artigo 11.º (funções do encarregado de proteção de dados) ou do artigo 13.º (encarregados de proteção de dados em entidades privadas). E não se trata aqui sequer de legislar sobre aspetos específicos que o Regulamento remeta para o campo de ação do Estado-Membro, mas apenas de uma tentativa de replicar disposições, com a agravante de, em alguns casos concretos, desvirtuar por completo o teor do RGPD, contrariando-o grosseiramente. Em segundo lugar, a Proposta pretende introduzir no direito nacional norma que difere a aplicação do RGPD para momento posterior à data prescrita no artigo 99.º do próprio Regulamento. Assim, apesar do RGPD ser aplicável a partir de 25 de maio de 2018, seria possível, nos termos do proposto no artigo 61.º (renovação do consentimento) da Proposta, demorar seis meses desde a entrada em vigor da lei nacional para obter um consentimento que constituiria o fundamento de legitimidade para certos tratamentos de dados, admitindo-se, portanto, à contrário a existência de tratamentos ilícitos durante esse período de tempo. (…) *O esforço de repetição de normas do Regulamento na lei nacional assume ainda maior gravidade quando o texto da Proposta entra em clara contradição com o conteúdo dos preceitos do RGPD*, salientando ainda que o artigo 2.º da Proposta sobre o âmbito de aplicação da lei nacional. O n.º 1 deste artigo prescreve: *A presente lei aplica-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante (…), aplicando-se todas as exclusões previstas no artigo 2.º do RGPD*. A alínea a) do n.º 2 determina que: *A presente lei aplica-se aos tratamentos de dados pessoais realizados fora do território nacional quando sejam efetuados no âmbito da atividade de um estabelecimento situado no território nacional*. Com efeito, estas normas traduzem-se numa manifesta violação do artigo 3.º n.º 1 do RGPD, pondo em causa o mecanismo de balcão único que constitui uma das características mais emblemáticas deste regulamento. Invocando ainda a existência de desconformidades com o direito da união no que concerne às normas relativas à autoridade de controlo em matéria de proteção de dados, assim como o facto de a proposta de lei no seu artigo 11.º estabelecer f*unções adicionais aos encarregados de proteção de dados, quando tal não é permitido pelo RGPD*, acrescentando que os n.º 3 e 4 do artigo 12.º não cumprem com o preceituado no RGPD, devendo para o efeito ser suprimidos, na medida que dispõe sobre matérias que não se encontram na disponibilidade dos Estados-Membros. O mesmo acontece com o artigo 18.º, que dispõe sobre a portabilidade e interoperabilidade dos dados, e o artigo 22.º sobre a transferência de dados, onde pretende-se legislar sobre matéria não permitida

Por sua vez, a 14 de julho de 2019 foi aprovada na Assembleia da República a proposta de Lei n.º 120/XIII/3.ª[8], que assegura a execução, na ordem jurídica nacional, do RGPD, tendo a mesma sido promulgada pelo Presidente da República a 26 de julho e publicada a 8 de agosto, sob a Lei n.º 58/2019, de 8 de agosto, volvidos um ano e três meses da produção de efeitos do RGPD (Proposta de Lei n.º 120/XIII, 2018).

Todavia, a 20 de setembro de 2019 a CNPD [9] publicou na sua página oficial a Deliberação 2019/494 sobre a Lei n.º 58/2019, deliberando desaplicar nove disposições[10] da referida lei de modo a *assegurar o primado do direito da União Europeia e a plena efetividade do RGPD*, na medida que *decorre do princípio do primado que, além dos tribunais nacionais, também as entidades administrativas estão obrigadas a desaplicar as normas nacionais que contrariam o direito da União Europeia, como determinou expressamente o TJUE, no acórdão Fratelli Contanzo, que veio vincular todos os órgãos da Administração Pública ao dever de aplicar integralmente o direito da União afastando se necessário as disposições nacionais que constituam um obstáculo à plena eficácia das normas daquele direito* (Tribunal de Justiça da União Europeia, 1989).

---

pelo RGPD, ao mesmo tempo que se altera o alcance das disposições do RGPD. Outra crítica suscitada foi a relacionada com o dever de sigilo, sendo que o artigo 20.º da Proposta suscita uma crítica veemente da CNPD pela violação flagrante da nossa Constituição e da Carta dos Direitos Fundamentais da União Europeia, além do incumprimento manifesto do RGPD, ao impedir liminarmente o exercício do direito de acesso". Outro dos pontos criticados prendeu-se com a consagração nos artigos 23.º (admite que os dados pessoais sejam tratados por entidades públicas para finalidades diferentes das que justificaram a recolha, desde que esteja em causa a prossecução do interesse público), 44.º e 54.º (preveem a isenção de coimas para as entidades públicas) da proposta de um regime diferenciado para os tratamentos de dados em que os responsáveis ou subcontratantes são entidades públicas. O modo como o legislador nacional optou por legislar em matérias de regulação obrigatória para o legislador nacional, nomeadamente, acreditação e certificação, idade para o consentimento de menores, tratamento de dados para efeitos de liberdade de expressão e de informação, para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, audiência dos interessados e os mecanismos de cooperação e coerência, também foi alvo de crítica. A CNPD também se pronunciou sobre consagração de limites máximos inferiores aos definidos no RGPD no que concerne ao regime sancionatório, concluindo que "o RGPD deixou às autoridades de controlo o poder de aplicar em concreto coimas nos montantes máximos aí previstos, naturalmente com a ponderação dos critérios orientadores do cálculo da coima a que se refere o artigo 83.º. Donde, a fixação em abstrato, em lei nacional, de limites máximos inferiores aos previstos nos n.ºs 4 e 5 do artigo 83.º do RGPD constituir uma violação dos mesmos. O mesmo raciocínio tem de valer para a fixação de limites mínimos, uma vez que o RGPD não deixa espaço ao legislador nacional para definir quadro sancionatório diferente do que está estabelecido nos n.ºs 4 e 5 do artigo 83.º do RGPD"

[8] Diário da República, II série A, N. º89/XIII/3 de 26/03/2018 p. 30-48.

[9] A CNPD é uma autoridade administrativa independente e competente com atribuição em Portugal, para controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados, a Comissão Nacional de Proteção de Dados.

[10] Com os fundamentos acima expostos, de forma a assegurar o primado do direito da União Europeia e a plena efetividade do RGPD, a CNPD delibera desaplicar, nas situações de tratamento de dados pessoais que venha a apreciar, as seguintes normas da Lei n.º 58/2019, de 8 de agosto: i. Artigo 2.º, n.ºs 1 e 2 ii. Artigo 20.º, n.º 1 iii. Artigo 23.º iv. Artigo 28.º n.º 3, alínea a) v. Artigo 37.º n.º 1, alíneas a), h) e k), e n.º 2 vi. Artigo 38.º n.º 1, alínea b), e n.º 2 vii. Artigo 39.º, n.ºs 1 e 3 viii. Artigo 61.º, n.º 2 ix. Artigo 62.º, n.º2

Dado a todo avanço tecnológico que acompanha esta sociedade moderna, a introdução do RGPD[11] no contexto europeu vem reforçar aquilo que há muito se previa, ou seja, a necessidade de novo jurídico-legal sobre o direito fundamental à privacidade, ao direito à reserva sobre a intimidade privada e o direito à utilização da informática. (Lambelho & Mendes, 2019, pp. 9-10).

1.2.O âmbito de aplicação do RGPD

1.2.1. Material

Quanto ao âmbito de aplicação material, o art.º 2.º n.º 1 do RGPD refere que o mesmo regulamento *aplica-se ao tratamento[12] de dados pessoais[13] por meios total ou parcialmente automatizados[14], bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.*

Nos termos do n.º 2, passamos a delimitar negativamente o seu âmbito, encontrando-se, assim, excluídos do âmbito de aplicação do presente regulamento (Parlamento Europeu, 2016b):

1. Ao tratamento efetuado no exercício de atividades não sujeitas à aplicação do direito da União [15];
2. Ao tratamento de dados efetuado pelos Estados-Membros no exercício de atividades abrangidas no âmbito de aplicação à política externa e de segurança comum (Título V, Cap. II do TUE);
3. Ao tratamento efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas[16];

---

[11] Segundo José Mañas (2016) *A União Europeia optou por realizar a mais importante reforma da proteção de dados das últimas décadas por meio de um Regulamento. Dessa forma, procura-se uma estrutura mais sólida e coerente que evita a aplicação fragmentada, a incerteza jurídica e as diferenças na proteção dos direitos e liberdades em Estados e, pelo contrário, garantem um nível de proteção uniforme e elevado. Com efeito, os Regulamentos da União Europeia têm um alcance geral e são obrigatórias em todos os seus elementos e diretamente aplicáveis em cada Estado-Membro (art.º 288º do Tratado sobre o Funcionamento do União Europeia*. Trata-se, portanto, de um ato legislativo da UE, que, pela sua natureza, é parte integrante do direito interno e produz efeito direto simultaneamente nas relações verticais e horizontais, sem necessidade de qualquer mecanismo de receção (Machado, 2010, pp. 199-201).

[12] Definição constante do art.º 4.º n.º 2.

[13] Cf. Art.º 4.º n.º 1, saliente-se que o legislador optou por uma definição do conceito de dados pessoais bastante ampla que abrange qualquer informação, de qualquer natureza e independentemente do suporte.

[14] Por automatização de dados pessoais, entende-se como o processo em que a organização otimiza, a recolha e tratamento, com o objetivo de reduzir o esforço associado, e permitir executar as atividades relacionadas com os mesmos, em aplicações digitais, substituindo os processos manuais. Este processo de automatização resulta em maior eficácia na otimização, monitorização e controlo por parte da organização.

[15] P. ex. no âmbito de medidas de segurança nacional.

[16] Sem ligação a uma atividade profissional ou comercial.

4. Ao tratamento de dados efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública;
5. Ao que se refere os dados anonimizados que de acordo com o considerando 26 os exclui do âmbito da aplicação do RGPD[17]

Importa agora apresentar o sentido da jurisprudência proveniente do TJUE que nos permite identificar que situações se enquadram no âmbito de aplicação material.

Sublinhe-se o Acórdão do TJUE de 11 de dezembro de 2014, em que Ryneš captou a imagem de dois indivíduos que partiram as janelas da sua casa através do sistema de vigilância CCTV doméstico que havia instalado. A gravação foi entregue à polícia e usada durante o processo criminal. Para o TJUE os tratamentos em causa não se integravam na *"household exemption"*, *uma videovigilância (...) ainda que parcialmente, ao espaço público e, por esse motivo, se dirige para fora da esfera privada da pessoa que procede do tratamento de dados por esse meio, não pode ser considerada uma atividade exclusivamente pessoal ou doméstica*.

A decisão do tribunal foi no sentido de que *a exploração de um sistema de câmara que dá lugar a uma gravação vídeo de pessoas, guardada num dispositivo de gravação contínua, como um disco rígido, sistema esse instalado por uma pessoa singular na sua casa de família para proteger os bens, a saúde e a vida dos proprietários dessa casa e que vigia igualmente o espaço público, não constitui um tratamento de dados efetuado no exercício de atividades exclusivamente pessoais ou domésticas, na aceção desta disposição.*

1.2.2. Territorial

O âmbito de aplicação territorial do RGPD é estabelecido no artigo 3.º nº 1 *ao tratamento de 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*.

[17] Tendo em conta a diretiva 95/46/CE e outros instrumentos jurídicos, a anonimização resulta do tratamento de dados pessoais a fim de evitar irreversivelmente a identificação. Além disso, os dados anónimos, são abrangidos pelo âmbito de aplicação da legislação da proteção de dados, ao qual os titulares dos dados podem ainda ter direito à proteção ao abrigo de outras disposições.

O legislador com o artigo 3.º do RGPD visa garantir uma proteção abrangente dos direitos dos titulares dos dados na UE e de criar, no que se refere ao requisito de proteção de dados, condições equitativas para as empresas ativas nos mercados da UE, num contexto de fluxos de dados a nível mundial (Comité Europeu para a Proteção de Dados, 2019).

Nomeadamente, define o âmbito de aplicação territorial do regulamento com base em dois critérios principais: o critério do "estabelecimento", nos termos do artigo 3.º n.º 1, e o critério do "direcionamento", nos termos do artigo 3.º n.º 2.

Verificando-se que estes dois critérios suprarreferidos se encontrem preenchidos aplicar-se-á ao correspondente tratamento de dados pessoais efetuado pelo responsável pelo tratamento ou pelo subcontratante[18] em questão. *Além disso, o artigo 3.º n.º 3, confirma a aplicação do RGPD ao tratamento sempre que o direito de um Estado-Membro se aplique por força do direito internacional público* (Comité Europeu para a Proteção de Dados, 2019).

Para alguns autores, o âmbito territorial do RGPD é a sua novidade mais controversa. *Veja-se, o artigo 3.º do RGPD pressupõe que o responsável pelo tratamento tem uma ligação substancial à UE, seja porque ali tem um estabelecimento seja porque trata os dados pessoais de titulares de dados aí localizados e as suas atividades são direcionadas para os mesmos ou, melhor dizendo, para o mercado da UE, para os seus consumidores ou para a "comunidade comercial da UE"* (Gomann, 2017, p. 586).

Como afirma Alsenoy (2017, p. 94), *o nexo principal com o território da UE não é a presença de um responsável pelo tratamento ou de um subcontratante na UE, mas a localização dos titulares de dados para os quais as atividades em causa (de oferta de produtos e serviço ou a monitorização de comportamentos) são direcionadas*.

É descrito por Hert e Czerniawski (2016) que a solução legislativa é como uma estratégia do destino das "atividades", estes autores defendem ainda a validade do artigo 3.º do RGPD como um suporte na ideia de que os operadores estrangeiros (exteriores à União Europeia) não serão surpreendidos com a vinculação ao regime da UE, sendo que só serão abrangidos pelo regulamento se as suas atividades tiverem como objetivo a própria União Europeia.

[18] Subcontratante, a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento.

Desta forma, o mais importante para a determinação da aplicação do RGPD numa situação em específico não é o local onde se encontra o responsável pelo tratamento, mas sim a localização do titular dos dados na União, quer seja nacional, residente ou viajante. Este vínculo do titular dos dados com a EU vai de encontro aos objetivos da Diretiva 95/46/CE, que foi reiterado no RGPD, visando garantir a proteção de todas as pessoas singulares, independentemente da sua nacionalidade ou local de residência, como descrito nos considerandos 2 e 14 (Moniz, 2018).

1.2.2.1. Aplicação do critério relativo ao estabelecimento – artigo 3º nº 1

O art.º 3.º n.º 1 refere o seguinte *o presente regulamento aplica-se ao tratamento de 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.*

Com efeito, há aqui três expressões em controvérsia, "contexto de atividades", "estabelecimento" e "subcontratante".

O CEPD considera que, para efeitos do artigo 3.º, n.º 1, o significado de "tratamento no contexto das atividades" de um estabelecimento de um responsável pelo tratamento ou subcontratante deve ser entendido à luz da jurisprudência pertinente. Por um lado, *o significado de no contexto das atividades de um estabelecimento não pode ser interpretado de forma restritiva* (Acórdão TJUE, 2015). Por outro lado não deve haver uma interpretação demasiado ampla caindo no erro de que qualquer presença na União, por mais reduzidas que sejam as ligações que seja suficiente para se subsumir no âmbito de aplicação da legislação europeia. (Diretrizes 3/2018, 2018).

Lokke Moerel (2011) refere o caso das empresas multinacionais que tratam os dados pessoais de forma centralizada: se a empresa-mãe trata os dados dos recursos humanos de forma centralizada, numa base de dados única, das empresas do seu grupo situadas na UE, a autora defende que o regime de proteção de dados pessoais da UE aplicar-se-á a essas partes do tratamento de dados pessoais porque estão relacionados com as atividades dos seus estabelecimentos situados na EU.

Apesar de o legislador europeu não apresentar, no extenso artigo 4.º, uma definição de estabelecimento[19], fornece-nos importantes pistas no considerando 22: *o*

[19] O artigo 4.º/16 apenas define o que se entende por estabelecimento principal. Este conceito, central de dimensão regulatória do direito da proteção de dados fornece-nos poucas pistas no que ao conceito de estabelecimento respeita.

estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto (Cordeiro, 2020, p. 93).

No parecer emitido pelo GT29, este refere que se *os dados pessoais forem tratados por um responsável pelo tratamento dos dados que não esteja estabelecido em nenhum Estado-Membro, o tratamento é regido pela lei nacional do Estado-Membro em que se encontrem os meios ou os equipamentos utilizados por esse responsável para o tratamento* (Grupo de trabalho artigo 29º, 2016c).

Segundo as diretrizes 3/2018, o RGPD prevê a aplicação de disposições e de obrigações diferentes e específicas aos responsáveis pelo tratamento e aos subcontratantes[20]. Neste sentido, o CEPD refere designadamente que um subcontratante situado na UE não deve ser considerado um estabelecimento de um responsável pelo tratamento de dados na aceção do artigo 3.º n.º 1, simplesmente por força da sua condição de subcontratante em nome de um responsável pelo tratamento. (Diretrizes 3/2018, 2018).

Caso o responsável pelo tratamento que dá instruções ao subcontratante que também esteja situado na União, tal responsável pelo tratamento também terá de cumprir as obrigações que o RGPD impõe a responsáveis pelo tratamento. (Diretrizes 3/2018, 2018).

Não fica excluído da aplicação do RGPD, por força do artigo 3.º n.º 1, o tratamento de dados quando realizado por um responsável pelo tratamento apenas pelo facto de o responsável pelo tratamento solicitar a um subcontratante não estabelecido na União Europeia para efetuar tal tratamento em seu nome. Especifica, o RGPD, que este se aplica ao tratamento de todas as atividades situadas dentro da União Europeia, mesmo que esse tratamento ocorra dentro ou fora da União. Aquilo que desencadeia a aplicação do RGPD às atividades de tratamento de dados, é a presença de um responsável pelo tratamento de dados ou de um subcontratante na União Europeia, através de um estabelecimento, da

[20] Em conformidade com o artigo 28.º, o CEPD recorda que as atividades de tratamento efetuadas por um subcontratante em nome de um responsável pelo tratamento são reguladas por um contrato ou por outro ato normativo ao abrigo do direito da União ou de um Estado-Membro, sendo o mesmo vinculativo para o subcontratante no que se refere ao responsável pelo tratamento, e recorda ainda que os responsáveis pelo tratamento apenas devem recorrer a subcontratantes que ofereçam garantias suficientes no que toca à aplicação de medidas apropriadas para que o tratamento cumpra os requisitos do RGPD e garanta a proteção dos direitos dos titulares dos dados.

mesma forma que o facto do tratamento de dados ocorrer no contexto desse estabelecimento.[21] (Diretrizes 3/2018, 2018).

Sublinhe-se o caso Weltimmo, o TJUE partiu de uma *definição flexível do conceito de 'estabelecimento'. O TJUE considerou que um responsável pelo tratamento está estabelecido num Estado-Membro quando tem uma "atividade real e efetiva, mesmo que "mínima" que pode consistir na gestão de um sítio web imobiliário, relativamente a imóveis localizados nesse Estado-Membro, e redigido na língua desse mesmo Estado; em segundo lugar, a presença de um representante que serve como ponto de contacto, juntamente com outros elementos, como uma conta bancária ou uma caixa postal, também foram aspetos destacados pelo TJUE para verificar a existência de um estabelecimento.* Já no caso Amazon, o TJUE limitou-se a esclarecer que "*um estabelecimento não pode existir apenas porque o sítio web da empresa é acessível*" a partir de um determinado Estado-Membro (Moniz, 2018).

1.2.2.2. Aplicação do critério relativo ao direcionamento – artigo 3.º n.º 2

Segundo o disposto no artigo 3.º n.º 2 do RGPD:

O presente regulamento aplica-se ao tratamento de dados pessoais de titulares que se encontrem no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:

a) 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; ou

b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.

Nos termos do artigo 3.º n.º 2 a aplicação do critério relativo ao direcionamento no que se refere a titulares dos dados que se encontrem no território da União, pode ser desencadeada por atividades de tratamento realizadas por um responsável pelo tratamento ou subcontratante não estabelecido na União que englobem dois tipos de atividades

[21] Exemplo: uma empresa farmacêutica com sede em Estocolmo decidiu efetuar na sua sucursal, situada em Singapura, todas as suas atividades de tratamento de dados pessoais no atinente aos seus dados de ensaios clínicos. Neste caso, embora as atividades de tratamento ocorram em Singapura, esse tratamento é efetuado no contexto das atividades da empresa farmacêutica situada em Estocolmo, ou seja, por um responsável pelo tratamento de dados estabelecido na União. Assim sendo, as disposições do RGPD aplicam-se a esse tratamento, nos termos do artigo 3.º n.º 1.

distintos e alternativos, desde que tais atividades de tratamento digam respeito a titulares dos dados situados na União. Para ser aplicável ao tratamento efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, *o critério relativo ao direcionamento presta especialmente atenção àquilo com que estão "relacionadas" as "atividades de tratamento", e que deve ser analisado caso a caso* (Diretrizes 3/2018, 2018).

O CEPD entende que se deve encarar o critério relativo ao direcionamento com uma dupla abordagem, primeiramente, analisar se o tratamento diz ou não respeito a dados pessoais dos titulares situados na União Europeia, em segundo lugar verificar se esse tratamento está ou não relacionado com a oferta de bens e serviços ou com o controlo do comportamento dos titulares dos dados da UE (Diretrizes 3/2018, 2018).

Capítulo II - Princípios Norteadores

O RGPD estabelece um conjunto de princípios de respeito obrigatório no tratamento de dados pessoais. Na verdade, o dever de informar o titular dos dados pessoais ou ainda o direito de este solicitar o apagamento ou a retificação da informação não esgotam o leque de obrigações que, nos termos do RGPD recaem sobre o responsável pelo tratamento (Magalhães & Pereira, 2018).

É estabelecido pelo RGPD, no seu art.º 5 n.º 1, inúmeros princípios pelos quais se regem o tratamento de dados pessoais, sendo estes de consideração obrigatória.

O n.º 2 do art.º 5º atribui ao responsável pelo tratamento de dados as obrigações e responsabilidades no cumprimento dos princípios emanados no RGPD, ou seja, este para além de cumprir os princípios descritos no RGPD terá de o comprovar (princípio do *accountability*). Desta forma, implica, nomeadamente, a implementação de uma verdadeira política de *data governance* (Magalhães & Pereira, 2018).

Segundo Pinheiro e Gonçalves (2018), este documento legal deve ser a orientação pela qual os responsáveis de tratamento de dados pessoais devem reger o ser comportamento, uma vez que este atua com uma Constituição do RGPD.

2.1. Princípio da Licitude, Lealdade e Transparência

De acordo com o art.º 5º n.º 1 alínea a) os dados pessoais devem ser:

Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados.

O titular dos dados em causa deverão consentir o tratamento dos dados pessoais, tornando-se a base para que o tratamento seja lícito[22]. Assim exige-se que os dados pessoais sejam processados de forma lícita, para tanto o art.º 6.º n.º 1 do RGPD inclui seis fundamentos para o tratamento lícito de dados pessoais.

A licitude não depende apenas do cumprimento da legalidade na prossecução do tratamento de dados, está associada também à aplicação do art.º 52º da CDFUE [23]. Um

[22] Considerando 40 do RGPD.

[23] 1. Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.
2. Os direitos reconhecidos pela presente Carta, que se baseiem nos Tratados comunitários ou no Tratado da União Europeia, são exercidos de acordo com as condições e limites por estes definidos.

tratamento de dados lícito cumpre as disposições que regulam direitos e fundamentos de legitimidade, e cumpre igualmente, as exigências da Carta.

Tratando-se de um direito fundamental, o regime determina que:

- As restrições devem ser previstas por lei;
- Devem obedecer ao princípio da proporcionalidade;
- Devem corresponder a objetivos de interesse geral conhecidos pela UE (Pinheiro & Gonçalves, 2018, p. 207).

Existe a obrigatoriedade de determinar finalidades, explícitas e legítimas para a recolha dos dados pessoais, não podendo ser tratados, à posterior, de forma incompatível com essas finalidades (Magalhães & Pereira, 2018).

Relativamente ao anteriormente descrito, veja-se o seguinte acórdão do TJUE, Patrick Breyer contra a República Federal da Alemanha. Onde Patrick Breyer consultou vários sítios da internet, acessíveis ao público, dos serviços federais da Alemanha. Tendo como objetivo de se proteger de ataques e permitir que sejam aplicadas ações penais contra os responsáveis desses ataques, a maioria dos sítios dos serviços federais da Alemanha gravam todos os acessos em ficheiros de registo. No término da consulta de informação, ficam registados o nome do sítio ou do ficheiro consultado, o texto inserido nos campos de pesquisa, a hora e data da pesquisa, a quantidade de informação transferida, a indicação de que a pesquisa foi bem-sucedida e o endereço IP (Internet Protocol) do computador de onde foi efetuada a consulta (Acórdão TJUE, 2016).

Os endereços IP são identificações numéricas atribuídas a computadores ligados à internet de maneira a viabilizar a comunicação entre eles dentro dessa rede. O endereço IP de um computador quando acede a um sítio da internet, é enviado ao servidor onde está localizado o sítio consultado. Este processo acontece para que a informação que se pretende consultar possa ser transferida para o endereço correto.

Patrick Breyer intentou uma ação com o objetivo a que a República Federal da Alemanha seja condenada a abster-se de conservar, ou de mandar conservar por terceiros, os dados descritos, na medida em que a conservação destes não é necessária.

3. Na medida em que a presente Carta contenha direitos correspondentes aos direitos garantidos pela Convenção europeia para a proteção dos direitos do Homem e das liberdades fundamentais, o sentido e o âmbito desses direitos são iguais aos conferidos por essa convenção, a não ser que a presente Carta garanta uma proteção mais extensa ou mais ampla. Esta disposição não obsta a que o direito da União confira uma proteção mais ampla.

O tribunal entente que *embora seja verdade que o artigo 5.º da Diretiva 95/46 autoriza os Estados Membros a precisarem, dentro dos limites do capítulo II desta diretiva e, logo, do artigo 7.º da mesma, as condições em que os tratamentos de dados pessoais são lícitos, a margem de apreciação de que os Estados Membros dispõem, nos termos do referido artigo 5.°, só pode assim ser utilizada em conformidade com o objetivo prosseguido pela referida diretiva, que consiste em manter um equilíbrio entre a livre circulação dos dados pessoais e a proteção da vida privada* (Acórdão TJUE, 2016).

Os Estados-Membros não podem introduzir, ao abrigo do artigo 5.º da mesma diretiva, outros princípios relativos à legitimação dos tratamentos de dados pessoais além dos enunciados no artigo 7.° dessa diretiva nem alterar, através de exigências suplementares, o alcance dos seis princípios previstos no referido artigo 7.º, o artigo 7.º, alínea f), da Diretiva 95/46 deve ser interpretado no sentido de que se opõe a uma regulamentação de um Estado-Membro nos termos da qual um prestador de serviços de meios de comunicação em linha apenas pode recolher e utilizar dados pessoais de um utilizador desses serviços sem o consentimento deste na medida em que essa recolha e essa utilização sejam necessárias para permitir e faturar a utilização concreta dos referidos serviços por esse utilizador, sem que o objetivo de garantir o funcionamento geral desses mesmos serviços possa justificar a utilização dos referidos dados após o termo de uma sessão de consulta desses meios de comunicação (Idem, 2016).

Em conformidade com o artigo 7.º alínea f), da Diretiva 95/46, *o tratamento de dados pessoais é válido se for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do n.º1 do artigo 1.º desta diretiva*.

É importante reforçar que o Tribunal de Justiça afirmou que o art.º 7º da diretiva prevê uma lista taxativa dos casos em que o tratamento de dados pessoais pode ser considerado lícito, e que não se pode acrescentar novos princípios referentes à legitimação dos tratamentos de dados pessoais, nem prever exigências suplementares que possam alterar o alcance de qualquer dos princípios previstos nesse artigo.

Quanto ao princípio da lealdade *está essencialmente relacionada com o desenvolvimento dos tratamentos de dados pessoais com respeito por uma relação de equilíbrio entre responsáveis e subcontratantes e titulares dos dados pessoais. Pode*

manifestar-se de uma forma mais evidente em tratamentos de dados realizados por entidades públicas ou por empregadores (Pinheiro & Gonçalves, 2018, p. 207).

Segundo Magalhães e Pereira (2018) os dados devem ser tratados de forma adequada, pertinente e limitados ao necessário tendo em conta as finalidades para os quais são tratados, devem ser leais cingindo-se ao fim a que se destinam e não outro.

O princípio da transparência *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*[24]. Significando que as informações ou comunicações relativas ao tratamento de dados pessoais devem ser expressas numa linguagem clara e simples, de fácil acesso e compreensão. Logo, deverá ser garantido que as informações dos titulares dos dados relativos à sua identidade e os fins a que se destina o tratamento seja de fácil compreensão para os indivíduos.[25]

2.2. Princípio da Limitação do tratamento às finalidades

Segundo o art.º 5.º n.º 1 al. b):

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.

Alexandre Sousa Pinheiro (2015, p. 826) afirma que *o espaço do princípio da finalidade no direito a proteção de dados pessoais é crucial, na medida em que funciona como a primeira justificação para a realização de um tratamento de dados, impondo-se até ao consentimento. A realização de recolha de informação pessoal ou qualquer outra operação de tratamento deve estar respaldada numa razão-finalidade para, em função dela, se determinar a natureza necessária e não excessiva da informação pessoal*

[24] Considerando 39 do RGPD.
[25] Considerando 39, 58 e 59 do RGPD.

recolhida. A imposição do princípio da finalidade ao consentimento assenta na necessidade de proteger situações em que o primeiro esteja por natureza limitado.

Tendo por base as finalidades do n.º 1 do art.º 89.º, veja-se que a al.) b) do n.º 1 do art.º 5.º determina que não são considerados incompatíveis com as finalidades iniciais o tratamento cujo fim seja de arquivo de interesse público, investigação científica, históricos ou estatísticos.

De maneira que se possa avaliar se o tratamento posterior é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, o responsável pelo tratamento de dados deverá ter em consideração diversos fatores, tais como, a presença de uma relação entre a finalidade inicial e a finalidade do tratamento futuro pretendido, o contexto da recolha dos dados pessoais, particularmente no que respeita às expectativas razoáveis dos titulares dos dados quanto à sua posterior utilização, a natureza dos dados pessoais, com especial atenção para as categorias especiais de dados pessoais, eventuais consequências para o titular dos dados decorrente do tratamento posterior pretendido e existência de salvaguardas e garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas.

Ora, face ao exposto, tal princípio circunscreve os dados recolhidos devem obedecer a finalidades definidas, explícitas e legítimas, não podendo ser posteriormente tratadas de forma incompatível com essas finalidades. Portanto, este princípio adota uma importância fulcral tendo em conta que só depois de determinada a finalidade para o tratamento dos dados é possível aferir se a informação pessoal recolhida necessária e não excessiva. Portanto, é importante referir a impossibilidade de recolher dados para finalidades futuras tendo em conta que essas finalidades não foram definidas no momento da recolha.[26]

2.3. O princípio da minimização dos dados

Este princípio surge intrinsecamente associado ao princípio da limitação das finalidades (Cordeiro, 2020). Explica-nos o art.º 5.º n.º 1 al. c) do RGPD, que os dados pessoais são: *adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados*.

Já previsto na Diretriz n.º 95/46/CE, o princípio da minimização assume, no Direito vigente, contornos mais exigentes: a expressão "não excessivos", presentes na

[26] Considerando 39 e 50 do RGPD.

Diretriz n.º 95/46/CE, foi substituída por "limitados ao necessário" (Cordeiro, 2020, p. 158).

Alexandre Pinheiro (2015, p. 209) considera que *é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Segundo este princípio, os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios (dimensão da adequação do princípio da proporcionalidade em sentido amplo).*

Significa este princípio que os dados recolhidos devem ser adequados, pertinentes e limitados ao que foi determinado nas finalidades para o tratamento desses mesmos dados. O princípio da minimização, pressupõe que os dados pessoais utilizados serão apenas e tão só para a finalidade pretendida e não qualquer outra. Apenas podem ser tratados dados pessoais que não podem ser alcançados de forma razoável por outros meios. O responsável pelo tratamento dos dados deve proceder à fixação de prazos para o apagamento ou revisão periódica, por forma a que estes sejam conservados ao período mínimo e estritamente necessário[27].

Veja-se o seguinte Ac. TJUE, de 20 de Maio de 2003, Österreichischer Rundfunk e outros *qualquer tratamento de dados pessoais deve ser conforme, por um lado, aos "princípios relativos da qualidade dos dados, enunciados no artigo 6.º da diretiva e, por outro, a um dos princípios relativos à legitimidade do tratamento de dados (…) os dados devem ser "recolhidos para finalidades determinadas, explícitas e legítimas" (artigo 6.º, n.º 1, alínea b), da Diretiva 95/46/CE), bem como "adequados, pertinentes e não excessivos", relativamente a essas finalidades (artigo 6.º n.º 1, alínea c)). Além disso (…) o tratamento de dados pessoais é lícito, respetivamente, se "for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito" ou se "for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento (...) a quem os dados sejam comunicados.*

2.4. O princípio da exatidão

Conforme enuncia o art.º 5.º n.º 1 al. d) do RGPD, que os dados pessoais são:

[27] Considerando 39 RGPD.

Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora.

Resulta do considerando 39 do RGPD, e dito por outras palavras, este princípio deve ser implementado em todas as operações de tratamento e deve ser assegurada a integridade dos dados. Disto resulta que, quando intimado pelo titular desses dados, o responsável pelo tratamento de dados tenha no imediato, as ferramentas necessárias para o cumprimento da exatidão e a atualização dos dados incorretos, assim como o apagamento, ou retificação dentro de um prazo concebível.

Por conseguinte, permite-se afirmar que este princípio está intimamente relacionado com os direitos de acesso, de retificação dos dados e do seu apagamento, previstos nos arts.º 15.º, 16.º e 17.º.

A título exemplificativo vejamos o Ac. de 17 Julho de 2014, Middelburget que o TJUE considerou: (..) *que os princípios de proteção devem encontrar expressão, por um lado, nas obrigações que impendem sobre as pessoas (..) responsáveis pelo tratamento de dados, em especial no que respeita à qualidade dos dados, à segurança técnica, à notificação à autoridade de controlo, às circunstâncias em que o tratamento pode ser efetuado, e, por outro, nos direitos das pessoas cujos dados são tratados serem informadas sobre esse tratamento, poderem ter acesso aos dados, poderem solicitar a sua retificação e mesmo, em certas circunstâncias, poderem opor-se ao tratamento. Considerando que todas as pessoas devem poder beneficiar do direito de acesso aos dados que lhes dizem respeito e que estão em fase de tratamento, a fim de assegurarem, nomeadamente, a sua exatidão e a licitude do tratamento.*

2.5. Princípio da limitação da conservação

Segundo o RGPD, no seu art.º 5.º n.º 1 al. e), o princípio da limitação da conservação, os dados pessoais *são conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º n.º 1, sujeitos à aplicação das*

medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados.

Significa isto que os dados pessoais só devem ser conservados pelo período necessário à prossecução das finalidades do tratamento pelo que o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica[28].

A título de exemplo, veja-se o Ac. de 8 de abril de 2014 Digital Rights Ireland e Seitlinge, no processo C-293/12, onde o Supremo Tribunal da Irlanda foi chamado a intervir num litígio que opunha a Digital Rights às autoridades irlandesas a respeito da legalidade de medidas nacionais relativas à conservação de dados relativos a comunicações eletrónicas. O Tribunal declarou inicialmente que, as autoridades irlandesas, ao impor tais obrigações a estas entidades, as disposições da Diretiva 2006/24/CE constituíam uma violação grave no que respeita aos direitos fundamentais pela vida privada e à proteção dos dados pessoais garantidos pelos artigos 7.º e 8.º da Carta.

Considerou ainda que, foram ultrapassados os limites definidos pelo respeito do princípio da proporcionalidade, aquando da adoção da diretiva relativa à conservação de dados pelo legislador da União. Consequentemente, o Tribunal declarou a diretiva inválida, tendo por base que a diretiva em causa não garantia a limitação ao estritamente necessário, considerando que violava com gravidade os direitos fundamentais.

Por outro lado, o Tribunal declarou que a Diretiva 2006/24/CE não prevê garantias suficientes, tendo em conta as exigências resultantes do artigo 8.º n.º 3 da Carta, que permitam garantir uma proteção eficaz dos dados conservados contra qualquer tipo de acesso e uso ilícito. Não define regras específicas e ajustadas à quantidade de dados cuja conservação é imposta por esta diretiva, à sensibilidade destes dados e ao risco de acesso ilegítimo aos mesmos. Estas regras destinar-se-iam, a regular de forma clara e estrita a proteção e segurança dos dados em causa, com a finalidade de garantir a sua total integridade e confidencialidade.

2.6. Princípio da integridade e confidencialidade

O princípio da integridade e confidencialidade, segundo o art.º 5.º n.º 1 al. f) do RGPD, que os dados pessoais são:

[28] Considerando 39 do RGPD.

Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.

Deve ser garantida a devida segurança e confidencialidade aquando do tratamento de dados pessoais, do mesmo modo que deve ser garantida a segurança ao seu acesso e a equipamentos utilizados para o seu tratamento, e ainda a utilização dos mesmos por pessoas não autorizadas.

Deste modo, devem ser adotadas medidas de proteção, que garantam a segurança da rede e das informações contra possíveis acessos indevidos. É a capacidade destas medidas de proteção utilizadas pelas organizações para fazer face a eventos acidentais, a ações maliciosas ou ilícitas que poderão colocar em causa a integridade, a confidencialidade, a disponibilidade, e a autenticidade dos dados pessoais[29].

2.7. O princípio da responsabilidade

Enuncia o art.º 5.º n.º 2 do RGPD, que o responsável pelo tratamento de dados:

O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo.

É da responsabilidade do responsável pelo tratamento de dados executar as medidas que foram mais eficazes e adequadas, assim como de comprovar que o tratamento de dados está a ser executado em consonância com o determinado pelo RGPD. Todas as medidas executadas deveram estar em sintonia com o contexto e as finalidades para o tratamento de dados, e devem ter em conta o risco que possa acarretar para os direitos e liberdades dos titulares.

As organizações, quando recorrem a um subcontratante para confiar as atividades de tratamento de dados, devem recorrer a entidades que ofereçam garantias suficientes, essencialmente em termos de conhecimentos específicos e fiáveis por forma a assegurar a execução de medidas técnicas e organizativas que traduzam o cumprimento dos regulamentos, nomeadamente no que concerne à segurança do tratamento.[30].

O responsável pelo tratamento, segundo o art.º 4.º n.º 7 do RGPD entende-se como *a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento*

[29] Considerando 39 e 49 do RGPD.
[30] Considerando 79, 80 e 81 do RGPD.

sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.

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

2.8. Princípio do consentimento

O art.º 6.º n.º 1 do RGPD enuncia-nos os diferentes pressupostos que constituem as causas de licitude do tratamento, nomeadamente o consentimento.

De acordo, com o art.º 4.º n.º 11 do RGPD define o conceito de consentimento como *uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*.

Para que o consentimento[31] seja válido, o artigo 4.º n.º 11, do RGPD define que o consentimento do titular dos dados traduz-se numa demonstração de vontade livre, específica, informada e explícita, pela qual o titular dos dados aceita, sob declaração ou ato positivo inequívoco, que os dados a si respeitantes sejam objeto de tratamento (Parlamento Europeu, 2018).

O considerando 42 determina que *sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados.*

No artigo 7.º n.º 1, o RGPD descreve evidentemente a obrigação explícita que recai sobre o responsável pelo tratamento de demonstrar que o titular dos dados deu o seu consentimento. O ónus da prova recai sobre o responsável pelo tratamento, de acordo com o artigo 7.º n.º 1 (Parlamento Europeu, 2018, p. 23).

Para ser informado, o consentimento dever ser dado por pessoas que sejam competentes para consentir, que o façam de forma voluntária, estejam totalmente informadas sobre a pesquisa e tenham compreendido a totalidade do que lhe foi transmitido (Reynolds, 1979, p. 261).

[31] Na Diretiva 95/46/CE, o consentimento foi definido como *qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento*, devendo esse consentimento ser "dado de forma inequívoca" para que o tratamento dos dados pessoais seja legítimo [artigo 7.º, alínea a), da Diretiva 95/46/CE].

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

Um exemplo de um consentimento inválido no âmbito das comunicações eletrónicas, no Ac. do TJUE de 21 de março de 2019, Planet49 contra Bundesverband der Verbraucherzentralen und Verbraucherverbände, foi considerado o seguinte: *para participar num jogo promocional organizado pela Planet49, um utilizador da Internet deparou com duas menções antecedidas de quadrículas de seleção que tinha de selecionar ou desmarcar antes de poder acionar o «botão de participação». Uma das menções exigia que o utilizador aceitasse ser contactado por uma lista de empresas para efeitos de ofertas promocionais e a outra exigia o consentimento do utilizador para a instalação de cookies no seu computador (...).*

O consentimento para além de ser ativo deve também ser dado em separado, garantido assim que este é dado de forma livre, especifica, informada e explícita. Particularmente, no ponto de vista do titular dos dados, o consentimento não aparenta ser de natureza secundária. Estas ações devem ser exibidas em igualdade de condições. Por sua vez, parece ser questionável que um conjunto de manifestações de intenção, onde se encontra incluído o consentimento, esteja de acordo com o significado de consentimento ao abrigo da Diretiva 95/46/CE.

Neste contexto, para o titular dos dados deve ficar bem explícito se a atividade que prossegue na Internet está sujeito a um consentimento. Não deve existir margem para dúvida, sendo que o utilizador deve estar em posição de decidir em que medida está disposto a fornecer os seus dados pessoais para continuar a sua atividade na Internet.

Conforme o disposto no artigo 5.º n.º 3, e do art.º 2.º al. f), da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, conjugados com o art.º 2.º alínea h), da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, considera-se que não é dado um consentimento válido.

Capítulo III - Direitos dos titulares dos dados pessoais

3.1. Transparência das informações, das comunicações e das regras para o exercício dos direitos dos titulares dos dados

Os direitos dos titulares dos dados ficaram reforçados com o RGPD, da mesma forma que este veio conceder novos direitos para além daqueles que estavam previstos pela Diretiva 95/46/CE. O RGPD atribui ao titular dos dados novos direitos individuais, principalmente no que respeita à garantia de uma proteção jurídica mais eficaz.

Um dos elementos mais reconhecidos no direito da UE é a transparência. É uma questão de criar confiança nos processos que afetam os cidadãos, tornando-os compreensíveis e, se necessário, se oponham a esses processos. É uma expressão do princípio da lealdade em relação ao tratamento dos dados pessoais enunciado no artigo 8.º da CDFUE. Para além dos requisitos de que os dados pessoais devem ser tratados de forma lícita e leal, o RGPD nos termos do art.º 5º n.º 1 al. a) introduz agora a transparência como um aspeto fundamental desses princípios (Grupo Trabalho Artigo 29, 2016a).

O RGPD através do seu artigo 12.º define as regras para o exercício dos direitos dos titulares dos dados, desta forma obriga as entidades a procurar e implementar soluções técnicas que lhes garantam respostas atempadas aquando das solicitações dos titulares dos dados. Esta imposição é atribuída ao responsável pelo tratamento dos dados pessoais e subcontratantes.

Entre as várias regras, o responsável pelo tratamento de dados tem o compromisso de:

1. *Tomar as medidas adequadas para fornecer ao titular dos dados pessoais as informações e qualquer comunicação, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças;*
2. *Facilitar o exercício dos direitos do titular dos dados pessoais;*
3. *Fornecer ao titular as informações sobre as medidas tomadas, mediante pedido, sem demora injustificada e no prazo de um mês a contar da data da receção do pedido;*
4. *Informar sem demora, se não der seguimento ao pedido apresentado pelo titular dos dados, no prazo de um mês a contar da data da receção do pedido, das razões*

que o levaram a não tomar as medidas e da possibilidade de apresentar reclamação a uma autoridade de controlo e intentar ação judicial;

5. *Fornecer gratuitamente todas as informações quanto às comunicações e medidas tomadas. No entanto, tal pode ser afastado, e ser exigido o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações, e se os pedidos forem manifestamente infundados ou excessivos, pode recusar-se a dar seguimento ao pedido;*
6. *Solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados, quando houver dúvidas razoáveis quanto à identidade da pessoa singular que se apresenta;*
7. *Fornecer ao titular de dados pessoais, ícones normalizados a fim de dar, de uma forma facilmente visível, inteligível e legível, uma perspetiva geral significativa do tratamento previsto*[32]*.*

Repare-se que o RGPD, não cita a definição de transparência. No considerando 39 do RGPD é transmitida a informação quanto ao significado e ao efeito do princípio da transparência no contexto do tratamento de dados:

Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse 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 lhes dizem respeito que estão a ser tratados (Grupo de Trabalho Artigo 29, 2016a).

3.2. Direito de informação e de acesso

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

[32] Art.º 12.º RGPD.

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

O artigo 13.º do RGPD, por sua vez, menciona quais as informações que o responsável pelo tratamento de dados tem de fornecer ao titular dos dados aquando os dados pessoais são recolhidos junto do mesmo, tendo em conta que o titular dos dados deve ser informado de todos os tratamentos e finalidades por forma a que este seja feito de forma transparente e equitativo, deve ainda ser informado da identidade do responsável pelo tratamento, a identidade do encarregado de proteção de dados e seus contactos, a identidade dos destinatários dos dados e da referência às garantias adequadas e a forma de obter cópia das mesmas quando o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional.

Veja-se a título de exemplo, o Acórdão de 01 de outubro de 2015 do TJUE, que opôs Smaranda Bara contra a Agenţia Naţională de Administrare Fiscală (Agência Nacional de Administração Fiscal da Roménia) e a Casei Naționale de Asigurări de Sănătate (Casa Nacional de Segurança Social da Roménia), esclarece o direito à informação implementado pela Diretiva 95/46/CE.

In casu, foram comunicados dados pessoais entre as duas entidades romenas, sem que o titular dos dados pessoais em questão, Smaranda Bara tivesse consentido ou sequer sido previamente informado, quanto à legalidade da transmissão dos dados, relativamente aos rendimentos declarados para pagamento de contribuições em atraso para o regime de seguro de doença. Entende o tribunal que houve uma violação clara dos arts.º 10.º, 11.º e 13.º da D95.

Quando os dados pessoais não são recolhidos junto do titular, o responsável pelo tratamento deve comunicar ao titular dos dados as informações elencadas no artigo 14.º do RGPD, designadamente a identidade e os contactos do responsável pelo tratamento, os contactos do encarregado de proteção de dados, as finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento, as categorias dos dados pessoais em questão, os destinatários ou categorias de destinatários dos dados, assim como, a intenção de transferência de dados pessoais para um país terceiro ou uma organização internacional e a existência ou não de uma decisão de adequação adotada pela Comissão.

Por outro lado, existem isenções, que estão previstas nos arts.º 13.º n.º4, 14.º n.º 5, do RGPD, quando o titular dos dados já detiver todas as informações não se aplica a

obrigação de informar, ou quando os dados não tiverem sido obtidos a partir do titular dos dados e a prestação de informações for impossível ou desproporcionada, designadamente quando os dados são tratados com finalidade de interesse público, de investigação científica ou histórica ou com objetivos estatísticos.

Por sua vez, o direito de acesso está previsto no art.º 15.º do RGPD e no n.º1 do art.º 35.º da CRP. Este consiste na capacidade do titular dos dados saber se estão a ser tratados dados pessoais, ou não, que a si respeitem, saber se os seus dados foram transmitidos para outra entidade ou que destino lhes foi dado, e ainda a capacidade de poder aceder aos seus dados e a todas as informações referentes às operações de tratamento dos mesmos.

O contexto deste direito não se limita apenas ao acesso aos dados, o titular pode solicitar a confirmação da existência, ou não, do tratamento dos dados e um conjunto de informações acessórias que concorra, em larga medida, com aquela que dever acompanhar a notificação, ao abrigo do direito à informação (Coutinho & Moniz, 2018).

3.3. Direito de retificação

O direito de retificação encontra-se previsto no art.º 16.º do RGPD. Consubstancia-se no *direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional*.

O direito de retificação (e atualização) de dados pessoais não aparece com o RGPD, o mesmo já se encontrava previsto na CRP, nomeadamente no seu art.º 35º, aqui esta definido que é atribuída a possibilidade, a todos os cidadãos, de exigirem a retificação e atualização dos dados informatizados que a si respeitem.

Quanto ao alcance do direito de acesso e retificação, analisemos o seguinte acórdão do TJUE de 20 de dezembro de 2017, P. Nowak contra Data Protection Commissioner.

Entende o tribunal *(...) há que considerar que o facto de conferir ao candidato um direito de acesso a essas respostas e a essas anotações, nos termos do artigo 12.º, alínea a), desta diretiva, serve o objetivo desta última, que consiste em garantir a proteção do direito à vida privada desse candidato relativamente ao tratamento dos dados que lhe dizem respeito e tal independentemente da questão de saber se o*

referido candidato dispõe ou não de tal direito de acesso igualmente ao abrigo da legislação nacional aplicável ao procedimento de exame.

Neste contexto há que recordar que a proteção do direito fundamental ao respeito da vida privada implica, designadamente, que qualquer pessoa singular possa assegurar-se de que os dados pessoais que lhe dizem respeito são exatos e que são tratados de forma lícita. Como resulta do considerando 41 da Diretiva 95/46, é para poder efetuar as verificações necessárias que a pessoa em causa dispõe, em virtude do artigo 12.º, alínea a), da mesma, de um direito de acesso aos dados que lhe digam respeito que são objeto de tratamento. Esse direito de acesso é necessário, designadamente, para permitir à pessoa em causa obter, se for caso disso, por parte do responsável pelo tratamento, a retificação, apagamento ou bloqueio desses dados e, por conseguinte, exercer o direito previsto no artigo 12.º alínea b), da referida diretiva.

(...) *por um lado, que os direitos de acesso e de retificação, ao abrigo do artigo 12.º alíneas a) e b), da Diretiva 95/46, não se estendem às questões do exame, que não constituem, enquanto tais, dados pessoais do candidato e por outro lado, tanto a Diretiva 95/46 como o Regulamento 2016/679 que a substitui preveem certas limitações a esses direitos.*

Conclui o tribunal que *tanto a Diretiva 95/46 como o Regulamento 2016/679 que a substitui preveem certas limitações a esses direitos. Assim, nos termos do artigo 13.° n.º 1, alínea g), da Diretiva 95/46, os Estados-Membros podem tomar medidas legislativas destinadas a restringir o alcance das obrigações e direitos referidos, sempre que tal restrição constitua uma medida necessária à proteção da pessoa em causa ou dos direitos e liberdades de outrem.*

3.4. Direito ao apagamento

O n.º 1 do art.º 17.º confere aos titulares dos dados pessoais o direito de solicitarem que os dados pessoais que lhes dizem respeito sejam apagados, criando assim nos responsáveis ou nos subcontratantes a obrigação de o fazer.

O RGPD atribui o direito aos cidadãos que os dados que lhe digam respeito sejam retificados ou apagados quando a conservação desses dados violar o regulamento ou o direito da União. Desta forma, deixam de ser objeto de tratamento se a necessidade pelo

qual foram recolhidos ou tratados deixa de existir, garantindo o direito a serem esquecidos[33].

Não obstante este direito do titular dos dados, encontramos limitações para exercer esse direito. Por conseguinte, o direito ao apagamento dos dados pessoais é possível se:

a. Os dados deixam de ser necessários para as finalidades pelo qual foram recolhidos ou tratados;
b. O titular dos dados retirar o consentimento (art.º 6.º n.º 1 al. a) ou (art.º 9.º n.º 2 al. a), quando o tratamento for necessariamente fundamentado neste e não exista outro fundamento legal para o tratamento dos dados;
c. O titular dos dados se opuser ao tratamento, nos termos do art.º 21.º n.º 1, e o responsável pelo tratamento não demonstrar que existam interesses legítimos prevalecentes que justifiquem o tratamento, conforme o art.º 21.º n.º 2;
d. Os dados foram tratados ilicitamente;
e. O apagamento dos dados for necessário para o cumprimento de uma obrigação legal a que o responsável pelo tratamento esteja sujeito;
f. Os dados foram recolhidos numa oferta de serviços da sociedade de informação a crianças com menos de 16 anos, sem o consentimento dado por quem exerce as responsabilidades parentais (art.º 8.º n.º 1).

Mesmo que o titular dos dados tenha na posse um dos fundamentos para o apagamento dos dados referidos anteriormente, o n.º 3 do art.º 17.º do RGPD acrescenta que é importante averiguar se os dados são necessários para o responsável pelo tratamento ou subcontratante, isto é, se os dados que se pretende apagar são necessários ao exercício do direito à liberdade de expressão e de informação, ao cumprimento de uma obrigação legal de um Estado-Membro, ao exercício de funções de interesse público ou exercício da autoridade pública, a fins de saúde pública, a fins de arquivo, investigação ou estatística ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial. Ocorrendo alguma das situações referidas, o direito ao apagamento pode não ser executado pelo responsável pelo tratamento.

A este propósito, veja-se o Ac. de 13 de maio de 2014 Google Spain SL, contra Agencia Española de Protección de Datos (Agência Espanhola de Proteção de Dados), No referido caso, Mario Costeja González ao fazer uma pesquisa pelo seu nome no motor de busca Google Spain, reparou que a lista de resultados exibia ligações para duas páginas

[33] Considerando 65 do RGPD.

do jornal diário da "La Vanguardia", que anunciavam, uma venda de imóveis em hasta pública organizada na sequência de um arresto destinado a cobrar as dívidas de Mario Costeja González à Segurança Social.

Entende o TJUE, que o operador de um motor de busca *"recolhe" esses dados, que "recupera", "regista" e "organiza" posteriormente no âmbito dos seus programas de indexação, "conserva" nos seus servidores e, se for caso disso, comunica e "coloca à disposição" dos seus utilizadores, sob a forma de listas de resultados das suas pesquisas. Na medida em que estas operações estão explícita e incondicionalmente referidas no artigo 2.° al. b), da Diretiva 95/46, devem ser qualificadas de "tratamento*.

(..) *Há que considerar que, tendo em conta o caráter sensível, para a vida privada dessa pessoa, das informações contidas nesses anúncios e o facto de a sua publicação inicial remontar há 16 anos, a pessoa em causa tem comprovadamente direito a que essas informações já não sejam associadas ao seu nome através dessa lista. Por conseguinte, na medida em que, no caso em apreço, não parece haver razões especiais que justifiquem um interesse preponderante do público em ter acesso a essas informações no âmbito dessa pesquisa, o que, todavia, cabe ao órgão jurisdicional de reenvio verificar, a pessoa em causa pode, ao abrigo dos artigos 12.° al. b), e 14.°, primeiro parágrafo, alínea a), da Diretiva 95/46, exigir a supressão das referidas ligações dessa lista de resultados*.

Em entendimento contrário, veja-se veja-se o Ac. de 9 de março de 2017 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce Contra Salvatore Manni ao qual em 12 de dezembro de 2007, S. Manni propôs uma ação contra a Câmara de Comércio de Lecce, ao qual alega que os imóveis desse complexo não se vendiam por resultar do registo das sociedades que ele tinha sido o administrador único e o liquidatário da Immobiliare e Finanziaria Salentina Srl, cuja falência tinha sido declarada em 1992, e que essa sociedade tinha sido cancelada do registo das sociedades, na sequência de um processo de liquidação, em 7 de julho de 2005.

Neste caso o tribunal começa por evidenciar que a publicidade dos registos das sociedades tem por finalidade garantir a segurança jurídica nas relações entre as sociedades e os terceiros, assim como proteger os interesses dos terceiros em relação às sociedades tendo em conta que estas apenas oferecem como garantia em relação a terceiros o seu património social. Além disso, o tribunal afirma, que podem ocorrer quesitos que obriguem a necessidade de dispor dos dados pessoais que se encontram no registo das sociedades mesmo vários anos após uma sociedade ter deixado de existir.

O Tribunal considera que esta ingerência nos direitos fundamentais das pessoas em causa (designadamente, o direito ao respeito da vida privada e o direito à proteção dos dados pessoais) não é desproporcionada na medida em que *1) apenas um número limitado de dados pessoais está inscrito no registo das sociedades e 2) justifica-se que as pessoas singulares que optem por participar nas trocas comerciais por intermédio de uma sociedade por ações ou de uma sociedade por quotas e que apenas oferecem como garantia perante terceiros o património dessa sociedade sejam obrigados a tornar públicos os dados que se referem à sua identidade e às suas funções nesta*.

No caso anteriormente referido, o Tribunal acaba por considerar que, por si só, as circunstâncias alegadas por S. Manni não basta para justificar uma limitação do acesso de terceiros a esses dados, tendo em conta, nomeadamente, o interesse legítimo deste de disporem desses dados.

3.5. Direito à limitação do tratamento

Prevê o art.º 18.º do RGPD, o direito à limitação do tratamento, donde o titular dos dados terá o direito à limitação do tratamento de dados que lhe digam respeito, e aplica-se as seguintes situações:

a. A contestação da exatidão dos dados que lhe dizem respeito, durante um período que permita ao responsável pelo tratamento apurar a sua exatidão;
b. O titular dos dados se opuser ao apagamento dos mesmos em caso de ilicitude no tratamento, e em contrapartida, solicitar a limitação dos mesmos;
c. Já não ser necessário o tratamento dos dados pessoais pelo responsável pelo tratamento, no entanto esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
d. Até se verificar, no caso de oposição ao tratamento nos termos do artigo 21.º n.º 1, que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados[34].

Afirmar que se trata de um direito que surge *ex novo* com o RGPD será incorreto, sendo que já se previsto na alínea b), do art.º 12.º da Diretiva 95/46/CE, de 24 de outubro de 1994.[35]

[34] Cfr. n.º1 do art.º 18.º do RGPD.
[35] O direito de limitação ao tratamento constituía um elemento integrante do direito de acesso. Era a possibilidade dada aos titulares dos dados de pedirem o bloqueio dos seus dados pessoais nas situações em que o tratamento não cumprisse com o disposto na Diretiva 95/46/CE, nomeadamente devido ao caráter incompleto ou inexato desses dados pessoais.

O efeito da limitação por sua vez, não tem implicações na conservação dos dados, mas afeta todas as restante operações de tratamento que só podem ser realizadas excecionalmente, nas situações previstas no art.º 18.º nº2 (Coutinho & Moniz, 2018).

Estabelece o n.º 2 do art.º 18.º do RGPD que, *quando o tratamento tiver sido limitado nos termos do n. º 1, os dados pessoais só podem, à exceção da conservação, ser objeto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro*. Será importante frisar que deverá ser informado pelo responsável pelo tratamento de dados, o titular que tenha adquirido a limitação dos seus dados com base num dos requisitos do n.º 1 do art.º 18º, antes de anular a limitação ao referido tratamento de dados previsto no n.º 2 do mesmo artigo.[36]

3.6. Direito à portabilidade dos dados

O direito à portabilidade dos dados pessoais vem consagrado no art.º 20.º do RGPD. O titular de dados pessoais, neste contexto, pode aceder aos seus dados e pedir que sejam transferidos para outro serviço, sempre que os dados pessoais sejam tratados de forma automatizada.

É com o objetivo de dar mais poderes aos titulares dos dados pessoais que surge o novo direito à portabilidade dos dados, uma vez que possibilita a sua capacidade para transferir, copiar ou transmitir facilmente dados pessoais de uma plataforma informática para outra (Grupo de Trabalho Artigo 29, 2016b).

O titular de dados pessoais *deverá ser autorizado a receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento num formato estruturado, de uso corrente, de leitura automática e interoperável, e a transmiti-los a outro responsável*[37].

É na relação entre o titular dos dados e o responsável pelo tratamento que se centra o direito à portabilidade de dados pessoais. É direito do titular dos dados solicitar os dados fornecidos ao responsável pelo tratamento, num formato organizado, de uso corrente e de leitura automática, e este os fornecer a outro responsável pelo tratamento ou de os

[36] Cfr. determinado pelo n.º 3 do art.º 18.º do RGPD.
[37] Considerando 68 do RGPD.

transferir para as suas próprias de armazenamento, sem que o responsável pelo tratamento o possa negar (Comissão Europeia, 2019).

O GT29 refere as três condições cumulativas para a aplicabilidade deste direito. Em primeiro lugar, *os dados pessoais solicitados devem ser tratados por meios automáticos, com base no consentimento prévio do titular dos dados*. Em segundo lugar, *os dados pessoais solicitados devem dizer respeito ao titular dos dados e ser fornecidos pelo mesmo*. Por último, na terceira condição, *o exercício deste novo direito não deve prejudicar os direitos e as liberdades de terceiros* (Grupo Trabalho Artigo 29, 2016b).

O art.º 20.º n.º 2, obriga aos responsáveis pelo tratamento a transmissão os dados transferíeis diretamente para outros responsáveis pelo tratamento "sempre que tal seja tecnicamente possível".

Este direito tem como objetivo obter, reutilizar e transmitir os dados entre diferentes serviços e para os seus próprios fins, com isso *espera-se que a portabilidade dos dados promova oportunidades de inovação e de partilha segura de dados pessoais entre os responsáveis pelo tratamento sob o controlo do titular dos dados* (Grupo Trabalho Artigo 29, 2016b, p. 6).

3.7. Direito de Oposição

O direito à oposição encontrava-se previsto no artigo 14.º da Diretiva 95/46/CE, sendo que o regulamento no seu artigo 22.º não introduziu grandes inovações, veja-se o art.º 21º nº 1 do RGPD:

O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.º n.º1 alínea e) ou f), ou no artigo 6.º n.º4, incluindo a definição de perfis com base nessas disposições.

Este direito de oposição não se considera aplicável se o responsável apresentar uma ponderação de interesses em que invoque *razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial." Trata-se dos requisitos de aplicação de interesse legítimo como fundamento de legitimidade para o tratamento de dados pessoais*.[38]

[38] Artigo 21.º nº1 segunda parte do RGPD.

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

O titular dos dados deverá ser informado da hipótese de exercer o seu direito à oposição, devendo este direito ser apresentado de modo "claro e distinto de quaisquer outras informações"[39]. Desta forma, o titular dos dados deverá ser explicitamente chamado à atenção para este direito, deve ser apresentado de modo claro, conciso e diferenciado de quaisquer outras informações.

No acórdão do TJUE de 13 de maio de 2014, Google Spain e Google, o tribunal precisou o alcance dos direitos de acesso e de oposição ao tratamento de dados pessoais na Internet, previstos pela Diretiva 95/46/CE.

Assim, aquando da questão do alcance da responsabilidade do operador de um motor de busca na internet, o Tribunal declarou a este respeito, que para garantir o direito de acesso e oposição disposto nos arts.º 12.º, al. b), e 14.º al. a) da Diretiva 95/46/CE, e desde que as condições que aqui estejam reunidas, este por sua vez é obrigado a suprimir da lista de resultados, exibido na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a páginas web publicadas por terceiros e que contenham informações sobre essa pessoa.

No entendimento do tribunal essa obrigação legal pode também existir no pressuposto de esse nome ou de essas informações não serem prévia ou concomitantemente apagadas dessas páginas web, isto, se for caso disso o conteúdo referido nessas páginas seja lícito.

Por outro lado, questionado o tribunal sobre se a diretiva permite que os titulares em causa possam solicitar que as ligações a páginas web sejam apagadas de uma lista de resultados tendo por base a intenção de que as informações que figuram relativas ao titular sejam "esquecidas" após determinado período de tempo, o tribunal, evidencia, que primeiramente mesmo um tratamento de dados exatos que inicialmente é lícito pode tornar-se, com o tempo, incompatível com esta diretiva quando esses dados deixam de ser necessários tendo em conta as finalidades para os quais foram recolhidos ou tratado,

[39] Considerando 70 do RGPD.

nomeadamente, quando são inadequados, quando já não são pertinentes ou quando são desmedidos às finalidades inicialmente previstas.

Portanto, caso se conclua, no seguimento de um pedido da pessoa em causa, que a inclusão dessas ligações na lista é, na situação atual, incompatível com a diretiva, as informações e ligações que figuram nesta lista devem ser suprimidas. Neste contexto, a constatação de um direito da pessoa em causa a que a informação sobre a sua pessoa deixe de ser associada ao seu nome através de uma lista de resultados não presume que a introdução dos dados em questão na lista de resultados prejudique a pessoa em questão.

Por fim, o Tribunal indicou que, na medida em que a pessoa em causa pode, tendo em conta os seus direitos fundamentais ao abrigo dos artigos 7.º e 8.º da Carta, requerer que os dados em questão deixem de estar visíveis ao público em geral através da sua introdução numa lista de resultados desta espécie, em princípio, esses direitos prevalecem sobre o interesse económico da entidade (motor de busca), assim como sobre o interesse público em encontrar os dados refentes ao titular em questão durante uma pesquisa.

No entanto, não configura, se for o caso disso, por razões especiais, que o papel desenvolvido por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada o acesso aos referidos dados pelo interesse preponderante do público referido.

Capítulo IV - Âmbito da Responsabilidade

Uma das principais características que o RGPD apresenta é a integração do princípio da responsabilidade, estabelecendo expressamente no art.º 24.º do RGPD que, *tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis,* cabe ao responsável pelo tratamento aplicar *as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o Regulamento* (Coutinho & Moniz, 2018, p. 52).

4.1. Princípio da Responsabilidade

Nos termos do art.º 24.º do RGPD, veja-se:

Nº1: Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

Nº2 Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o n.º1 incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento.

Logo à partida, o n.º 1 atribui, ao responsável pelo tratamento, duas obrigações indissociáveis. A primeira é a obrigação de aplicação das medidas técnicas e organizativas adequadas por forma a poder assegurar e comprovar que o tratamento é executado em conformidade com o RGPD, tendo em conta a natureza, o âmbito, o contexto, as finalidades do tratamento dos dados, os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, e a eficácia das medidas (Pinheiro & Gonçalves, 2018, p. 396).

A segunda obrigação é a de revisão e atualização dessas medidas técnicas e organizativas, consoante as necessidades. O critério das necessidades que pode implicar

a revisão e atualização das medidas fica a cargo do responsável do tratamento (Pinheiro & Gonçalves, 2018, p. 397).

Por responsável pelo tratamento entende-se, nos termos do artigo 4.º n.º 7 *a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo, que, individualmente ou em conjunto, determine as finalidades e os meios de tratamento dos dados pessoais* (Cordeiro, 2020, p. 307).

Relativamente às obrigações que incidem sobre o responsável pelo tratamento e subcontratante, é importante referir que o RGPD adotou a chamada "abordagem baseada no risco". Este raciocínio vai para além de uma estrita "abordagem baseada no risco", tendo em conta todo o potencial ou real efeito adverso avaliado numa escala abrangente, desde o impacto no titular dos dados em questão ao impacto geral na sociedade (por exemplo, a perda de confiança social) (Coutinho & Moniz, 2018).

Segundo Coutinho e Moniz (2018, p. 51) *poderão existir diferentes níveis de obrigações e responsabilidades dos responsáveis pelo tratamento e subcontratantes, dependendo do grau de risco colocado pelo tratamento em questão para os titulares dos dados e para a sociedade. Assim, a necessidade de implementação pelos responsáveis pelo tratamento de medidas técnicas e organizativas que assegurem o cumprimento das regras de proteção de dados poderá variar consoante o tipo de tratamento de dados e os respetivos riscos para os titulares dos dados. Isto significa que um responsável pelo tratamento que realiza um tratamento de dados com um nível de risco relativamente baixo pode não estar vinculado às mesmas obrigações legais que são aplicáveis a um responsável cujo tratamento representa um elevado risco.*

4.2. Os princípios *data protection by design e by default*

Do RGPD, e associado ao princípio da responsabilidade, advêm ainda dois novos princípios fundamentais que devem orientar os processos de tratamento de dados pessoais: a proteção de dados desde a conceção (*data protection by design*) e a proteção de dados por defeito (*data protection by default*) (art.º 25.º do RGPD) (Coutinho & Moniz, 2018, p. 55).

Numa aceção ampla, a expressão *privacy by design* é usualmente entendido como conjunto de medidas técnicas, princípios e linhas orientadoras introduzidas *ab initio* nos sistemas que realizam tratamentos de dados pessoais, com o propósito de proteger de forma mais efetiva os direitos dos titulares dos dados (Cordeiro, 2020, p. 326).

Adicionalmente, de acordo com o princípio *data protection by default*, o responsável pelo tratamento deverá assegurar que só sejam tratados os dados pessoais que forem estritamente necessários para cada finalidade específica de tratamento (minimização do tratamento de dados pessoais). *Esta obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em particular, o responsável pelo tratamento deverá aplicar medidas técnicas e organizativas que garantam que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares* (art.º 25.º n.º 2 do RGPD) (Coutinho & Moniz, 2018, p. 57).

Assim sendo, ao optar por incluir os conceitos de data protection by design e by default como princípios-chave do RGPD, o legislador europeu visou assegurar que a proteção de dados representa uma componente fundamental na conceção e manutenção dos sistemas de informação e no modus operandi de cada organização (Coutinho & Moniz, 2018, p. 57).

A defesa dos direitos e liberdades das pessoas singulares em relação ao tratamento dos seus dados pessoais obriga as entidades à adoção de medidas técnicas e organizativas adequadas, por forma a garantir a execução dos requisitos do regulamento, conforme previsto no considerando 78. Deverão ser adotadas orientações internas, pelo responsável pelo tratamento, e aplicadas medidas que respeitem os princípios da proteção de dados desde a conceção e da proteção de dados por defeito. Medidas estas que devem introduzir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais, a capacidade de o titular dos dados controlar o tratamento de dados, a transparência no que concerne a todo o processo de tratamento de dados e a possibilidade de o responsável pelo tratamento criar medidas de segurança e melhorar as mesmas.

4.3. O Subcontratante

Segundo o art.º 28.º n.º 1 do RGPD, *quando o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular de dados*.

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

Na diretiva de proteção de dados, nomeadamente pelo art.º 2.º al. e), o subcontratante é definido como alguém que trata dados pessoais por conta do responsável pelo tratamento (Conselho da Europa, 2014, p. 54). Com este regulamento, independentemente de o responsável pelo tratamento dos dados continuar a ser responsável pelo cumprimento das regras de proteção de dados pessoais, é imposto ao subcontratante uma série de deveres que, até agora, não estava previsto, tais como a obrigatoriedade de registo das atividades de tratamento (art.º 30.º, n.º 2), a garantia da segurança no tratamento dos dados (art.º 32.º) ou a nomeação de EPD (art.º 37.º).

O Regulamento preceitua ainda que os subcontratantes são responsabilizados pelo incumprimento das regras do RGPD, nos termos previstos no art.º 82.º, se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento, podendo, inclusivamente, ficar sujeitos ao pagamento das coimas previstas no art.º 83.º do RGPD.

Segundo (Cordeiro, 2020, p. 309) o responsável pelo tratamento apenas pode recorrer nos termos do art.º 28.º nº 1 do RGPD, a subcontratantes que ofereçam garantias suficientes em termos de conhecimentos especializados, fiabilidade e recursos, de execução das medidas técnicas e organizativas adequadas de forma a cumprir as exigências do RGPD. A conformidade com estas exigências pode ser comprovada através da demonstração do cumprimento dos códigos de conduta ou dos procedimentos da certificação mencionados, respetivamente, nos arts.º 40.º e 42.º.[40]

O cumprimento dos requisitos do Regulamento e a garantia do exercício efetivo dos direitos dos titulares dos dados no âmbito da relação de subcontratação deve iniciar-se aquando da escolha do subcontratante, através da verificação de que a externalização das operações de tratamento permitirá ao responsável pelo tratamento assegurá-los (Pinheiro & Gonçalves, 2018).

O subcontratante é um mandatário[41] do responsável pelo tratamento, ele atua por conta deste último. O subcontratante será ainda, por maioria de razão, titular de uma

[40] Cfr. art.º 28.º nº5.

[41] Artigo 1157.º do CC: "Mandato é o contrato pelo qual uma das partes se obriga a praticar um ou mais atos jurídicos por conta de outra".

posição fiduciária, está obrigado a atuar sempre no melhor interesse do beneficiário da relação, o responsável pelo tratamento (Cordeiro, 2020, p. 309).

É regulada por contrato[42] a relação estabelecida entre o responsável pelo tratamento e o subcontratante, podendo as partes recorrer a cláusulas contratuais padronizadas para o efeito.

A norma do n.º 10 art.º 28.º constitui um corolário da atribuição de responsabilidades com base na concreta influência no tratamento de dados, ou seja, se o subcontratante agir como responsável pelo tratamento será o responsável pelo tratamento. A consideração do subcontratante como responsável pelo tratamento não prejudica os termos do direito à indemnização e a aplicação de coimas e sanções, previstos nos arts.º 82.º, 83.º e 84.º.

Significa que o regulamento pretendeu, por um lado, assegurar a imputação das responsabilidades coerente com a influência efetiva no tratamento e, por outro lado, salvaguardar a aplicabilidade dos mencionados artigos, cuja aplicação não é prejudicada em função da convolação do estatuto de subcontratante em responsável pelo tratamento (Pinheiro & Gonçalves, 2018, p. 441).

Quanto ao âmbito da responsabilidade os subcontratantes ao contrário do que se verifica com os responsáveis, apenas podem ser responsabilizados por duas situações concretas:

I. Por violação de obrigações decorrentes do RGPD que lhe sejam especificamente dirigidas;
II. Por incumprimento das instruções lícitas recebidas pelo responsável pelo tratamento (Cordeiro, 2018b, p. 14).

O grosso das obrigações específicas dos subcontratantes encontra-se nos arts.º 28.º, 29.º, 32.º, 37.º e 38.º.

A violação de um destes preceitos permite que o lesado faça uso do mecanismo da responsabilidade civil previsto no art.º 82.º do RGPD. (Cordeiro, 2018b). O Regulamento define que os subcontratantes são responsabilizados pelo incumprimento das regras do RGPD, nos termos previstos no art.º 82.º, *se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo*

[42] Art.º 28.º nº 3 do RGPD.

tratamento, podendo, inclusivamente, ficar sujeitos ao pagamento das coimas previstas no art.º 83.º do RGPD.

4.4. Encarregado de Proteção de Dados

Surge uma nova categoria de profissional, com a introdução do RGPD, dirigida fundamentalmente ao tratamento de dados pessoais: *Isso essencialmente cria uma profissão, talvez uma das várias novas profissões e carreiras relacionadas a questões de proteção de dados e o novo regime de proteção de dados. Isso enfatiza a nova importância atribuída aos dados pessoais* (Lambert, 2017, p. 37).

Este ponto tratarei com mais detalhe no capítulo VII.

4.5. Autoridade para o Controlo

Constitui um elemento essencial da proteção das pessoas singulares no que respeita ao tratamento dos seus dados pessoais[43], a criação de autoridades de controlo[44] nos Estados-Membro, sendo uma forma de os mesmos estarem habilitados a desempenhar as suas funções e a exercer os seus poderes com total independência.

Por sua vez, relativamente às autoridades de controlo, umas das alterações estruturais do RGPD prende-se com o modelo de supervisão: o controlo "ex ante" é substituído pela fiscalização "ex post", eliminando-se assim a supervisão prévia dos tratamentos de dados pessoais e transferindo a intervenção administrativa para o plano de orientação das condutas e, essencialmente, para o plano do controlo à posteriori dos tratamentos de dados pessoais (Calvão, 2018, pp. 37 e ss.).

Ainda neste sentido, Alexandre Sousa Pinheiro (2018), *a transformação do modelo de supervisão e o papel das autoridades nacionais de controlo na matéria da proteção de dados foi das maiores novidades do RGPD*. A ratio desta opção legislativa vem plasmada no considerando 89, onde se explica que a supervisão prévia, através de uma *obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo*.

Existe uma necessidade de criação de autoridades de controlo independentes ao abrigo do direito nacional, com a finalidade de garantir uma eficaz proteção de dados. As

[43] Considerando 117 do RGPD.

[44] Nos termos do art.º 4º do RGPD, entende-se por autoridade de controlo, uma autoridade pública independente criada por um Estado-Membro nos termos do art.º 51º do mesmo diploma.

ACI agem com *total independência na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos nos termos do regulamento.*[45]

Os membros das ACI *devem possuir habilitações, experiência e conhecimentos técnicos necessários, nomeadamente no domínio da proteção de dados*.[46]

Por seu turno, estas autoridades de controlo devem desempenhar funções especificas, entre elas:

- Fiscalizar e promover a proteção de dados a nível nacional;
- Aconselhar as pessoas em causa e os responsáveis pelo tratamento, bem como o Governo e o público em geral;
- Apreciar queixas e auxiliar as pessoas em causa que aleguem violações dos seus direitos à proteção de dados;
- Supervisionar os responsáveis pelo tratamento e os subcontratantes; intervir, se necessário:
    - Dirigindo advertências ou censuras aos responsáveis pelo tratamento e subcontratantes ou aplicando-lhes uma multa;
    - Ordenando a retificação, bloqueio ou apagamento dos dados;
    - Proibindo o tratamento;
- Reencaminhar casos para o tribunal (Conselho da Europa, 2014).

Integrado no âmbito do direito da EU, foram descritas no artigo 28.º n.º 1 da diretiva de proteção de dados as competências e a estruturas organizativa das autoridades de controlo. A AEPD é criada pelo Regulamento de Proteção de Dados, a autoridade de controlo do tratamento de dados pelos órgãos e instituições da EU. É com base na experiência adquirida desde a promulgação da Diretiva de Proteção de Dados, que este Regulamento descreve as funções e responsabilidades da autoridade de controlo.

O n.º 2 do artigo 16.º do TFUE e o n.º 3 do artigo 8.º da Carta garantem a independência das autoridades de controlo de proteção de dados. O último define claramente que o controlo assumido por uma autoridade independente é um elemento essencial do direito fundamental à proteção de dados.

[45] vide art.º 52.º n.º 1 do RGPD.
[46] vide art.º 53.º n.º 2 do RGPD.

A Diretiva de Proteção de Dados obriga, por sua vez, que os Estados-Membros criem autoridades de controlo por forma a fiscalizar a aplicação e cumprimento do regulamento, agindo com total independência.[47]

4.6. Da CNPD

A natureza da CNPD foi alterada com a Lei n.º 58/2019, onde lhe foi atribuída personalidade e autonomia administrativa e financeira, de forma a garantir a sua independência[48], que foi definido constitucionalmente e imposto pela legislação da União Europeia (cfr. n.º 3 do artigo 35.º da CRP e n.º 1 do artigo 51.º do RGPD). Sendo que este reclama a capacidade efetiva de gestão de contas evidenciando o exercício da função de supervisão e sancionamento dos tratamentos de dados pessoais (Comissão Nacional de Proteção de Dados, 2021b).

O controlo e fiscalização do cumprimento do RGPD, da Lei 58/2019, da Lei 59/2019 e da Lei 41/2004 é garantido pela CNPD, assim como as diversas disposições legais e regulamentares referentes à proteção de dados pessoais, com a finalidade de

[47] Diretiva Proteção de Dados, artigo 28.º n.º 1, último período; Convenção 108, Protocolo Adicional, artigo 1.º n.º 3.

[48] Sobre este conceito de "independência" veja-se a título de exemplo o seguinte acórdão do TJUE de 09 de março de 2010:

A Comissão/Alemanha: Na sua petição, a Comissão pedia ao Tribunal de Justiça que declarasse que a República Federal da Alemanha, ao submeter à tutela do Estado as autoridades de controlo competentes para fiscalizar o tratamento de dados pessoais no setor não público nos diferentes *Länder*, transpondo, assim, de forma errada a exigência de «total independência» das autoridades encarregadas de garantir a proteção desses dados, não cumpriu as obrigações que lhe incumbem por força do artigo 28.º n.º 1, segundo parágrafo, da Diretiva 95/46/CE.

O Tribunal declarou que a garantia de independência das autoridades nacionais de controlo prevista na Diretiva 95/46/CE visa assegurar a eficácia e a fiabilidade da fiscalização do respeito das disposições em matéria de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e deve ser interpretada à luz deste objetivo. Não foi estabelecida para conferir um estatuto especial às próprias autoridades e aos seus agentes, mas com vista a reforçar a proteção das pessoas e dos organismos abrangidos pelas suas decisões, sendo que as autoridades de supervisão devem, portanto, no exercício das suas funções, agir de forma objetiva e imparcial.

O Tribunal considerou que essas autoridades de controlo competentes para fiscalizar o tratamento dos dados pessoais no setor não público devem gozar de uma independência que lhes permita exercer as suas funções sem influência externa. Essa independência exclui não só qualquer influência exercida pelos organismos de fiscalização mas também qualquer instrução ou qualquer outra influência externa, direta ou indireta, que possam pôr em causa o cumprimento, pelas referidas autoridades, da sua tarefa de estabelecer um justo equilíbrio entre a proteção do direito à vida privada e a livre circulação de dados pessoais. O mero risco de as autoridades de tutela poderem exercer uma influência política nas decisões das autoridades de controlo é suficiente para impedir o exercício independente das suas funções. Por um lado, daí poderia resultar uma "obediência antecipada" dessas autoridades atendendo à prática decisória da autoridade de tutela. Por outro lado, o papel de guardiãs do direito à vida privada que as referidas autoridades de controlo desempenham exige que as suas decisões e, consequentemente, elas próprias, estejam acima de qualquer suspeita de parcialidade. Segundo o Tribunal, a tutela do Estado exercida sobre as autoridades nacionais de controlo não é, por conseguinte, compatível com a exigência de independência.

garantir a defesa dos direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos dos dados pessoais (Comissão Nacional de Proteção de Dados, 2021a).

No caso de uma violação de dados pessoais[49], o art.º 33.º n.º 1 do RGPD estabelece que os responsáveis pelo tratamento ficam obrigados a notificar[50] as autoridades de proteção de dados (em Portugal a CNPD) *sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma*.

É essencial que o responsável pelo tratamento de dados, ou o subcontratante, seja capaz de identificar qualquer violação de dados logo que a mesma ocorra e nos termos definidos no Regulamento de notificar. Esta notificação deve conter o seguinte[51]:

a. A descrição da natureza da violação de dados pessoais, incluindo, sempre que possível, as categorias e o número aproximado de pessoas em causa, bem como as categorias e o número aproximado de registo de dados pessoais em questão;
b. O nome e os dados de contacto do responsável pela proteção de dados;
c. Descrição das consequências prováveis da violação de dados pessoais;
d. Descrição das medidas tomadas/propostas pelo responsável pelo tratamento, para reparar a violação de dados pessoais, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos negativos.

Sempre que uma violação de dados seja suscetível de representar um alto risco para os direitos e liberdades dos seus titulares, segundo o n.º 1 do art.º 34º, o responsável deve comunicar a violação ao titular dos dados, em linguagem acessível e simples, sem demoras não justificadas.

[49] Na Diretiva não se encontrava qualquer definição de "violação de dados pessoais", nem se fazia referência à necessidade de notificação às autoridades de proteção de dados nem aos titulares dos dados pessoais.
[50] A CNPD já publicou um modelo de formulário para as situações de violações de dados.
[51] Tendo em conta o prazo é permitido no n.º 4 que as informações sejam fornecidas faseadamente.

Capítulo V – Sanções

5.1. Sanções e a sua natureza

Segundo Ramalho e Moutinho (2015, p. 31), entendem que o legislador *criou um edifício cuja excessiva solidez não se adaptará às forças das Constituições nacionais e ruirá sobre si mesma*, isto porque *a tutela dos bens jurídicos subjacentes à proteção de dados não se cria pela imposição externa de sanções desproporcionais ao agente da infração (...) devendo ser antes o fruto de um labor de sensibilização que faça brotar da consciência jurídica comum a compreensão dos referidos valores e a importância do seu respeito para tutela da pessoa humana*.

A expressão "sanções" não se encontra tipificada no artigo 83.º, esta norma refere-se materialmente ao campo penal e contraordenacional. No entanto, *deve ressaltar-se, que na versão em português do RGPD duas expressões são usadas de forma intercambiável como se fossem exatamente iguais, o que pode originar alguma confusão perfeitamente escusada* (Freitas, 2018, p. 115).

O RGPD na versão portuguesa usa duas expressões que poderá criar alguma confusão ao leitor, no que diz respeito às expressões "sanções administrativas" e "coimas". É um detalhe importante, na medida em que são expressões do domínio jurídico específico diferente do Direito Administrativo. É idêntico ao direito alemão, mais concretamente ao "Ordnungswidrigkeitenrecht" que partilha muitos dos seus princípios e garantias fundamentais com o direito penal e processo penal. O nosso ordenamento jurídico, diferente de outros países europeus, atribui autonomia teórico-prática a um domínio jurídico denominado "Direito de Mera Ordenação Social" no qual encontramos as "coimas". Este domínio é diferente do direito administrativo e direito penal, tendo este último, um papel punitivo. (Freitas, 2018, p. 116).

5.2. Destinatário e quantum das Coimas

Veja-se que o Regulamento estabelece no art.º 83.º dois níveis de aplicação de coimas e distingue-os consoante se aplique (ou não) a uma empresa:

a. No caso do n.º 4 do art.º 83.º aplicam-se coimas até 10 000 000 euros ou, sendo uma empresa, até 2% do seu volume de negócios anual, a nível mundial, correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado, estando em causa violações das obrigações do responsável pelo tratamento e do subcontratante nos termos dos artigos 8.º, 11.º, 25.º a 39.º; de

obrigações do organismo de certificação nos termos dos artigos 42.º e 43.º e de obrigações do organismo de supervisão nos termos do artigo 41.º, n.º 4.

b. No caso do n.º 5 art.º 83.º aplicam-se coimas até 20 000 000 euros ou, sendo uma empresa, até 4% do seu volume de negócios anual, a nível mundial, correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado, para o caso de incumprimento de obrigações dos princípios básicos do tratamento, incluindo as condições de consentimento, nos termos dos artigos 5.º, 6.º, 7.º e 9.º; dos direitos dos titulares dos dados nos termos dos artigos 12.º a 22.º; das transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional nos termos dos artigos 44.º a 49.º; das obrigações nos termos do direito do Estado-Membro adotado ao abrigo do capítulo IX e ainda pelo incumprimento do disposto no artigo 58.º n.º 1 e n.º2.

Do descrito, note-se que o RGPD criou um limite máximo sancionatório a aplicar, no entanto não definiu os limites mínimos para as sanções que prevê. Veja-se o caso das pessoas singulares o montante mínimo aplicável poderá ser de 3,74 euros segundo o artigo 17.º do RGCO (Moutinho, 2017, p. 55).

Neste sentido, os Estados-Membros têm margem de discricionariedade, segundo Miguel Henriques (2014, p. 297), a "autossuficiência normativa" de que gozam os Regulamentos, *não implica que todo e cada regulamento seja em si mesmo preciso e suficiente. É o que acontece com Regulamentos que, expressa ou implicitamente, habilitam os Estados membros a adotar medidas de aplicação legislativas, regulamentares, administrativas e financeiras necessárias à sua efetiva aplicação, reconhecendo a estes, inclusivamente, poderes discricionários*.

Vem-se discutindo na doutrina que a fixação das sanções viola as normas da CRP, isto porque para além de desencadear problemas de proporcionalidade, na medida em que às infrações da mais ínfima gravidade possam fazer-se seguir sanções de gravidade inversamente severas, também se verifica um desrespeito pelo princípio da legalidade previsto no art.º 29.º CRP já que *(...) sanções com limites tão distantes entre si (...) traduziriam a transferência da função legislativa (ou normativa) para o aplicador da sanção e, portanto, a ausência de qualquer garantia contra o arbítrio* (Moutinho, 2017, p. 55-56).

5.2.1. Outra questão que se coloca é quem são os destinatários pelas coimas?

Como se viu mais acima, no contexto sancionatório, o Regulamento usa da expressão "empresa".

Através da leitura do considerando 150 extrai-se que o legislador pretendeu esclarecer a quem compete a responsabilidade ao expor que *sempre que forem impostas coimas a empresas, estas deverão ser entendidas como empresas nos termos dos artigos 101.º e 102.º do TFUE para esse efeito*.

É portanto, fundamental destacar o entendimento do TJUE sobre o conceito de empresa, em conformidade com os artigos 101.º e 102.º do TFUE. Na opinião do TJUE, empresa será *uma unidade económica do ponto de vista do objeto do acordo em causa, mesmo que, do ponto de vista jurídico, essa unidade económica seja constituída por várias pessoas singulares ou coletivas* (Freitas, 2018, p. 117).

O RGPD por sua vez oferece uma definição de empresa no artigo 4.º n.º 18, quando afirma que se trata de *uma pessoa singular ou coletiva que, independentemente da sua forma jurídica, exerce uma atividade económica, incluindo as sociedades ou associações que exercem regularmente uma atividade económica*.

Sucede que, pelo exposto no Tratado, embora se use a expressão "empresa", em nada inclui a definição da mesma, ao qual a expressão "empresa" versa apenas sobre as práticas anti concorrenciais. Todavia, pela jurisprudência do Tribunal de Justiça e dos Direitos nacionais (entre nós art.º 3.º do Regime Jurídico da Concorrência, aprovado pela Lei n.º 19/2012, de 8 de Maio), é que podemos perceber melhor o conceito.

Para aplicação das normas sancionadoras, o conceito de "empresa" traz consigo a perplexidade sobre a sanção a aplicar, pois temos a empresas integradas em grupos, uma vez que a coima a aplicar às "empresas" tem como máximo uma percentagem do seu *volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior* (cf. art.º 83.º n.º 4, 5 e 6) é evidentemente diferente consoante se considere a empresa em si e por si ou o grupo de empresas em que ela se insira. Mais uma vez, temos que nos auxiliar da legislação interna.

Capítulo VI - Tutela Judicial e Responsabilidade Civil

Os titulares de dados pessoais podem e devem recorrer a ações judiciais sempre que os seus direitos relativos ao tratamento dos dados pessoais sejam violados, sendo a forma de efetivar a defesa dos seus direitos e liberdades.

Falamos nomeadamente nas vias de recurso, responsabilidade e sanções, segundo os artigos 77.º e seguintes do RGPD.

De acordo com o n.º 1 do art.º 77.º o titular dos dados pode apresentar uma reclamação a uma de três autoridades de controlo: à autoridade do Estado-Membro da sua residência habitual, à autoridade do seu local de trabalho ou à autoridade do local onde foi alegadamente praticada a infração. Em consonância com o disposto no art.º 57.º n.º 1 al. f), o n.º 2 do art.º 77.º estabelece um dever de informação, que impende sobre a autoridade de controlo onde foi apresentada a reclamação, estabelecendo que o reclamante deve constantemente ser informado do ponto de situação da mesma e as suas conclusões e, inclusive, de ser informado do seu direito de agir judicialmente contra a própria autoridade de controlo.[52]

O direito de recorrer judicialmente contra as decisões juridicamente vinculativas da autoridade de controlo está previsto no n.º 1 do art.º 78º, *maxime* daquelas que impunham coimas ou que indefiram reclamações. Isto decorria das normas do direito português, pois a Diretiva não consagrava este direito, sendo que a CNPD é uma entidade administrativa cujas decisões são passíveis de recurso judicial.

O n.º 2 do art.º 78.º explicita que o titular dos dados tem direito à via judicial se ocorrer omissão da autoridade de controlo no que toca à obrigação de informar o titular dos dados sobre o andamento e resultado de reclamações que lhe tenham sido apresentadas ao abrigo do disposto no art.º 77.º, por mais de 3 meses. Logo, o direito afeto ao titular de dados em exercer uma ação judicial contra uma autoridade de controlo não preclude o recurso às vias administrativas ou à resolução extrajudicial de litígios, da mesma forma que não é prejudicado pelo facto de estas terem sido utilizadas.

[52] Veja-se que o considerando 141 reflete a mesma ideia: *a autoridade de controlo deverá informar o titular dos dados do andamento e do resultado da reclamação num prazo razoável. Se o caso exigir maior investigação ou a coordenação com outra autoridade de controlo, deverão ser comunicadas informações intermédias ao titular dos dados. As autoridades de controlo deverão tomar medidas para facilitar a apresentação de reclamações, nomeadamente fornecendo formulários de reclamação que possam também ser preenchidos eletronicamente, sem excluir outros meios de comunicação.*

Por sua vez, o n.º 3 do art.º 78º define uma regra de competência jurisdicional, estabelecendo que devem ser propostas nos tribunais dos respetivos Estados-Membro as ações contra as autoridades de controlo.

Ao responsável pelo tratamento, ou ao subcontratante, é atribuída a responsabilidade pelo tratamento de dados pessoas, ou seja, quem trata a informação. Desta forma, se na sequência de tratamento de dados, os responsáveis pelo tratamento violem os direitos que assiste ao titular dos dados, este pode recorrer ao art.º 79.º do RGPD, de modo, a requerer ação judicial.

Tendo em conta o descrito no considerando 142, quando o titular dos dados considerar que os direitos previstos nos arts.º 77.º a 79.º foram violados, o art.º 80.º n.º 1 atribui a este o direito de mandatar um organismo, organização ou associação sem fins lucrativos que seja constituído ao abrigo do direito do Estado-Membro para o representar. Sendo que, a tal entidade exige-se que tenha por objeto atividades relacionadas com a proteção dos dados pessoais e que os respetivos fins sejam de interesse público.

As entidades referidas sem fins lucrativos devem estar ativas na área da proteção de dados e ter objetivos estatutários dentro da esfera de interesse público. Estas representam o titular de dados e podem apresentar reclamação ou exercer o direito a recurso judicial em seu nome.

6.1. Direito a indemnização e responsabilidade

Se de facto, observar-se que o titular de dados pessoais sofre danos materiais ou imateriais devido a uma violação segundo o RGPD, o titular tem o direito de receber uma indemnização pelos danos sofridos do responsável pelo tratamento ou do subcontratante (Barbosa, 2018, p. 438).

Deverá, assim, verificar-se o preenchimento dos vários pressupostos da responsabilidade civil extracontratual, a saber a prática de ato ilícito, a culpa, a existência de um dano e o nexo de causalidade entre o ato ilícito culposo e o prejuízo sofrido. Neste sentido, o titular tem direito de indeminização pela responsabilidade no tratamento de dados pessoais, pelo exposto no art.º 82.º do RGPD.

Por sua vez, é importante ter em consideração a responsabilidade contratual, uma vez que *basta para tanto que a violação dos dados ocorra pela preterição de determinados deveres que oneram o responsável pelo tratamento, numa relação contratual firmada entre ele e o titular daqueles. Ainda que o contrato não tenha como*

objeto essa proteção dos dados, a boa-fé pode impor determinados deveres de cuidado que, quando violados, geram responsabilidade contratual. E, se o que se defende implica a adesão a duas teses – a aceitação da ideia de concurso entre modalidades de responsabilidade civil, entendido enquanto concurso de fundamentos de uma mesma pretensão indemnizatória; e a adesão à posição doutrinal segundo a qual a violação de deveres de conduta, porque reconduzidos ao núcleo da relação contratual, vista como uma relação obrigacional complexa, gera uma hipótese que é assimilada pela responsabilidade contratual (Barbosa, 2018, p. 453).

O subcontratante pode ser responsabilizado pela violação do tratamento de dados, sendo que o n.º 2 do art.º 82.º esclarece em que casos, o subcontratante só é responsabilizado pelos danos causados se não tiver cumprido as obrigações determinadas pelo RGPD no que concerne em específico aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento. Em termos processuais, o lesado, não conhecendo as instruções, deverá demandar quer o responsável pelo tratamento, assim como o subcontratante e aguardar pelas respetivas defesas.

Podem ser isentos de responsabilidade na eventualidade de se provar que o facto que causou o dano não for de modo algum imputável ao responsável pelo tratamento ou ao subcontratante. No entanto, os pedidos de indemnização por danos causados pelo não cumprimento de outras regras do direito da União ou dos Estados-Membros não são colocados em causa. Sempre que, quer o responsável pelo tratamento quer o subcontratante estiverem envolvidos nos danos sofridos ao titular dos dados, devem estes ser responsabilizados pela totalidade dos danos causados, sendo que os titulares dos dados deverão indemnizados integralmente pelos danos que tenham sofrido.

O regime do RGPD é favorável ao lesado quanto ao ónus da prova, pois traduz-se na sua inversão, ao titular dos dados basta demonstrar que foram causados prejuízos pela violação do tratamento dos seus dados, passado para a entidade que fez o tratamento a responsabilidade de demonstrar que os factos não lhe podem ser imputados.

No seguimento do n.º 4 e n.º 5 do art.º 82.º, e em conformidade com o previsto no considerando 146, *qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento.*

Capítulo VII – O Impacto do RGPD nas Empresas

7.1. O impacto na liberdade das transações comerciais

7.1.1 Introdução da problemática

A densificação dos direitos dos titulares de dados pessoais, o agravamento dos deveres dos responsáveis pelo tratamento dos dados e subcontratantes, o reforço das competências das autoridades de controlo ou a obrigatoriedade de designação de encarregados de proteção de dados, são desde logo uns dos vários impactos do RGPD (Cordeiro, 2018a, p. 18).

Este direito de proteção de dados contemporâneo coloca renovados problemas às empresas (e não só).

No novo paradigma, as empresas transitam de um modelo de hétero-regulação para um modelo de autorregulação. Um desafio que se estende também para as organizações, com impacto nos sistemas de informação e na forma como é realizada a gestão da informação. (Cordeiro & Gouveia, 2018, p. 2)

Falar em impacto na liberdade das transações comerciais, também nos leva ao ponto da aplicação territorial deste regulamento. Ou seja, mesmo que uma organização não esteja situada territorialmente na UE, mas que cuja atividade esteja direcionada para os consumidores residentes na UE, esta organização está sujeita ao RGPD.

No que respeita ao critério do âmbito territorial este a ser aplicado de forma mais abrangente, leva a que o tratamento seja mais equilibrado entre os responsáveis que se situam dentro e fora da UE.

A ausência de estabelecimento na União não significa obrigatoriamente que as atividades de tratamento realizadas por um responsável pelo tratamento de dados ou por um subcontratante estabelecido num país terceiro ficarão excluídas do âmbito de aplicação do RGPD, visto que o artigo 3.º n.º 2, define as circunstâncias nas quais o RGPD se aplica a um responsável pelo tratamento ou a um subcontratante não estabelecido na União, em função das suas atividades desse tratamento.[53]

A este respeito, veja-se o considerando 124 do RGPD, *quando o tratamento de dados pessoais ocorra no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante na União e o responsável pelo tratamento ou o subcontratante esteja estabelecido em vários Estados-Membros, ou*

[53] Para mais esclarecimentos desta matéria vide capítulo I, ponto 1.2.2.1 e 1.2.2.2 do presente trabalho.

quando o tratamento no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, na União, afete ou seja suscetível de afetar substancialmente titulares de dados em diversos Estados-Membros, a autoridade de controlo do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante deverá agir na qualidade de autoridade de controlo principal.

7.1.2 Breve análise ao conceito de sociedade comercial

Antes de avançarmos com a douta análise ao problema que me propus responder e visto que o tema cinge-se sobretudo às empresas, veja-se que o RGPD faz menção em muitas partes às "empresas"[54]. Apesar de falarmos em "empresa" parece-me mais oportuno fazer uma breve análise sobre as sociedades comerciais dado que o ordenamento jurídico português, nomeadamente o CSC, trata as sociedades comerciais e os seus diferentes tipos.

Posto isto, as sociedades comerciais representam a estrutura das empresas nas economias de mercado e, nos termos do artigo 1º do CSC, as sociedades comerciais têm por objeto a prática de atos de comércio. Adotam o tipo de sociedades anónimas, as sociedades em nome coletivo, sociedades por quotas, sociedade em comandita simples ou sociedades em comandita por ações.

A palavra sociedade diz respeito a duas realidades jurídicas distintas e interligadas, um centro de imputação de efeitos jurídicos, dotado a maior parte das vezes, de personalidade jurídica e um tipo de negócio jurídico. Neste sentido, a sociedade entidade representa o tipo de organização de pessoas e bens que se centra no seguimento de uma determinada atividade económica. É gerada pragmaticamente por uma sociedade contrato, embora sem obrigatoriedade e, representa um negócio jurídico unilateral ou por atos não negociais e atos políticos.

A forma clássica de afirmar que a *sociedade comercial é uma simples espécie do género sociedade. Se a legislação mercantil não define ela própria o conceito genérico, pois limita-se a indicar as notas essenciais do conceito específico, é ao direito civil, Direito subsidiário em matéria comercial – que deveremos recorrer para preencher a lacuna. Deste modo, sociedade comercial vem a ser toda a sociedade* (Correia, 1968, p. 4).

[54] Sobre a definição e conceito de empresa vide ponto 5.2.1 do presente trabalho.

Ora, a adequação de uma noção legal de sociedade comercial está descrita de forma simplificada, ou seja, as sociedades comerciais são desde há alguns anos, a forma jurídica comum de exercício de uma empresa comercial, e neste contexto o sujeito comerciante por excelência. A transformação das estruturas jurídicas da empresa, ou seja, a passagem das empresas individuais para as empresas coletivas evoluiu naturalmente, pois incluiu a necessidade de partilha de investimentos e do risco da empresa, permitindo numa fase posterior, o benefício da limitação da responsabilidade[55] (Gomes F. , 2012, p. 136).

Neste sentido, a sociedade surge atualmente como uma forma usual de empresa singular e, confirmada pela sua polivalência como um instituto central do domínio jurídico comercial[56].

Uma das noções jurídicas de sociedade comercial diz respeito à qualificação de sociedade comercial como comerciante, descrita no artigo 13º nº 2, do CCom e de igual forma, a descrita no artigo 1º nº 2 do CSC, onde o legislador estabeleceu os principais requisitos de comercialidade da sociedade comercial.

Ao nível da lei civil, o artigo 980º do CC define contrato de sociedade como o *contrato de sociedade é aquele em que duas ou mais pessoas se obrigam a contribuir com bens ou serviços para o exercício em comum de certa atividade económica, que não seja de mera fruição, a fim de repartirem os lucros resultantes dessa atividade*[57] (Correia & Xavier, 1961, p. 5 e ss).

As sociedades comerciais podem ser de vários tipos, sendo suficiente que os sujeitos indiquem o tipo de sociedade de acordo com as exigências do artigo 9º do CSC, para que entre em vigor o regime jurídico aplicável a esse tipo societário específico. Assim, para uma sociedade em nome coletivo, aplica-se o regime dos artigos 1.º a 197.º e 530.º a 545.º do CSC, e se tratar de uma sociedade gestora de participações sociais aplicam-se os artigos 1.º a 74.º, 271.º a 466.º, e 481.º a 545.º do CSC, e com base no descrito no Decreto-Lei nº 495/88 de 30 de dezembro.

Não obstante existe na tradição terminológica comum a sociedade civil, em nome coletivo, por quotas, anónimas e em comandita. De acordo com o descrito no artigo 5º,

[55] Além destas vantagens, a sociedade comercial, sendo uma pessoa jurídica e não estando, consequentemente, sujeita à efemeridade da vida humana, permite a perpetuação da empresa.
[56] A hegemonia alcançada pela sociedade comercial não é sequer ameaçada pelo fenómeno plurissocietário (grupos de sociedades), uma vez que, apesar da sua indiscutível importância económica, este não granjeia – ou não granjeia ainda – de um reconhecimento jurídico pleno.
[57] O texto corresponde exatamente ao proposto no Anteprojeto.

do Decreto-Lei nº 133/2013 de 3 de outubro as empresas públicas são constituídas sob a forma de sociedade de responsabilidade limitada nos termos da lei comercial, através das quais o Estado ou outras entidades públicas exercem de forma isolada ou em conjunto, de forma direta ou indiretamente influência dominante (Vasconcelos et. al, 2019, pp. 439 e ss.).

A tabela seguinte demonstra os vários tipos de sociedades comerciais:

Tipo de sociedade	Definição e descrição
Estabelecimento Individual de Responsabilidade Limitada	Um único indivíduo ou pessoa singular (nº1 do Art.º 1 do DL nº 248/86 de 25/08) Capital não inferior a 5.000 euros, em que no mínimo 2/3 têm de ser realizados em dinheiro, podendo o remanescente ser realizado em bens objeto de penhora (Art.º 1º nº 1 e 2, Art.º 3º do DL nº 248/86).
Sociedade unipessoal por quotas	Constitui-se por um único sócio, que pode ser uma pessoa singular ou coletiva (nº 1 do Art.º 270.º A do Código das Sociedades Comerciais - CSC). Inclui a palavra "Unipessoal" ou a expressão "Sociedade Unipessoal", figurando antes da palavra "Limitada" ou a da abreviatura "Lda." (Art.º 270.º B do CSC).
Sociedade por Quotas	Mínimo de dois sócios, não se admitindo sócios de indústria, que entrem com o seu trabalho (nº1 do Art.º 202.º do CSC). A responsabilidade está limitada ao capital social, sendo este que responde face a eventuais dívidas da sociedade (nº 3 do Art.º 197.º do CSC). Se o contrato o estipular, os sócios poderão ter acréscimos de responsabilidade (nº 2 do Art.º 197.º do CSC).
Sociedade Anónima	Mínimo de cinco acionistas (singulares ou coletivos, conforme o nº 1 do Art.º 273.º do CSC), ou um único acionista sempre que este constitua uma sociedade. Em qualquer caso, não são previstos acionistas de indústria (nº 1 do Art.º 277.º do CSC). A firma finaliza com o aditamento "Sociedade Anónima" ou a abreviatura "SA", podendo escolher-se o resto do nome a

	partir das seguintes opções: a) nome composto pelo nome completo ou abreviado de um, alguns ou de todos os sócios; b) expressão referente ao ramo de atividade; c) conjugação das situações reportadas em a) e b) (nº 1, nº 2 e nº3 do Art.º 275.º do CSC).
Sociedade em Nome Coletivo	Mínimo de dois sócios (Art.º 980.º do CC e nº 2 do Art.º 7.º do CSC), com a possibilidade de admissão de sócios de indústria sempre que, no pacto social da sociedade, lhe seja atribuído o respetivo valor de indústria (Art.º 176 e nº 3 do Art.º 178.º, do CSC).
Sociedade em Comandita	As sociedades em comandita podem assumir a forma jurídica de comandita simples (o capital social não é representado em ações) ou de comandita por ações (as participações dos sócios comanditários estão representadas por ações), conforme o art.º 465.º n º3, do CSC. No caso das sociedades em comandita por ações, é exigido um número mínimo de seis sócios, pelo menos cinco sócios comanditários e um comanditado (arts.º 465.º n º1 e 479.º do CSC).

Tabela 1 - Tipos de sociedades comerciais.

7.2. Transações transfronteiriças

Em matéria de fluxos transfronteiriços de dados, a Lei n.º 67/98 começa por tornar explícito o princípio da livre circulação de dados pessoais entre Estados membros da UE (art.º 18.º). No que se refere às transferências para países exteriores à União, reproduz-se, naturalmente a regra da reciprocidade contemplada na diretiva, assim como as suas exceções (arts.º 19.º e 20.º) (Gonçalves, 2003, p. 110).

Compete à CNPD decidir se um Estado não pertencente à UE assegura ou não um nível de proteção adequado (art.º 19.º nº3), prevendo-se um mecanismo de informação da comissão europeia relativamente aos casos em que a CNPD tenha concluído pela negativa (Gonçalves, 2003, p. 110).

As abordagens transnacionais na utilização dos contadores inteligentes dos cidadãos para aplicações de redes inteligentes e maior segurança dependem da livre

circulação de dados pessoais. A título de exemplo, e tendo em conta um surto epidémico, a partilha de dados sobre este assunto pelos diferentes países poderia contribuir para uma resposta mais atempada por partes das autoridades sanitárias. A partilha e o acesso a dados pessoais de saúde poderiam melhorar o diagnóstico e o tratamento. A partilha de dados dos automóveis e dos meios de transporte poderia melhorar a gestão do tráfego e reduzir a sua congestão. Tudo isto é possível, garantindo ao mesmo tempo um elevado grau de proteção dos dados pessoais (Comissão Europeia, 2018).

O Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679) é uma lei da União Europeia que entrou em vigor em 2016 e, após um período transitório de dois anos, tornou-se a lei diretamente aplicável em todos os Estados-Membros da União Europeia a 25 de maio de 2018, sem exigir a implementação pelos Estados-Membros através da legislação nacional.

Um "regulamento" (ao contrário da diretiva substituída) é diretamente aplicável e tem um efeito consistente em todos os Estados-Membros. Contudo, subsistem mais de 50 áreas abrangidas pelo RGPD, em que os Estados-Membros podem legislar de forma diferente nas leis de proteção de dados nacionais, e continua havendo espaço para diferentes práticas de interpretação e fiscalização entre os Estados-Membros.

Relativamente à aplicação territorial, o RGPD aplica-se *ao tratamento de 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.* Ou seja, engloba todas as sociedades comerciais que tenham a suas sedes na UE e, fora desta, no caso em que o tratamento de dados pessoais tal como descreve o artigo 3º nº 1 do RGPD[58].

De evidenciar que, o n.º 2 do art.º 3.º define que o RGPD se aplica não apenas *ao contexto das atividades de um estabelecimento responsável pelo tratamento ou de um subcontratante*, como também *ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante*. E, no que respeita ao tratamento dos dados de titulares residentes na UE, aplica-se o RGPD se as atividades estiverem relacionadas com a oferta de bens e serviços.

Uma das mudanças que o novo regulamento trouxe, a qual teve um impacto significativo nos processos diários das empresas, é que estas tiveram de rever alguns dos seus procedimentos e respeitem novas obrigações. Neste sentido, todas as organizações

[58] Art.º 3.º n.º 1 do RGPD

tiveram como principal obrigação contratar um Encarregado de Proteção de dados[59] que fosse responsável pelo cumprimento da respetiva regulamentação diariamente na empresa.

Não obstante, a noção de EPD não é recente, já a Diretiva 95/46/CE não manteve a obrigação da organização de nomear um EPD, mas a sua prática em diversos países da UE ao longo dos anos.

Ao nível legislativo, o artigo 37.º do RGPD descreve a exigência da designação do EPD em três situações específicas[60]:

a) no caso em que o tratamento seja efetuado por uma autoridade ou organismo público[61];

b) sempre que as atividades principais do responsável pelo tratamento de dados ou o seu subcontratante correspondam a operações de tratamento e que exijam um controlo regular e sistemático dos titulares de dados em grande escala; ou

c) *Sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações*[62].

Ainda, de acordo com o mesmo artigo 37.º nº 1, alienas a) e b) do RGPD refere-se às atividades principais do responsável ou subcontratante pelo tratamento de dados, e o considerando 97, descreve estas atividades, condizentes com as suas *atividades primárias e não estão relacionadas com o tratamento de dados pessoais como atividade auxiliar*. Neste sentido, as atividades principais são essenciais e necessárias para atingir os objetivos do responsável pelo tratamento de dados.

---

[59] A nomeação de um EPD é igualmente obrigatória para as autoridades competentes, em conformidade com o artigo 32.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, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, pp. 89-131), e com a legislação nacional de execução. Embora as presentes orientações incidam nos EPD ao abrigo do RGPD, são igualmente pertinentes para os EPD ao abrigo da Diretiva (UE) 2016/680, no que diz respeito às suas disposições semelhantes.

[60] Nos termos do artigo 37.º, n.º 4, o direito da União ou dos Estados-Membros poderá igualmente exigir a designação de EPD noutras situações.

[61] Excetuando os tribunais no exercício da sua função jurisdicional. Ver artigo 32.º da Diretiva (UE) 2016/680.

[62] Artigo 10.º.

O GT29 emanou orientações sobre a interpretação dos conceitos consagrados no RGPD, uma vez que o RGPD definiu as situações em que se designa um encarregado de proteção de dados, no entanto não as aprofundou. Assim sendo, o GT 29 estabelece que para *determinar se um tratamento de dados é efetuado em grande escala deverá considerar-se ao número de titulares de dados afetados como número concreto ou em percentagem da população em causa; o volume de dados e/ou o alcance dos diferentes elementos de dados objeto de tratamento; a duração, ou permanência, da atividade de tratamento de dados; o âmbito geográfico da atividade de tratamento* (Grupo Trabalho Diretiva 95/46/CE, 2016, p. 23).

De igual modo, o Grupo de Trabalho do art.º 29.º (2016c) estabeleceu o significado de atividades principais como *as operações essenciais para alcançar os objetivos do responsável pelo tratamento ou do subcontratante, as quais incluem também todas as atividades em que o tratamento de dados constitui parte indissociável das atividades do responsável pelo tratamento ou do subcontratante* (Grupo Trabalho Diretiva 95/46/CE, 2016, p. 23).

As funções do EPD são exercidas com autonomia, o que significa que pode exercer outras funções, desde que não fique sujeito a um eventual conflito de interesses. De forma mais especifica, o EPD é a entidade sobre a qual recai a competência de verificação, controlo e fiscalização sobre o cumprimento escrupuloso do RGPD por parte do responsável e/ou subcontratante no tratamento de dados pessoais, sendo que este poderá recolher informações acerca da atividade do responsável e/ou subcontratante de maneira a aconselhar e recomendar melhoria de medidas no tratamento dos dados pessoais.

No entendimento de Pica (2018), o EDP trata-se de uma figura híbrida pois, por um lado, surge na hierarquia da entidade responsável pelo tratamento e, por outro lado, as suas funções poderão assemelhar-se a um intermediário da Comissão Nacional de Proteção de Dados, no que respeita ao cumprimento de todas as normas jurídicas definidas no RGPD.

Assim, em termos gerais, as funções do encarregado da proteção de dados surgem no art.º 39.º do RGPD, e são as seguintes:

a. *Ter capacidade para informar, aconselhar e monitorizar a administração da empresa/instituição, bem como os seus trabalhadores, a respeito das obrigações*

constantes do RGPD, assim como das outras disposições de proteção de dados em vigor na UE ou noutros Estados-Membros;

b. *Manter-se atualizado, recorrendo a formação e sensibilização para matérias de proteção de dados pessoais;*
c. *Realizar auditorias;*
d. *Aconselhamento em AIPD;*
e. *Colaborar com as autoridades de proteção de dados;*
f. *Relacionar-se com os titulares dos dados nomeadamente no âmbito do exercício dos seus direitos;*
g. *Estar vinculado à obrigação de sigilo ou de confidencialidade.*

A responsabilidade pelo tratamento cabe apenas ao responsável pelo tratamento e ao subcontratante, sendo que, o art.º 38.º do RGPD sublinha que quanto à designação do EPD, este demarca-se da responsabilidade no respeita ao tratamento de dados. Logo, na eventualidade de violação de dados pessoais, este não pode ser penalizado nem destituído das funções pela organização (Lambert, 2017, pp. 40-41).

A figura do EPD deverá estar entrosada no seio de todo o processo de implementação inicial do RGPD da organização e por inerência em todos os assuntos relacionados com a proteção de dados. O próprio regulamento prevê explicitamente que o EPD deverá estar envolvido nas avaliações de impacto, definindo que o responsável pelo tratamento de deverá aconselhar-se com o EPD no que concerne à realização de avaliação referida[63].

O RGPD reconhece assim, o papel essencial do EPD enquanto participante no novo sistema de governação de dados e estabelece as condições aplicáveis à sua nomeação, posição e atribuições (Grupo Trabalho Artigo 29, 2016c).

Numa fase anterior à adoção do RGPD, o GT 29 defendeu que a figura do EPD é uma responsabilidade da empresa e a sua conformidade pode proporcionar uma vantagem competitiva significativa. Neste sentido, a implementação de ferramentas de responsabilização como a viabilização de avaliações do impacto sobre a proteção de dados e auditorias, os EPD têm uma posição de intermédios entre as autoridades de controlo, titulares de dados e unidades empresariais.

Outro dos impactos mais significativos para as empresas comerciais da aplicação do RGPD é que estas ficam obrigadas a realizarem *Data Protection Impact Assessments*

[63] Cfr. Número 2 do artigo 35.º do RGPD.

(DPIA) sempre que existam operações de processamento de dados invasivas. Esta avaliação de impacto da proteção de dados é um processo de ajuda às empresas para identificar e minimizar os riscos de proteção de dados de um projeto. Assim, o DPIA deve descrever a natureza, escopo, contexto e propósitos do processamento; avaliar a necessidade, proporcionalidade e medidas de conformidade; identificar e avaliar os riscos para os indivíduos; e identificar quaisquer medidas adicionais para mitigar esses riscos.

Segundo o GTA29 *uma DPIA é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos* (Grupo Trabalho Diretiva 95/46/CE, 2016).

Segundo o art.º 35.º do RGPD constitui-se uma obrigação legal a realização de uma avaliação de impacto sobre a proteção de dados (AIPD) sempre que o exija o tratamento de dados pessoais em causa, nomeadamente o previsto no art.º 9.º ou no art.º 10.º do RGPD, quando forem tratados dados pessoais em larga escala (Comissão Nacional de Proteção de Dados, 2021a).

No n.º 3 do referido artigo, o RGPD prevê alguns exemplos de quando é que é necessário realizar uma AIPD, nomeadamente:

a) *Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;*

b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º; ou

c) Controlo sistemático de zonas acessíveis ao público em grande escala.

Cabe ao responsável pelo tratamento de dados, introduzir na organização um guia que forneça as práticas relativamente ao tratamento de dados pessoais, desde que contemple o disposto no art.º 35.º, n.º 7 do RGPD.

O RGPD não estabelece nenhuma metodologia em específico a adotar, ainda assim, as várias autoridades de controlo independente dos Estados-Membros publicaram diversas metodologias a adotar.[64]

Estas metodologias visam essencialmente, cumprir os critérios de forma exaustiva em conformidade com o RGPD. Sendo que a AIPD deve abranger pelo menos *uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, a necessidade e proporcionalidade das operações de tratamento em relação aos objetivos, uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos, e as medidas previstas para fazer face ao discos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais*.[65]

As AIPD podem assumir diversas dimensões e diferentes formas, no entanto o RGPD define requisitos básicos para uma AIPD eficaz. Os responsáveis pelo tratamento de dados devem ver uma AIPD como uma forma útil de se aplicarem sistemas de tratamento de dados em conformidade com o RGPD, tendo em conta que em alguns tipos de operações de tratamento estas podem ser obrigatórias. Posto isto, os responsáveis pelo tratamento devem encarar a realização de uma AIPD como uma ajuda à conformidade jurídica devendo ser vista como uma atividade útil e positiva (Grupo Trabalho Diretiva 95/46/CE, 2016 p.22).

Os fluxos de dados transfronteiriços foram descritos como os habilitadores de comércio, ou as marcas da globalização do século XXI, bem como a sustentação da economia global (Mckinsey Global Institute, 2016).

O comércio globalizado de dados e serviços digitais não tem sido acompanhado por uma harmonização geral da lei da internet, nem dados verdadeiros em convergência com a lei de proteção e privacidade de dados, exemplificada pela divergência entre os dois blocos ocidentais, os Estados Unidos e a Europa. Esta divergência está presente apesar da influência crescente dos dados da UE e do modelo de proteção em todo o mundo.

---

[64] Por exemplo, o Modelo Normalizado de Proteção de Dados da Alemanha, disponível em https://www.huntonprivacyblog.com/wpcontent/uploads/sites/28/2017/04/SDMMethodology_V1_EN1.pdf; Guia para uma Avaliação de Impacto na Proteção de Dados Pessoais da Espanha, disponível em https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf; e, o Código de Prática de Avaliações de Impacto de Privacidade do Reino Unido, disponível em https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

[65] Art.º 35.º n.º 7 do RGPD.

No contexto transatlântico, existem alguns obstáculos à harmonização da lei da privacidade de dados na UE, ao nível regional e os Estados Unidos ao nível federal, bem como vários padrões legais utilizados na governança da internet, em estratégias específicas (Voss, 2019). Como exemplo, a China utiliza uma regulamentação, inovação e política externa para ganhar mais poder na governança da internet (Voss, 2019, p. 408).

Com a adoção do RGPD a Europa também assumiu uma estratégia, criar a confiança online nos serviços digitais necessários para fortalecer as economias, com uma legislação que quase parece ter um carácter "evangélico", de acordo com Helen Dixon (2018, p. 28), chefe da autoridade supervisora da Irlanda.

De acordo com o descrito no considerando 33 do Regulamento Livre Fluxo de dados Não Pessoais, a promoção da confiança na segurança do tratamento ao nível transfronteiriço de dados deve reduzir a tendência dos intervenientes do mercado e do setor público de utilizar a localização.

Segundo o RGPD os dados pessoais podem ser transferidos para fora da UE apenas nas condições do Capítulo V, as disposições do que deve ser aplicado *com a finalidade de garantir que o nível de proteção das pessoas físicas seja garantido por este regulamento e não prejudicado*[66].

Neste sentido, é desafiador ao lidar com a descoberta transfronteiriça envolvendo a UE e os Estados Unidos, pois estes últimos são considerados pela UE como um país com mecanismos inadequados para a proteção de dados pessoais. Na ausência desta decisão de adequação, as transferências de dados pessoais para os Estados Unidos podem ocorrer apenas se as salvaguardas estiverem em conformidade[67].

O artigo 46.º e o Considerando 108 da RGPD descrevem os requisitos para as salvaguardas adequadas para permitir as transferências da União para países como os Estados Unidos que não são considerados como possuidores de uma proteção adequada dos dados pessoais. Neste contexto, existem vários mecanismos, sendo o mais popular o Privacy Shield, cláusulas de proteção de dados padrão e as regras corporativas vinculativas.

De salientar que a estrutura de dados UE-US Privacy Shield (Privacidade Shield) é um mecanismo de auto-certificação para empresas com sede nos Estados Unidos que

[66] Art.º 44.º RGPD "Principio Geral das Transferências".
[67] Art.º 46.º RGPD "Transferências sujeitas a salvaguardas adequadas".

permitem a transferência de dados pessoais a qualquer empresa que assine a estrutura do Privacy Shield.

O artigo 49.º do RGPD é claro no caso em que nenhum dos mecanismos acima referidos são aplicáveis, uma transferência de dados pessoais para um país terceiro ou uma organização internacional somente é permitido se uma das seguintes condições se aplicar:

a) O titular dos dados consente de forma explícita a proposta de transferência dos dados, após ter sido informado dos possíveis riscos deste tipo de transferências para o titular dos dados devido à ausência de uma decisão de adequação e salvaguardas adequadas;

b) A transferência é necessária para a execução de um contrato entre o titular os dados e o controlador ou a implementação das medidas pré-contratuais tomadas na solicitação do titular dos dados;

c) A transferência é necessária para a conclusão ou execução de um contrato celebrado no interesse do titular dos dados entre o responsável pelo tratamento e outra pessoa singular ou coletiva;

d) A transferência é necessária por importantes razões de interesse público;

e) A transferência seja necessária para o estabelecimento, exercício ou para a defesa de ações judiciais;

f) A transferência é necessária, a fim de proteger o interesse vital do titular dos dados ou de outras pessoas, onde o titular dos dados é fisicamente ou legalmente incapaz de dar consentimento[68].

g) A transferência é realizada nos termos do direito da União, e destina-se a informar o público ou qualquer pessoa com interesse legítimo, que se encontra aberta à consulta mas apenas nas condições do direito da União ou do Estado Membro que se encontrem preenchidas nesse caso concreto.

Não obstante o artigo 48.º parece limitar de forma clara a aplicação do artigo 49.º ao excluir da reivindicação legal permitida, ou seja, *qualquer julgamento de um tribunal e qualquer decisão de uma autoridade de um país terceiro exigindo um controlador ou processador (EPD) para transferir ou divulgar dados pessoais*[69]. Ou no caso em que esta decisão seja apoiada por um acordo internacional como a Convenção de Haia.

[68] Art.º 49.º RGPD "Derrogações para situações específicas".
[69] Art.º 48.º RGPD "Transferências ou divulgações não autorizadas pela legislação da União Europeia".

Se as derrogações de acordo com o descrito no artigo 49.º nº 1, alínea a) e alínea g) não se aplica, o que seria o caso do artigo 48.º se realmente excluir julgamentos de terceiros e as decisões como reivindicações legais válidas. De igual modo, para se qualificar na segunda frase do artigo 49.º, exige um teste de equilíbrio abrangente em que a transferência *pode ocorrer apenas se não for repetitiva, dizendo respeito apenas a um número limitado de titulares de dados, é necessário para fins de compelir interesses legítimos perseguidos pelo controlador que não são substituídos pelos interesses ou direitos e liberdades do titular dos dados, e o controlador avaliou todas as circunstâncias que envolvem a transferência de dados e tem, com base nessa avaliação fornecida*.

A Convenção do Conselho da Europa para a proteção dos Indivíduos em relação ao processamento automático de dados pessoais (Convenção COE) teve como pretensão proteger no território de cada parte para cada indivíduo, seja qual for a sua nacionalidade ou residência, respeito pelo seu direito á proteção dos seus dados.

O Princípio da equivalência é identificado como o critério principal no fluxo de dados transfronteiriços, sendo que os obstáculos ao fluxo de dados transfronteiriços não são permitidos entre os Estados contratantes. A justificação para este princípio para todos os contratantes tendo subscrito que o núcleo comum de proteção de dados nas disposições estabelecidas na Convenção oferecem um certo nível mínimo de proteção (Conselho Europeu, 1992).

Não obstante o CEPD reflete que as organizações extracomunitárias possam proceder a uma análise das suas atividades de tratamento, determinado se estão a ser tratados os dados pessoais e, identificar as possíveis ligações entre a atividade para a qual estão a ser trados os dados.

Conclusão

No contexto social moderno em que nos encontramos, os dados pessoais são elementos caracterizadores da pessoa singular, e devido à facilidade de circulação e divulgação desses dados, é fundamental que haja uma tutela jurídica de proteção dos dados pessoais, sob pena de causar danos irreversíveis nos titulares desses dados.

O nexo segurança/privacidade tem gerado muita atenção na UE nos últimos anos. No contexto da criação do espaço europeu de liberdade, segurança e justiça, a UE promoveu um amplo espectro de medidas que atendem a um entendimento de segurança e caracteristicamente implicando o processamento massivo de informações sobre os indivíduos. No sentido de combater os riscos para os indivíduos e empresas associados a estas medidas, a UE confiou um sistema elaborado de proteção de dados pessoais através de leis, e detalhando as salvaguardas concretas que fundamentem o direito humano de respeitar a vida privada, de acordo com o estabelecido pelo Conselho Europeu e a Convenção sobre os Direitos Humanos e Liberdades Fundamentais (CEDH).

Reorganizando a lei de proteção de dados pessoais da UE, o pacote legislativo publicado em janeiro de 2012 consiste em duas propostas legislativas, acompanhadas de um comunicado (Comissão Europeia, 2012). Esta é uma proposta de Regulamento sobre a proteção dos indivíduos no que se relaciona com o processamento de dados pessoais e livre circulação de dados. Ora, este regulamento foi projetado para substituir as disposições existentes sobre a proteção de dados pessoais, a Diretiva 95/46/CE.

O RGPD apesar do seu objetivo persistente de garantir uma proteção uniforme e coerente no tratamento de dados pessoais na UE que promove a sua livre de circulação apresenta limitações ou exceções. Assim, por um lado, as limitações naturais ou relacionadas com o direito à proteção de dados não representam um direito absoluto, mas deve ser considerado em relação ao seu papel na sociedade manter um equilíbrio com outros direitos fundamentais de acordo com o princípio da proporcionalidade.

Estas são as exceções incluídas por uma lei e justificadas por interesse público, segurança nacional ou defesa, prevenção do crime ou respeito por outros direitos fundamentais e liberdades públicas como o direito à informação. O RGPD contém autorizações e imposições para os Estados-Membros regulamentarem certas questões impedindo a unificação antecipada e contribuindo para perpetuar diferentes níveis de proteção na União.

Por outro lado, ao implementar o regime de proteção de dados alterou de forma profunda as organizações e este regulamento obriga-as a alterar profundamente a forma como se opera diariamente com os dados pessoais que possuem, seja em termos de procedimentos internos ou externos com os clientes. Definiu-se assim, novas regras para o tratamento de dados pessoais, direitos dos titulares dos dados, as obrigações nas empresas que tratam especificamente dos dados pessoais.

Neste sentido, o RGPD tenta simplificar a burocracia que a implementação de sistemas de proteção de dados impõe às empresas e aos responsáveis pelo tratamento pessoal de dados. O aviso prévio ou notificação à autoridade de supervisão exigida para realizar o tratamento de dados pessoais desaparece, mas incorpora nos seus artigos as obrigações e princípios diretamente relacionados com a governança corporativa, modelos de gestão de risco e conformidade regulatória, já exigida noutras áreas jurídicas, como a prevenção de riscos trabalhistas ou de conformidade criminal.

Bibliografia

ALSENOY, B. V. (2017). Reconciling the (extra)territorial reach of the GDPR with public international law. Data Protection and Privacy under Pressure, 94.

BARBOSA, M. M. (15 de março de 2018). Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil. Revista de Direito Comercial, p. 438.

CALVÃO, Filipa U. (2018). Direito da Proteção de Dados Pessoais: Relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina, 1.ª edição, Universidade Católica

CANOTILHO, J. G., & MOREIRA, V. (2014). Constituição da República Portuguesa Anotada V.I. Coimbra: Coimbra editora.

CASTRO, Catarina S. (2004). *O direito a autodeterminação informativa e as novos desafios gerados pelo direito à liberdade e a segurança no pós 11 de setembro*. Disponível em: http://www.estig.ipbeja.pt/~ac_direito/CatarinaCastro.pdf

CORDEIRO, A. B. (2018a). Autonomia da função de encarregado de proteção de dados e a independência do exercício da advocacia. Revista da Ordem dos Advogados, 20.

CORDEIRO, A. B. (2018b). Da responsabilidade civil pelo tratamento dos dados pessoais. Obtido de book beta: https://blook.pt/publications/publication/2ae6399f13bb/

CORDEIRO, A. B. (2020). Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019. Coimbra: Almedina.

CORDEIRO, Silvério B. & GOUVEIA, Luís B. (2018). *Regulamento Geral de Proteção de Dados (RGPD): o novo pesadelo das empresas?*, Relatório Interno Tenologia, Redes e Sociades.

CORREIA, Ferrer, & XAVIER, V. Lobo. (1961). Do Contrato de Sociedade – Separata do Boletim do Ministério da Justiça n.º 104, Lisboa

CORREIA, Ferrer. (1968). Lições de Direito Comercial, vol. II – Sociedades Comerciais – Doutrina geral, Coimbra, Universidade de Coimbra

COUTINHO, F. P., & MONIZ, G. C. (2018). Anuário da Proteção de Dados. Lisboa: CEDIS.

DIXON, Helen (2018). Regulate to Liberate: Can Europe Save the Internet?, FOREIGN AFF., at 28, 30

FAZENDEIRO, Ana. (2018). Regulamento Geral de Proteção de Dados- Algumas notas sobre o RGPD, 2.ª edição, Almedina, Coimbra, ISBN 978-972-40-7154-1

FREITAS, P. M. (2018). Regulamento Geral de Proteção de Dados: uma visão portuguesa sobre o regime sancionatório. UNIO - EU Law Journal, pp. 115-116.

GOMANN, M. (2017). The new territorial scope of EU protection law: deconstructing a revolutionary achievement. Common market law review, 586.

GOMES, Fátima. (2012). Manual de Direito Comercial, Universidade Católica Portuguesa, Lisboa.

GOMES, R. (2017). Portal da Ordem dos Advogados. Obtido de https://portal.oa.pt/media/121529/estudo_rgpd_kpmg.pdf

GONÇALVES, M. E. (2003). Direito da Informação. Almedina

HENRIQUES, Miguel G. (2014). Direito da União, 7.ª edição, Coimbra: Almedina, Coimbra, ISBN 9789724055541

HERT, P. d., & CZERNIAWSKI , M. (2016). Expanding The European data protection scope beyond territory. International Data Privacy Law, 231.

LAMBELHO, Ana & MENDES, J. Barros. (2019). *O RGPD e o impacto nas organizações: 6 meses depois*. X Congresso Internacional de Ciência Jurídico-Empresariais

LAMBERT, P. (2017). The Data Protection Officer. First Edition. Taylor & Francis Group.

MACHADO, Jónatas E. M. (2010). Direito da União Europeia, 1.ª edição, Coimbra: Wolters Kluwer Portugal- Coimbra Editora, Coimbra, ISBN 9789723218589

MAGALHÃES, F. M., & PEREIRA, M. L. (2018). Regulamento Geral de Proteção de Dados. Vida Económica.

MAÑAS, José Luís Piñar. (2016). Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de protección de datos, Editorial Reus

MOEREL, Lokke (2011), *The long arm of EU data protection law: Does the data protection directive apply to processing of personal data of EU citizens by websites worldwide?,* International Data Privacy Law, Oxford Academy, pp 28-46, Disponível em: https://academic.oup.com/idpl/article/1/1/28/759646

MONIZ, G. C. (2018). Finalmente: coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! O fim do enigma linguístico do artigo 3.º, n.º 2 do RGPD. UNIO - EU Law Journal, 128.

MOUTINHO, J. L. (2017). Legislador português precisa-se. Algumas notas sobre o regime sancionatório no Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679). Fórum de Proteção de Dados, pp. 56-57.

MOUTINHO, José L. (2008). Direito das contra-ordenações- Ensinar e Investigar, Universidade Católica Editora, Lisboa, ISBN 9789725402078

PICA, L. (2018). As Avaliações de Impacto, O Encarregado de Dados Pessoais e a Certificação no Novo Regulamento Europeu de Proteção de Dados Pessoais. Cyber Law, p. Vol 1. No.5.

PINHEIRO, A. S., & GONÇALVES, C. J. (2018). Comentário ao Regulamento Geral de Proteção de Dados. Almedina.

PINHEIRO, Alexandre Sousa. (2015). Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional. AAFDL.

RAMALHO, J. L., & MOUTINHO, D. S. (2015). Notas sobre o regime sancionatório da proposta de Regulamento Geral sobre a Proteção de Dados do Parlamento Europeu e do Conselho. Fórum de Proteção de Dados, p. 31.

REYNOLDS, P. D. (1979). Ethical Dilemmas and Social Science Research. San Francisco: Jossey-Bass Publishers.

VASCONCELOS, Joana, CUNHA, D. Xavier & DALHUISEN, Jan (2019). Estudos em Homenagem a Agostinho Pereira de Miranda, Almedina, Coimbra

VOSS, W. Gregory (2019). Obstacles to Transatlantic Harmonization of Data Privacy Law in Context, U. ILL. J.L. TECH. & POL'Y 403, 408

Documentação

Comissão Europeia (2012). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, Bruxelas.

Comissão Europeia. (2018). Proteção dos dados e o mercado único digital . Obtido de https://ec.europa.eu/transparency/regdoc/rep/1/2018/PT/COM-2018-320-F1-PT-MAIN-PART-1.PDF

Comissão Europeia. (2019). Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados não pessoais na União Europeia. Bruxelas.

Comissão Nacional de Proteção de Dados. (2019). Deliberação/2019/494

Comissão Nacional de Protação de Dados. (2021a). Comissão Nacional de Proteção de Dados. Obtido de https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/

Comissão Nacional de Proteção de Dados. (2021b). Relatório de atividades 2019/2020. Lisboa, Portugal. Obtido de https://www.cnpd.pt/cnpd/relatorios-de-atividades/

Comité Europeu para a Proteção de Dados. (2019). edpb.europa.eu. Obtido de Diretrizes 3/2018 sobre o âmbito de aplicação territorial do: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf

Conselho da Europa. (2014). Manual da Legislação Europeia de Proteção de Dados. Obtido de: https://op.europa.eu/pt/publication-detail/-/publication/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1

Conselho Europeu (1992). Model Contract to Ensure Equivalent Protection in the Context of Transborder Data Flows with Explanatory Report (1992), Study Made Jointly by the Council of Europe, the Commission of the European Communities and International Chamber of Commerce, Strasbourg, at 4–6.

Diretiva 95/46/CE (1995). Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, JO L 281

Diretrizes 3/2018. (2018). Diretrizes 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3º). Obtido de Diretrizes 3/2018 sobre o âmbito de aplicação

territorial do RGPD (artigo 3º): https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf

Grupo de Trabalho Artigo 29. (2010). Parecer 8/2010 sobre a lei aplicável. Obtido em: https://www.gpdp.gov.mo/uploadfile/others/wp179_pt.pdf

Grupo Trabalho Artigo 29. (2016a). Guidelines on Transparency under Regulation 2016/679. Obtido de https://ec.europa.eu/newsroom/article29/items/622227

Grupo Trabalho Artigo 29. (2016b). Orientações sobre o direito à portabilidade dos dados. Obtido de https://ec.europa.eu/info/law/law-topic/data-protection_en

Grupo Trabalho Artigo 29. (2016c). Orientações sobre os encarregados da proteção de dados (EPD).

Grupo Trabalho Artigo 29. (2017). Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679. JOUE, 4. Obtido de CNPD: https://www.cnpd.pt/media/zgkec1q0/data-breach-_wp250rev01_pt.pdf

Grupo Trabalho Diretiva 95/46/CE (2016) O grupo de trabalho sobre a proteção das pessoas no que diz respeito ao tratamento de dados pessoais. Disponível em: https://www.gpdp.gov.mo/uploadfile/2017/0109/20170109103502288.pdf

Parecer n.º 20/2018. (2018) Parecer sobre a proposta de lei n.º 120/XIII/2018. Disponível em: https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e45544563765247396a6457316c626e527663306c7561574e7059585270646d4644623231706334e686279396a5a57593359544d794f4330325a44526c4c54526c4e546b74596a41304e4331694e54426d4f5449314d6a64684d7a45756347526d&fich=cef7a328-6d4e-4e59-b044-b50f92527a31.pdf&Inline=true

Parlamento Europeu. (2020). Fichas temáticas sobre a União Europeia. Obtido de Espaço de liberdade, de segurança e de justiça: https://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais

Parlamento Europeu. (2001). Regulamento (CE) nº 45/2001 do Parlamento Europeu e do Conselho. Jornal Oficial da União Europeia, 01-22.

Parlamento Europeu. (2002). Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas. Jornal Oficial das Comunidades Europeias, 37-47.

Parlamento Europeu. (2006). Diretiva 2006/24/CE do Parlamento Europeu e do Conselho . Jornal Oficial da União Europeia.

Parlamento Europeu. (2016a). Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho. Jornal Oficial da União Europeia.

Parlamento Europeu. (2016b). Eur-Lex. Obtido de Regulamento (UE) 2016/679 : https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679

Parlamento Europeu. (2018). Obtido de Grupo de Trabalho do Artigo 29.º Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679: https://www.uc.pt/protecao-de-dados/suporte/20180410_orientacoes_relativas_ao_consentimento_wp259_rev01

PINHEIRO, Alexandre Sousa (2018). *RGPD: o regime jurídico*, Boletim da Ordem dos Advogados, Disponível em: http://historico-ordemadvogados.impresa.pt/oa-11/destaque-opiniao-asp

Proposta de Lei n.º 120/XIII. (2018). Proposta de Lei n.º 120/XIII. Lisboa.

Regulamento EU 2016/679. (2016). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial da União Europeia.

Jurisprudência

1 – Tribunal de Justiça da União Europeia:

Acórdão do TJUE, de 22 de junho de 1989, processo 103/88, Milão, disponível em: http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30d52b26c65a76604e50811a96dd39ff0903.e34KaxiLc3qMb40Rch0SaxuNbxr0?text=&docid=96045&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=19496

Acórdão do TJUE, de 6 de Novembro de 2003, processo C-101/01 – Bodil Lindqvist, ECLI:EU:C:2003:596, disponível em http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&dong=PT&mode=lst&dir=&occ=first&part=1&cid=9063485

Acórdão do TJUE, de 20 de Maio de 2003, processo C-465/00 –Österreichischer Rundfunk e outros, ECLI:EU:C:2003:294, disponível em: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48330&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=9063485

Acórdão do TJUE, de 11 de Dezembro de 2014, processo C-212/13 František Ryneš, ECLI:EU:C:2014:2428, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=9063485

Acórdão do TJUE, de 17 de julho de 2014 processos C-141/12 e C-372/12 pelo Rechtbank Middelburg (C-141/12) e pelo Raad van State (C-372/12) ECLI:EU:C:2014:2081. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62012CJ0141

Acórdão do TJUE, de 8 de Abril de 2014, processo C-293/12 – Digital Rights Ireland e Seitlinger e outros, ECLI:EU:C:2014:238. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageInd ex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485

Acórdão do TJUE, de 13 de Maio de 2014, processo C-131/12 – Google Spain e Google, ECLI:EU:C:2014:317, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485

Acórdão do TJUE, de 1 de outubro de 2015, No processo C-230/14, Weltimmo s.r.o. ECLI:EU:C:2015:639, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62014CJ0230

Acórdão do TJUE, de 1 de outubro de 2015, Processo n.º C- 201/14, Smaranda Bara, Disponível em: https://curia.europa.eu/juris/document/document.jsf?docid=168943&doclang=PT

Acórdão do TJUE, de 19 outubro de 2016, No processo C-582/14, Patrick Breyer, ECLI:EU:C:2016:779. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=o%2Btratamento%2Bde%2Bdados%2Bpessoais%2B%25C3%25A9%2Bl%25C3%25ADcito&docid=184668&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=160792#ctx1

Acórdão do TJUE, de 9 de março de 2017, processo C-398/15 - Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce e Salvatore Manni, ECLI:EU:C:2017:197, disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=2502278

Acórdão do TJUE, de 20 de dezembro de 2017, no processo C-434/16. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=os%2Bdados%2Bdevem%2Bser%2B%25E2%2580%259Crecolhidos%2Bpara%2Bfinalidades%2Bdeterminadas%252C%2Bexpl%25C3%25ADcitas%2Be%2Bleg%25C3%25ADtimas&docid=198059&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=633850#ctx1

Acórdão do TJUE, de 21 de março de 2019 processo C-673/17 Planet49 GmbH Contra Bundesverband der Verbraucherzentralen und Verbraucherverbände ECLI:EU:C:2019:246, disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=212023&doclang=PT