COIMBRA BUSINESS SCHOOL

iscac Politécnico de Coimbra

100 ANOS

since 1921

A Responsabilidade Civil do Responsável pelo Tratamento de Dados Pessoais e do Subcontratante

Vilma Sofia Rodrigues Correia

ISCAC | 2021

COIMBRA BUSINESS SCHOOL

iscac Politécnico de Coimbra

100 ANOS

Vilma Sofia Rodrigues Correia

A Responsabilidade Civil do Responsável pelo Tratamento de Dados Pessoais e do Subcontratante

Coimbra, abril de 2025

Vilma Sofia Rodrigues Correia

A Responsabilidade Civil do Responsável pelo Tratamento de Dados Pessoais e do Subcontratante

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de **Mestre em Solicitadoria no ramo de Empresas**, realizada sob a orientação do Professor Armando Ferreira Soares Veiga.

Coimbra, abril de 2025

TERMO DE RESPONSABILIDADE

Declaro ser a autora desta dissertação, que constitui um trabalho original e inédito, que nunca foi submetido a outra Instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação da presente dissertação.

PENSAMENTO

"O sucesso é a soma de pequenos esforços repetidos dia após dia."

Robert Collier

DEDICATÓRIA

Aos meus pais e ao meu irmão

Ao meu namorado

Às minhas amigas

AGRADECIMENTOS

Esta dissertação não poderia começar de outra forma se não com os agradecimentos às pessoas que, com o seu apoio incondicional, tornaram possível a realização e conclusão deste percurso.

Para começar, agradeço à minha família, especialmente aos meus pais e ao meu irmão, por nunca me deixarem desistir e por estarem sempre ao meu lado, dando-me força e coragem em todos os momentos, e fazendo-me acreditar que, com perseverança e dedicação, tudo é possível.

Dirijo um agradecimento especial ao meu namorado, pelo apoio incansável, pela paciência e pelas diversas vezes em que dedicou o seu tempo a ajudar-me de tantas formas diferentes ao longo deste processo.

Agradeço também às minhas amigas, pelo apoio, pelas palavras de motivação e pelo conhecimento partilhado, que contribuíram para que esta jornada fosse encarada com uma perspetiva mais ampla e confiante.

Por fim, expresso o meu agradecimento ao Professor Armando Veiga, por ter aceitado orientar a elaboração da presente dissertação.

A todos, o meu muito obrigada.

RESUMO

A realização da presente dissertação, tem como principal objetivo, analisar a Responsabilidade Civil do Responsável pelo tratamento de dados pessoais e do Subcontratante, um tema de extrema relevância no contexto da proteção de dados.

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, que é o RGPD da UE, estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à sua livre circulação, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na UE.

Nesta dissertação, pretende-se não apenas abordar os conceitos fundamentais presentes no art. 4.º do RGPD, mas também contextualizar historicamente a evolução das regulamentações de proteção de dados que culminaram na criação do RGPD. Tal análise histórica traduz-se num alicerce substancial, fornecendo uma base sólida para a compreensão da imprescindibilidade de uma legislação tão abrangente no cenário atual.

Por fim será fundamental examinar o tema da responsabilidade civil imputada ao responsável pelo tratamento de dados e ao subcontratante, sobretudo no caso de eventual tratamento inadequado de dados pessoais. Pelo que é necessário, proceder ao escrutínio dos direitos atribuídos aos titulares dos dados pessoais, com vista a identificar quais as obrigações e deveres imputados tanto ao responsável pelo tratamento quanto ao subcontratante.

Palavras-chave: Proteção de Dados; Responsável pelo tratamento; Subcontratante; Titulares dos dados; Dados pessoais; Direitos; Deveres;

ABSTRACT

The main objective of carrying out this dissertation is to analyze the Civil Liability of the Person Responsible for processing personal data and the Subcontractor, a topic of extreme relevance in the context of data protection.

Regulation (UE) 2016/679 of the European Parliament and of the Council, which is the UE RGPD, establishes the rules relating to the protection of natural persons with regard to the processing of personal data and its free movement, by a person, a company or an organization, of personal data relating to people in the UE.

Throughout this dissertation, we intend not only to address the fundamental concepts present in article 4 of the RGPD, but also to historically contextualize the evolution of data protection regulations that culminated in the creation of the RGPD. Such historical analysis translates into a substantial foundation, providing a solid basis for understanding the indispensability of such comprehensive legislation in the current scenario.

Finally, it will be essential to examine the issue of civil liability attributed to the data controller and the subcontractor, especially in the case of possible inappropriate processing of personal data. Therefore, it is necessary to scrutinize the rights attributed to holders of personal data, with a view to identifying the obligations and duties attributed to both the controller and the subcontractor.

Keywords: Data Protection; Responsible for the treatment; Subcontractor; Data subjects; Personal data; Rights; Duties;

ÍNDICE GERAL

Lista de abreviaturas, acrónimos e siglas

Ac. – Acórdão

AIPD – Avaliação de Impacto sobre a proteção de dados

Al. ou al. – Alínea

Art. ou art. – Artigo

CC – Código Civil

CdE – Conselho da Europa

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CEDH – Convenção Europeia dos Direitos do Homem

CNPD – Comissão Nacional de Proteção de Dados

CNPDPI – Comissão Nacional de Proteção de Dados Pessoais Informatizados

CRP – Constituição da República Portuguesa

EPD ou Encarregado – Encarregado da Proteção de Dados

N.º ou n.º – Número

NTIC – Novas Tecnologias de Informação e Comunicação

ONU – Organização das Nações Unidas

Pág. ou pág. – Página

Proc. ou proc. – Processo

Responsável – Responsável pelo Tratamento de Dados

RGPD ou Regulamento – Regulamento Geral da Proteção de Dados

TAC – Tribunal Administrativo do Círculo

TEDH – Tribunal Europeu dos Direitos do Homem

TJUE – Tribunal de Justiça da União Europeia

UE – União Europeia

Introdução

Esta dissertação, faz parte do programa de Mestrado em Solicitadoria realizado no Instituto Superior de Contabilidade e Administração de Coimbra, especificamente na componente não letiva. O tema em foco está relacionado com "**A Responsabilidade Civil do Responsável pelo Tratamento de Dados Pessoais e do Subcontratante**". A escolha deste tema decorre da sua extrema relevância no contexto da proteção de dados, motivada pela crescente importância da regulamentação nesse domínio em todo o mundo, destacando-se o RGPD da UE.

Procurarei organizar a presente dissertação em cinco pontos que se complementam entre si. No primeiro e segundo ponto irei realizar um breve enquadramento à evolução histórica da proteção de dados, no que diz respeito à UE e ao nosso ordenamento jurídico.

Seguidamente, no terceiro ponto, serão abordados conceitos fundamentais, princípios e direitos dos titulares dos dados pessoais. Os conceitos fundamentais estabelecem as bases para uma correta compreensão do RGPD. Relativamente aos princípios, delineiam as diretrizes essenciais que regem o tratamento de dados pessoais. Darei ainda a devida atenção aos direitos concedidos aos titulares dos dados, ressaltando a importância da proteção e privacidade das informações pessoais no âmbito do regulamento. Este capítulo, visa fornecer uma compreensão abrangente do RGPD e qual o seu impacto no contexto da proteção de dados.

Nesta sequência, no quarto ponto, serão explorados diversos aspetos relacionados com a gestão e responsabilidade face ao tratamento de dados pessoais. Inicialmente, procurarei apresentar os conceitos de Responsável pelo Tratamento e Subcontratante, delimitando as suas responsabilidades face ao processamento dos dados pessoais, por forma a obter uma compreensão mais clara das responsabilidades e deveres das partes envolvidas no processo de tratamento de dados. Posteriormente, falarei da relação entre essas duas entidades, destacando a importância da cooperação e conformidade com as regulamentações de proteção de dados. Além disso, serão discriminadas as obrigações

tanto do responsável pelo tratamento quanto do subcontratante no que diz respeito ao tratamento adequado e seguro dos dados pessoais.

Por fim, mas não menos importante, no quinto ponto irei abordar a questão da responsabilidade legal decorrente do tratamento de dados pessoais. Este tema é de grande relevância, uma vez que envolve as consequências legais das ações relacionadas ao tratamento inadequado ou ilegal de informações pessoais. Esta abordagem é feita a fim de obter uma melhor perceção das implicações legais associadas ao tratamento de dados, contribuindo para uma atuação mais consciente e responsável por parte dos envolvidos.

Desde já, é possível aferir que o RGPD representa uma resposta robusta aos desafios trazidos pela era digital, que procurou preservar os direitos fundamentais dos cidadãos europeus no cenário atual de processamento de dados pessoais em larga escala. A história da proteção de dados na Europa reflete o crescimento constante das leis e regulamentos para enfrentar os desafios emergentes da era digital.

1 Evolução Histórica da Proteção de Dados na União Europeia

Antes de abordar o tema propriamente dito, é fundamental retroceder um pouco até à história da Proteção de Dados, tanto a nível da UE como a nível nacional, a fim de perceber o surgimento das regulamentações e a necessidade destas no que toca à matéria da Proteção de Dados.

A crescente e célere evolução das NTIC[1] e a sua globalização, trouxeram consigo uma ferramenta que permitia facilmente recolher, armazenar, processar e transferir dados pessoais, em grande escala, tornando-se assim indispensável a criação de leis relacionadas com a proteção de dados pessoais, que promovessem e garantissem a transparência, no que toca ao tratamento dos dados pessoais, procurando desta forma, combater o indevido e abusivo processamento e uso dos dados pessoais, justificando-se assim a elevada necessidade de implementar regulamentação adequada.

No que concerne à proteção de dados, a história europeia, começou logo após a II Guerra Mundial. Foi nessa época, que surgiram as primeiras ferramentas basilares referentes à proteção de dados. Primeiramente, em 1945, deu-se a criação do CdE, a fim de promover um Estado de direito, uma democracia e os direitos humanos. [2] Posteriormente, no ano de 1948, a ONU adotou a Declaração Universal dos Direitos do Homem e em 1950, foi adotada a Convenção Europeia dos Direitos do Homem pela CdE,[3] entrando apenas em vigor em 1953.[4] Com esta Convenção, foi implementado o direito à privacidade como parte integrante dos direitos fundamentais, tendo sido este direito considerado um passo significativo no avanço da proteção dos dados pessoais.

---

[1] Conforme consta do considerando (6), do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, as novas tecnologias transformaram a economia e a vida social e contribuíram para agilizar a livre circulação de dados pessoais na UE e a sua transparência para países terceiros e organizações internacionais, procurando assegurar ao mesmo tempo um elevado nível de proteção dos dados pessoais.

[2] Nuno Saldanha, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica?* Como implementar? Lisboa, FCA – Editora de Informática, 2018, pág. 3.

[3] Este Conselho, inicialmente era composto por 10 países, disponível in História da União Europeia – 1945-59 | União Europeia (27 abril 2025).

Acresce ainda dizer que este Conselho atualmente é composto por todos os Estados-Membros da EU, disponível in Estados-Membros - O Conselho da Europa em resumo (27 abril 2025).

[4] Ainda que estes documentos não tratassem especificamente da proteção de dados, foi com os mesmos que se estabeleceram os princípios fundamentais relacionados com a privacidade e os direitos individuais, que numa fase posterior se tornariam partes fulcrais das leis de proteção de dados.

Recorrendo ao art. 8.º da CEDH, que nos diz que "*1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência*."[5] desde logo é possível aferir que o direito à proteção de dados pessoais, ainda que de forma indireta, é um direito devidamente consagrado nesta convenção. Neste sentido, a fim de garantir a correta aplicação e interpretação da CEDH, nomeadamente do art. 8.º, foi criado em 1959 o TEDH com o objetivo de fazer com que todos os Estados da CEDH cumprissem as suas obrigações, respeitando efetivamente os direitos consagrados no art.º 8, para tal, este tribunal devia apreciar as queixas apresentadas pelos cidadãos ou pelos seus grupos, pelas organizações não governamentais ou pelas pessoas coletivas que alegassem violação das normas estipuladas na convenção.[6]

Mais tarde, no ano de 1981, tendo mais uma vez por base o art. 8.º da CEDH, foi adotada a Convenção n.º 108, consequência da crescente evolução das NTIC, sentida nas décadas de 60 e 70,[7] gerando uma grande necessidade de adotar regras mais específicas de forma a salvaguardar as pessoas através da proteção dos seus dados pessoais.[8] Esta convenção, aplica-se a todos os tratamentos de dados realizados tanto no domínio privado como no público, englobando o respetivo tratamento de dados realizado pelas autoridades judiciárias e policiais.

A Convenção n.º 108, estabeleceu alguns princípios, nomeadamente que o tratamento de dados pessoais devia ser feito de forma leal e lícita, devendo ser armazenados para fins precisos e legítimos, significando isto, que os dados não podiam ser utilizados para fins incompatíveis com essas finalidades, não podendo ser conservados

[5] Este art. ainda é composto pelo n.º 2 que diz o seguinte " Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros."

[6] O TEDH desempenha um papel fundamental na interpretação e aplicação do art. 8.º, cabendo a este analisar casos individuais que alegam violação do direito ao respeito pela vida privada e familiar. Este tribunal deveria decidir se efetivamente houve ou não violação dos direitos protegidos pela CEDH com base nos princípios estabelecidos na mesma. Podemos aferir que este facto contribuiu para a promoção dos direitos humanos na Europa e para o desenvolvimento de uma jurisprudência consistente em questões relacionadas à vida privada e familiar.

[7] Nuno Saldanha, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 3.

[8] Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa - *Manual da Legislação Europeia sobre Proteção de Dados*, Luxemburgo: Serviço das Publicações da União Europeia, 2022, edição 2018, pág. 28.

por tempo superior ao estipulado.[9] Pelo exposto, podemos aferir que a Convenção n.º 108 foi um dos marco importantíssimo, no que diz respeito à promoção da privacidade e da segurança dos dados pessoais, visando o equilíbrio entre o uso legítimo da informação e a proteção dos direitos de cada individuo.

Posteriormente, foi adotada em 1995 a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, com vista a estabelecer normas para o processamento de dados pessoais e a sua livre circulação dentro da UE.[10] A adoção desta diretiva, prendeu-se com a necessidade de harmonizar um determinado leque de normas dos Estados-Membros que já legislavam nesta matéria, ou seja, procurou tornar equivalente em todos os Estados-Membros o nível de proteção dos direitos e liberdades das pessoas face aos tratamento dos seus dados pessoais.[11] Uma vez mais, debruçamo-nos em princípios, como a transparência e a licitude, no que toca ao tratamento dos dados pessoais, o respeito pelos titulares pelo facto de existir o dever de pedir o consentimento aos mesmos para o uso e processamento dos seus dados pessoais e de existir o dever de manter os titulares dos dados informados relativamente ao modo como são usados os seus dados. Acresce mencionar, que posteriormente em 25 de maio de 2018, esta diretiva, foi substituída pelo RGPD.[12]

A falta de menção, por parte de EU, nos seus tratados, da temática dos Direitos Humanos, levou a que no dia 7 de dezembro de 2000 fosse proclamada a CDFUE, tornando-se juridicamente vinculativa como direito primário da UE, com a entrada em vigor do Tratado de Lisboa em 2009.[13] Esta carta fixou no seu art. 7.º o respeito pela vida

[9] Nuno Saldanha, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 4.
Nesta Convenção também se prevê o tratamento de dados pessoais e obrigações relativas à segurança dos mesmos, proibindo assim a ausência de garantias legais ao processamento de dados pessoais considerados sensíveis, tais como dados ligados à raça, à opinião política, à saúde, às convicções religiosas, à vida sexual ou relativamente ao registo criminal de determinado individuo.
A Convenção n.º 108 passou por revisões e emendas para manter sua relevância em face das mudanças nas tecnologias da informação e nas práticas de processamento de dados.
[10] Conforme consta do considerando (3), do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[11] Nuno Saldanha, op. cit. pág. 4.
[12] Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa - *Manual da Legislação Europeia sobre Proteção de Dados*, Luxemburgo: Serviço das Publicações da União Europeia, 2022, edição 2018, pág. 33 e 34.
[13] Disponível in Tratado de Lisboa (27 abril 2025).

privada e familiar e no seu art. 8.º a proteção de dados pessoais.[14] Com a CDFUE reuniram num único documento os direitos fundamentais dos cidadãos europeus, concedendo uma base legal para a proteção desses direitos dentro da UE.

Relativamente à proteção das pessoas singulares no que toca ao tratamento de dados pessoais e à livre circulação desses dados, de momento, vigora o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, denominado de RGPD. Este regulamento veio, conforme mencionado anteriormente, revogar a Diretiva 95/46/CE do Parlamento Europeu e do Conselho. A introdução do RGPD no contexto europeu, veio reforçar a ideia de que a matéria da proteção de dados em todos os Estados-Membros, tem um papel cada vez mais importante e que esta matéria exige um quadro mais sólido e coerente na UE, apoiado por uma aplicação rigorosa das regras no contexto jurídico e legal,[15] e que dado todo o avanço tecnológico existia a necessidade de ser reformulada em alguns aspetos, garantindo que o titular de dados pessoais, teria a primazia sobre o seu direito fundamental à privacidade.

[14] Disponível in Carta dos Direitos Fundamentais da União Europeia (27 abril 2025).
[15] Conforme consta do considerando (7) - presente no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

2 A História Portuguesa da Proteção de Dados

Em diversos países, foi testemunhada uma notável evolução na proteção de dados ao longo do tempo e Portugal não foi exceção, demonstrando um progresso significativo na proteção de dados ao longo das últimas décadas, adotando normativas internacionais e adaptando-se avanços tecnológicos sentidos. Esta análise, oferece uma perspetiva abrangente dessa evolução, desde os marcos legais iniciais até às adaptações mais recentes às regulamentações da UE.

A nível nacional, a matéria da proteção de dados pessoais foi reconhecida como um direito fundamental, através da CRP de 1976, sendo este o primeiro texto jurídico que abordou esta temática.[16] Com a revisão feita à CRP em 1997, mais precisamente no art. 35.º da CRP, no seu n.º 2, foi consagrada a existência de uma entidade administrativa independente que visaria garantir a proteção de dados.[17]

Ainda tendo em conta o processamento de dados no que toca à informática, foi publicada no ano de 1991 a Lei da Proteção de Dados Pessoais face à informática, mais precisamente a Lei n.º 10/91 que estabelecia no seu art. 1.º que o "O uso da informática deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada e familiar e pelos direitos, liberdades e garantias fundamentais do cidadão."[18]

Houve um aproveitamento da Lei n.º 10/91 a fim de criar e regular a CNPDPI, devendo esta controlar o processamento automatizado de dados pessoais, garantindo que o mesmo era feito respeitando os direitos, liberdades e garantias consagrados na lei e na Constituição. Posteriormente, em 1994 foi aprovada a Lei n.º 28/94, que veio introduzir medidas para reforçar a proteção de dados pessoais, verificando-se significativas alterações à lei anterior. Uma das alterações foi atribuir o direito de informação e acesso

[16] Nuno Saldanha, Novo Regulamento Geral de Proteção de Dados – *O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 9.
[17] Conforme tudo consta do n.º 2 dos art. 35.º da CRP "A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.", ainda que este art. trata-se da temática da proteção de dados ligado à informática, concedia um determinado conjuntos de direitos aos titulares dos dados, nomeadamente o direito à proteção de dados, à informação, ao acesso aos seus dados e a sua retificação.
[18] Disponível in Lei n.º 10/91 | DR (27 abril 2025).

à CNPDPI, por forma a ter meios para fiscalizar os sistemas informáticos podendo assim cumprir de forma mais competente as suas funções, desta forma tanto o setor público como o setor privado, devem facultar as informações solicitadas pela comissão.[19] Acresce mencionar, que em 7 de janeiro de 1994, a CNPDPI passou a designar-se CNPD.

Atualmente, esta entidade administrativa independente, é denominada de CNPD, sendo estabelecida no ano de 1998, quando a Diretiva 95/46/CE foi transposta para o nosso ordenamento jurídico através da Lei n.º 67/98, de 26 de outubro. Tendo em conta o exposto, o regime jurídico de proteção de dados passou a abranger tanto os dados manuais como os dados informatizados, visto que, anteriormente, somente abrangia os arquivos informatizados não incluindo o tratamento de dados manual.

A Lei n.º 67/98 apresentou um conjunto de princípios que foram posteriormente aprofundados no RGPD. Estes princípios incluem o tratamento lícito de dados pessoais, a recolha para finalidades específicas, a garantia de que os dados são adequados e relevantes, dados exatos e conservados de forma a identificar os seus titulares.[20]. Além disso, esta lei regulamentou a natureza, as atribuições, as competências, a composição e o respetivo funcionamento da CNPD, por sua vez o RGPD versa sob as organizações de controlo europeias, deixando para as jurisdições nacionais a adequação do regulamento às autoridades locais.

A posteriori, ainda relacionado com a lei acima mencionada, foi publicada a Lei n.º 43/2004 com o objetivo de regular a organização e o funcionamento da CNPD, sem fazer quaisquer alterações às atribuições e competências estabelecidas pela lei anterior.

Após a entrada em vigor desta lei, o cenário da proteção de dados no nosso ordenamento jurídico passou por uma nova fase significativa com a implementação do

[19] Conforme nos diz o art. 1.º, com a epigrafe Dever de Colaboração, da Lei n.º 28/94 "1 - As entidades públicas e privadas devem dispensar a sua colaboração à Comissão Nacional de Proteção de Dados Pessoais Informatizados, facultando-lhe todas as informações que por esta, no exercício das suas competências, lhes forem solicitadas. 2 - O dever de colaboração é designadamente assegurado quando a Comissão tiver necessidade, para o cabal exercício das suas funções, de examinar o sistema informático, os ficheiros automatizados e demais documentação relativa à recolha, tratamento automatizado e transmissão de dados pessoais."

[20] Nuno Saldanha, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 11.

RGPD, que entrou em vigor de 2016, e acarretou mudanças substanciais no tratamento e na proteção dos dados pessoais não apenas em Portugal, mas em toda a UE.

Em suma, a evolução da proteção de dados em Portugal reflete a sua integração nas normativas internacionais e a sua adaptação ao progresso das sociedades e aos avanços tecnológicos sentidos. Desde as primeiras leis até às mais recentes adaptações às regulamentações da UE, Portugal tem um percurso de progressão em direção à proteção de dados, com o reconhecimento desta temática como um direito fundamental desde a Constituição de 1976.

Esta evolução é evidenciada, desde a criação da CNPDPI em 1991 até passar a designar-se CNPD, reflete o compromisso do país com a segurança e privacidade dos dados pessoais. As legislações subsequentes, como a Lei n.º 28/94 e a Lei n.º 67/98, ampliaram as competências da CNPD, acompanhando assim as mudanças tecnológicas e sociais. A implementação da Lei n.º 43/2004 e posteriormente do RGPD são exemplos adicionais desse compromisso, evidenciando a adaptação contínua às demandas emergentes e o estabelecimento de um quadro legal abrangente para proteção de dados em Portugal.

3 O Regulamento Geral sobre a Proteção de Dados (RGPD)

O RGPD, já falado de forma breve nos pontos anteriores, é uma legislação da UE que entrou em vigor a 25 de maio de 2016, sendo apenas aplicável a partir de 25 de maio de 2018, visando fortalecer e unificar as regras da proteção de dados para todos os países membros da UE, proporcionando aos cidadãos um maior controlo sobre as suas informações pessoais, implementando diretrizes claras para as organizações que lidam com dados pessoais.

Desde logo, surge a seguinte questão, "**Qual a importância de criar o RGPD?**"; antes da implementação deste regulamento, na EU, vigorava a Diretiva 95/46/CE do Parlamento Europeu e Conselho, com o aumento dos fluxos de dados transfronteiriços, a maior integração económica, a evolução tecnológica, a globalização, e o crescente intercâmbio e uso de dados pessoais entre setores público e privado, impulsionaram a necessidade de uma regulamentação abrangente,[21] levando à substituição da diretiva em vigor. Pelo facto de a diretiva permitir que cada país transcrevesse o seu conteúdo com certa liberdade, resultando numa legislação fragmentada sobre a temática da proteção de dados pessoais, levando isso a uma aplicação pouco uniforme entre os países da UE, gerando alguma insegurança jurídica que dificultava o desenvolvimento económico e tornava mais difícil para as autoridades nacionais fazerem cumprir as suas obrigações de fiscalização.[22] Todos estes fatores levaram a UE a legislar sobre a proteção de dados pessoais, de forma a obter uma legislação harmonizada, coerente[23] e na qual fosse possível verificar uma aplicação rigorosa das regras, levando à criação do RGPD.[24]

[21] Conforme consta do considerando (6) – presente no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[22] Nuno Saldanha, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 16.
[23] Conforme consta do considerando (7) – "Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas." – presente no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[24] A UE com a criação do RGPD visou alcançar **três objetivos fundamentais**, nomeadamente harmonizar a legislação, garantir a coerência no tratamento de dados pessoais em todo o território europeu e assegurar a segurança jurídica. Somente, por meio de uma aplicação uniforme em toda a UE, seria possível atingir esses objetivos de forma eficaz.

O RGPD, estabelece um quadro regulamentar robusto no que diz respeito ao tratamento de dados pessoais, adaptado ao contexto tecnológico atual e aos modelos de negócios baseados em informação, com o objetivo de proteger os cidadãos da UE. Este regulamento assenta em três pilares fundamentais,[25] sendo esses:

- O pilar da territorialidade, assegurando que o regulamento tenha aplicabilidade extraterritorial, responsabilizando todas as entidades que processam dados pessoais de cidadãos da UE, independentemente da sua localização ou da autonomia ou forma jurídica.
- Segue-se o pilar das sanções, em que o RGPD veio introduzir um sistema de sanções rigoroso, que permitia a aplicação de multas severas, de até 4% do facturamento global anual ou 20 milhões de euros, o que for maior, reforçando assim as obrigações das entidades que tratam dados pessoais,[26] sendo exemplo disso a violação de deveres perante os titulares, das regras de consentimento, das transferências internacionais de dados.
- Por fim, o pilar ligado aos direitos e deveres, estabelecendo novas exigências sobre o consentimento, o acesso e a informação, introduzindo novos direitos, como o direito à portabilidade dos dados. Impondo ainda deveres aos responsáveis pelo tratamento, nomeadamente a obrigação de garantir a integridade, a segurança dos dados e de notificar os titulares em caso de violações.

Após falar do que levou à criação do RGPD e dos pilares fundamentais nele assentes, importa esclarecer **a QUEM** se aplica o mesmo. O RGPD considera a proteção de pessoas singulares, um direito fundamental, não pondo em causa a nacionalidade ou o seu local de residência,[27] procurando deste modo proporcionar um espaço de liberdade, segurança

[25] Nuno Saldanha, *RGPD – Guia para uma auditoria de conformidade, dados, privacidade, implementação, controlo, compliance*, Lisboa, FCA – Editora de Informática, 2019, pág. 17.
[26] A introdução deste pilar, foi a maior novidade do RGPD, foi com este regulamento, introduzido o pagamento de coimas, quando se verificasse o incumprimento das obrigações impostas no mesmo.
[27] Este regulamento apenas se aplica a pessoas singulares, não abrangendo desta forma o tratamento de dados pessoais relacionados com pessoas coletivas, conforme referido no considerando (14) - presente no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

e justiça e de uma união económica.[28] Por fim, este regulamento aplica-se ao tratamento de dados pessoais, de **todas as pessoas singulares**, realizado por meios totalmente ou parcialmente automatizados ou até mesmo por meios não automatizados, procurando defender os direitos e as liberdades fundamentais destas pessoas face ao seu direito à proteção de dados e promover a livre circulação dos dados pessoais, conforme consta do art. 1.º nos respetivos números que o compõem e art. 2.º n.º 1.[29]

Depois de mencionar a quem se aplica o RGPD, importa apontar quando não se aplica, nomeadamente em questões de defesa dos direitos e liberdades fundamentais; à livre circulação de dados pessoais referentes a atividades fora do âmbito de aplicação do direito da UE, especificamente a segurança nacional; a atividades relacionadas com a política externa e de segurança comum da UE; ao tratamentos de dados pessoais efetuado por pessoas singulares no exercício de atividades de índole pessoal ou doméstica; ao tratamento de dados pessoais relativos a pessoas coletivas, alusivo à sua denominação, forma jurídica e os seus contactos; a atividades de tratamento para efeitos de proteção de pessoas singulares no que diz respeito à prevenção, investigação, deteção e repressão de infrações penais ou execução de sanções penais.[30][31]

Acresce salientar que existe um conjunto alargado de sujeitos jurídicos a quem se aplica o regulamento e que estão todos em contacto com o titular dos dados pessoais, designadamente o responsável pelo tratamento de dados e o subcontratante, as autoridades nacionais, os destinatários e os terceiros. Mais á frente, nesta dissertação, procurarei esclarecer quem são estes sujeitos e qual o seu papel.

---

[28] Conforme referido no considerando (2), "(…) tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas." - presente no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[29] A. Barreto Menezes Cordeiro (Coordenação), *Comentários ao Regulamento geral de proteção de dados e á Lei n.º 58/2019*, Coimbra, Almedina, 2021, pág. 63.

[30] Nuno Saldanha, *RGPD – Guia para uma auditoria de conformidade, dados, privacidade, implementação, controlo, compliance*, Lisboa, FCA – Editora de Informática, 2019, pág. 20;
e
A. Barreto Menezes Cordeiro, *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*, Reimpressão, Coimbra, Almedina, 2020, pág. 87 a 89.

[31] Conforme ainda consta do art.º 2, n.º 2 al. a) a d) do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Mediante o exposto, é possível afirmar que o objeto do RGPD se prende com regulamentação da proteção das pessoas singulares, face ao tratamento dos seus dados pessoais e à livre circulação desses dados. Estando aqui presente os dois grandes objetivos deste regulamento, designadamente defender os direitos e liberdades fundamentais das pessoas singulares e promover a livre circulação dos seus dados. O RGPD representa uma mudança significativa na forma como se deve abordar a proteção de dados e a privacidade dos indivíduos. Com a sua aplicação pretende-se aumentar a transparência, a segurança e o controle sobre como os dados pessoais são coletados, processados e armazenados.

3.1 Conceitos fundamentais do RGPD

O RGPD, é uma legislação da UE que estabelece diretrizes para a proteção de dados pessoais, que define e regula como as organizações devem coletar, processar, armazenar e proteger os dados pessoais dos cidadãos europeus. Com este regulamento foram introduzidas diversas definições importantes relacionadas à proteção de dados pessoais, algumas das quais já estavam previstas em leis anteriores, como a Lei n.º 10/91, a Diretiva 95/46/CE e a Lei n.º 67/98, sendo que da diretiva e desta última lei foram mantidas quase todas as definições, sendo essas consolidadas e ampliadas no RGPD.

Neste regulamento estão inclusos 26 conceitos cruciais para uma melhor perceção da sua aplicação e do seu impacto na proteção de dados pessoais, visando garantir que os direitos de privacidade e proteção de dados de cada pessoa sejam respeitados e que as organizações cumpram as obrigações legais de forma adequada.

Esses conceitos demonstram o grau de detalhamento do RGPD e a sua ampla abordagem para proteger a privacidade dos dados dos indivíduos na UE. Ao especificar de forma clara os papeis, responsabilidades, direitos e medidas de segurança, o RGPD procurou garantir um maior controlo dos titulares sobre os seus dados pessoais e incentivar práticas responsáveis de tratamento de dados pelas organizações.

Diante do exposto, é fundamental abordar algumas das definições que incorporam o art. 4.º do RGPD, definições essas que facilitaram a interpretação do regulamento.

3.1.1 Dados Pessoais[32]

Recorrendo ao art. 4.º do RGPD no n.º 1,[33] entende-se por dados pessoais toda a "informação relativa a uma pessoa singular identificada ou identificável (...)", ou seja, é

[32] Em primeiro lugar, importa fazer referência a alguns dados considerados pessoais e depois a alguns dados que não considerados pessoais. Para os dados considerados pessoais temos o nome completo; os números de identificação constante no cartão de cidadão; a morada; o número de telemóvel; o endereço de correio eletrónico pessoal; a matrícula de um automóvel. Para os dados não considerados pessoais temos o n.º de registo de uma empresa; um endereço de correio eletrónico como por exemplo "info@institutopublico.pt"; e dados anonimizados.

[33] Segundo o art. mencionado entende-se por dados pessoais "(…) a informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um

o mesmo que dizer que são tidos como dados pessoais qualquer informação relativa a pessoas singulares que as identifique ou que as torne identificáveis, de forma direta ou indireta. Desta breve análise já é possível depreender que este conceito é composto por **quatro elementos** automatizáveis (descritos acima entre aspas).[34]

Começando pelo elemento **qualquer informação**, no que toca aos dados pessoais, toda a informação é considerada relevante, designadamente quanto à aplicação do RGPD. A noção de informação engloba todos os aspetos relacionados à pessoa, quer sejam familiares ou socias, privados ou públicos, físicos ou mentais. Ao falar de informação, podemos estar a falar de dados identificativos, nomeadamente o nome, a data de nascimento, o número do cartão de cidadão ou da morada; de considerações íntimas, como por exemplo desejos, posições religiosas ou políticas, opiniões; de dados físicos, como o género, a altura, a cor quer dos olhos como do cabelo; ou até mesmo falar de dados profissionais ou académicos, como os estatutos profissionais ou laborais ou graus académicos. Deste modo, podemos referir que vários são os dados que permitem identificar uma determinada pessoa singular.

Passando para o elemento **relativa a**, sendo desde logo percetível, este elemento faz nos entender que a informação tem de estar relacionada com uma determinada pessoa. Dentro deste elemento, é fundamental perceber qual o conteúdo, finalidade e resultado pretendido com essa informação. Quando falamos do conteúdo, referimo-nos à informação que incide sobre uma pessoa, isto significa que é a própria pessoa que é objeto de estudo.[35] Quando se fala na finalidade, ainda que aqui não seja a própria pessoa o objeto de estudo, é possível pelos dados recolhidos, avaliar, tratar de determinada forma ou influenciar o comportamento de uma pessoa. Por fim, quando nos referimos ao resultado, é aquela informação que não incide sobre uma determinada pessoa, como no

número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;".

[34] A. Barreto Menezes Cordeiro (Coordenação), *Comentários ao Regulamento geral de proteção de dados e á Lei n.º 58/2019*, Coimbra, Almedina, 2021, pág. 81.

[35] Aqui temos com exemplo, as análises clínicas que nos leva a um doente. Outro exemplo registo criminal que nos leva ao cidadão.

conteúdo, e que não visa avaliar ou influenciar uma pessoa, como na finalidade, mas que no fundo, sem ser o principal objetivo, o permita fazer.[36]

Relativamente ao elemento **pessoa singular**, conforme já referido nesta dissertação, o RGPD abrange as pessoas singulares, não estando em causa a sua nacionalidade ou local de residência, sendo desde logo possível excluir as pessoas coletivas. Importa ainda mencionar, que este regulamento não abrange dados pessoais de pessoas falecidas, não obstante atribui competências aos Estados-Membros para legislarem nesse sentido, ou seja, permite-lhes que estabeleçam normas para o tratamento de dados pessoais de pessoas falecidas.[37]

Por fim, abordando o elemento **identificada ou identificável**, no n.º 1 do art. 4.º do regulamento, é referido que "(...) é identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador (...)", significando isto, que falamos da expressão identificada sempre que de forma direta e inequívoca seja possível identificar uma determinada pessoa, ou seja, identificar o titular dos dados pessoais.[38] Por sua vez, o titular dos dados pessoais será identificável, por um terceiro, um responsável pelo tratamento ou qualquer pessoa que possua os meios necessários para aceder a mais informação, por exemplo, por essa informação ser pública. A identificabilidade tem, consequentemente, uma natureza relativa, variando consoante a informação detida por cada sujeito considerado individualmente.[39] Em suma, uma pessoa, é considerada identificável, se houver possibilidade de a identificar, ainda que não tenha sido identificada, pelo que, toda a informação que possa ser utilizada para identificar uma pessoa, identificada ou não, é considerada um dado pessoal.

[36] Para a situação do resultado podemos ter em conta o seguinte exemplo, uma empresa de transportes pesados de mercadorias instalou um sistema de localização de satélite, com o objetivo de gerir melhor a sua frota.
[37] Conforme consta do conteúdo do considerando (27), "O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas." - presente no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[38] Como exemplo de um dado pelo qual pode a pessoa ser diretamente e de forma inequívoca identificada, temos o nome completo de uma determinada pessoa, e os dados do cartão de identificação, uma vez que são dados entregues apenas a uma pessoa. Relativamente aos dados pelos quais será possível identificar indiretamente uma determinada pessoa, temos como exemplo o número de telefone ou a matrícula de um veículo.
[39] A. Barreto Menezes Cordeiro (Coordenação), *Comentários ao Regulamento geral de proteção de dados e á Lei n.º 58/2019*, Coimbra, Almedina, 2021, pág. 84.

3.1.2 Tratamento e Limitação do Tratamento

No que toca ao conceito do tratamento de dados, segundo o art. 4.º no n.º 2 do RGPD, é tido como tratamento a operação ou o conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não. Desde logo, é possível verificar que esta definição é composta por três elementos, nomeadamente **a operação ou o conjunto de operações**, entendendo-se por tal o ato ou os atos efetuados sobre dados pessoais; **efetuada sobre dados pessoais**, deste elemento depreende-se que apenas têm relevância os atos realizados sobre dados pessoais, sendo desta forma excluídos os dados públicos, as operações relacionados com dados anónimos e dados que não sejam sobre pessoas singulares; e **por meios automatizados ou não automatizados**,[40] aqui é de fácil perceção que por este regulamento são abrangidos os tratamentos efetuados por meios automatizados, bem como os efetuados por meios não automatizados.

Nota fundamental, quando falamos de tratamento de dados pessoais nem todos são, em termos jurídicos, relevantes. Conforme é referido pelo art. 2.º n.º 1 do RGPD, este regulamento só é aplicado aos tratamentos por meios total ou parcialmente automatizados e aos tratamentos por meios não autorizados contidos em ficheiros ou a eles destinados.

Como exemplos de tratamentos de dados temos a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição, conforme previsto no n.º 2 do art. 4.º do RGPD.[41]

[40] **Tratamento de dados por meios automatizados** são as operações sobre dados pessoais realizadas por equipamentos de processamento de dados, podendo esse tratamento ser feito por meio parcial ou totalmente automatizados, isto significa dizer que podem ser operações com intervenção humana, mas reduzida ou poder ser operações sem intervenção humana, respetivamente. Quanto ao **tratamento de dados por meios não automatizados**, falamos de operações sobre dados pessoais em que não é utilizado nenhum equipamento de processamento de dados, ou seja, são operações realizadas manualmente, por exemplo a recolha de dados pessoais através de uma caneta e papel.

[41] Tipos de operação de tratamento: processamento salarial e gestão de pessoal; destruição de documentos que contenham dados pessoais; colocação de fotografias pessoais em websites; recolha de elementos identificativos num serviço de receção.

No que diz respeito à limitação do tratamento, conforme consta do art. 4.º n.º 3 do RGPD, esta consiste n' "(…) a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro." Com essa marca,[42] pretende-se dar a conhecer de forma clara no sistema, que o tratamento de um determinado conjunto de dados pessoais se encontra sujeito a algumas restrições. A fim de restringir o tratamento de dados pessoais, podem ser usados métodos como transferir temporariamente os dados para outro sistema, bloquear o acesso aos dados ou retirar temporariamente informações de um site. Nos sistemas automatizados, as restrições devem ser feitas com meios técnicos para evitar que os dados sejam sujeitos a outras operações de tratamento ou alterados.[43]

3.1.3 Definição de Perfil

Segundo o art. 4.º n.º 4 do RGPD o conceito de definição de perfil consiste em "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses mesmos dados para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações".

Do exposto, é possível aferir que este conceito abrange o tratamento de dados pessoais, realizado total ou parcialmente por meios automatizados, não abrangendo desta forma o tratamento de dados realizado por meios manuais, ou seja, por meios não automatizados.[44]

Este conceito, ganha importância, uma vez que garante ao titular o direito de não ser submetido a uma decisão fundamentada exclusivamente no tratamento automatizado, especialmente quando tal decisão afeta sua situação legal ou o afeta de maneira significativa. Não obstante, a tomada de decisões com base no tratamento automatizado, incluindo a definição de perfis, é permitida se for autorizada pelo direito da União ou dos

[42] Como alguns exemplos de marcas, temos as seguintes expressões "restrito", "confidencial" e "bloqueado"
[43] Conforme consta do teor do considerando (67) - presente no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[44] Estes conceitos de tratamento por meios automatizados ou não automatizados, encontra-se explicado no subponto anterior.

Estados-Membros, como por exemplo para controlo de fraudes e de evasões fiscais, de encontro com os regulamentos e diretrizes da UE. É igualmente permitida para garantir a segurança do serviço ou se for necessária para a celebração ou executar de um contrato entre o titular dos dados e o responsável pelo tratamento, ou com o consentimento explícito do titular.[45]

Assim sendo, o responsável pelo tratamento, deve informar os titulares dos dados pessoais sobre a existência de definição de perfis e informações relativas a essa definição, de forma a compreender como o algoritmo chega àquela conclusão. [46] Cabe ao responsável pelo tratamento de dados, no caso de o tratamento implicar um elevado risco para os direito e liberdades das pessoas singulares, proceder à realização de uma avaliação de impacto sobre a proteção de dados (AIPD),[47] se falarmos de tratamentos de dados que incluam a definição de perfis esta avaliação é obrigatória.[48]

3.1.4 Pseudonimização

A pseudonimização consiste num tratamento de dados efetuado sobre os dados pessoais que impossibilita a identificação do seu titular, sem recorrer ao uso de informação suplementar, pelo que, essa informação deve ser conservada, separadamente, de forma a não se conseguir identificar o titular dos dados, conforme o mencionado no art. 4.º, n.º 5 do RGPD.[49]

O uso da pseudonimização ajuda a diminuir os riscos de exposição da identidade dos titulares dos dados pessoais, protege os seus interesses e, simultaneamente, facilita o

[45] Conforme consta do art. 22.º e dos considerandos (71) e (72) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[46] Conforme o referido nos art.s 13.º, n.º 2, al. f), 14.º, n.º 2, al. g) e 15.º, n.º 1, al. h) do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[47] O AIPD é um documento de Avaliação de Impacto sobre Proteção de Dados, que descreve diversas operações de tratamento, avalia a necessidade do tratamento e auxilia a gestão dos riscos, com o objetivo de determinar quais as medidas necessárias no tratamento dos dados pessoais, disponível in Avaliação de Impacto sobre Proteção de Dados - Portal do DPO - Encarregado de Protecção de Dados (27 abril 2025).
[48] Conforme consta do art. 35.º, n.º 3 al. a) do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[49] Art. 4.º, n.º 5 - "«Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;"

papel do responsável pelo tratamento de dados ou do subcontratante, no que diz respeito ao cumprimento das obrigações estabelecidas pelo RGPD.[50]

Acresce mencionar, que o conceito em estudo, não se deve confundir com a anonimização, uma vez que nesta não é tecnicamente possível identificar o titular dos dados.[51] Explicando de forma breve o que se entende por anonimização, para que qualquer dado seja anonimizado, é necessário remover elementos suficientes de modo que a identificação do titular dos dados se torne impossível, de forma irreversível. Em termos mais específicos, os dados devem ser manipulados de maneira que não possam mais ser usados para identificar uma pessoa, mesmo considerando "todos os meios razoavelmente utilizáveis", tanto pelo responsável pelo tratamento quanto por terceiros. Em suma, a anonimização deve ser um processo irreversível, comparável à eliminação definitiva dos dados.[52]

3.1.5 Responsável pelo Tratamento

O responsável pelo tratamento é a entidade que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais, isto significa, que é o responsável pelo cumprimento das regras legais de proteção de dados, podendo esta entidade ser uma pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo. [53]Quando falamos de uma pessoa coletiva, o responsável pelo tratamento de dados, é a própria pessoa coletiva, não sendo o funcionário, o auxiliar ou representante. A pessoa singular estará sujeita aos mecanismos civis, criminais ou administrativos aplicáveis.[54]

[50] Conforme consta do considerando (28) primeira parte - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[51] Conforme consta do considerando (26) parte final, "(…) Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação." - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[52] Disponível in Anonimização e Pseudonimização (27 abril 2025).
[53] Conforme consta do art. 4.º, n.º 7 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[54] A. Barreto Menezes Cordeiro, *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*, Reimpressão, Coimbra, Almedina, 2020, pág. 307 e 308.

Ao responsável pelo tratamento, ainda lhe está incumbida a contratação de um subcontratante, a fim de este desempenhar as suas funções, quando se verificar necessidade de tal contratação. O responsável pelo tratamento de dados desempenha um papel crucial na proteção dos dados pessoais, sendo o principal ponto de decisão sobre como os dados são usados.

Conforme acima referido no primeiro parágrafo, o tratamento de dados pessoais, pode ser desempenhado em conjunto, isto significa dizer que este tipo de tratamento, será desempenhado com a intervenção de mais do que um responsável pelo tratamento, contudo, ainda que esteja em causa um tratamento de dados realizado de forma conjunta, não é o mesmo que recorrer a um subcontratante (devidamente explicado no subponto seguinte), nem com o tratamento autónomo do mesmo conjunto de dados por responsáveis diferentes.[55]

3.1.6 Subcontratante

O subcontratante é "(...) uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes" [56], ou seja, o subcontratante, corresponde a um mandatário do responsável pelo tratamento de dados, que trata os dados pessoais por conta do responsável pelo tratamento. Como exemplo de subcontratante, temos a entidade que processa os salários ou que trata do armazenamento dos processos administrativos.

Posteriormente, nesta dissertação, será novamente abordado tanto este conceito como o constante no subponto anterior, de forma mais detalhada, onde procurarei dizer quais os deveres deste perante os titulares dos dados e quais as respetivas consequências do incumprimento das obrigações a ele subjacentes.

[55] A. Barreto Menezes Cordeiro (Coordenação), *Comentários ao Regulamento geral de proteção de dados e á Lei n.º 58/2019*, Coimbra, Almedina, 2021, pág. 89.
[56] Conforme consta do art. 4.º, n.º 8 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

3.1.7 Consentimento

O consentimento, de acordo com o art. 4.º n.º 11, consiste numa "manifestação de vontade, livre, específica, informada e inequívoca, 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". O consentimento, deve ser dado, previamente, pelo próprio titular dos dados objeto do tratamento, não devendo o silêncio, as opções pré-validadas ou a omissão, constituir um consentimento.[57]

Para uma melhor perceção deste conceito, é fundamental ter em atenção os art. 7.º e 8.º do RGPD, que nos falam, respetivamente, das condições aplicáveis ao consentimento e das condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade de informação.

Estando em causa um tratamento de dados realizado com base no consentimento do titular dos dados pessoais, o responsável pelo tratamento, deverá poder demonstrar que o consentimento foi efetivamente prestado pelo titular. Acresce dizer, que caso o responsável pelo tratamento formule previamente uma declaração de consentimento, a mesma deve ser fornecida de forma inteligível e de fácil acesso, numa linguagem clara e simples e sem conter cláusulas abusivas.[58]

A manifestação de vontade, não será considerada válida nos casos em que "(…) o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado."[59] Estaremos perante uma privação de liberdade, nas seguintes situações: se o titular der o seu consentimento pressionado por falta de tempo; se o consentimento for acompanhado de contraprestações aparentemente excessivas ou desproporcionais; se o titular dos dados estiver numa situação de fragilidade ou de necessidade; se o não consentimento prejudicar o titular dos dados pessoais; se for patente um desequilíbrio de posições entre o titular dos dados e o

[57] Segundo o exposto no considerando (32) - presente no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[58] Conforme consta do art. 7.º, n.ºs 1 e 2 e do considerando (42) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[59] Conforme considerando (42) parte final - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

responsável pelo tratamento.[60] Presume-se que o consentimento não é livremente dado se não for possível consentir, separadamente, para diferentes operações de tratamento de dados, ou se a execução de um contrato, incluindo a prestação de um serviço, estiver condicionada ao consentimento, mesmo quando este não é necessário para essa execução.[61]

Nota importantíssima, ainda que o titular dos dados ao dar o seu consentimento, o preste de livre e espontânea vontade, este tem o direito de retirar o seu consentimento a qualquer momento, sem colocar em causa a licitude do tratamento efetuado com base no consentimento, devendo esta retirada ser tão fácil de fazer como é dar o seu consentimento.[62]

Quando for aplicável o art. 6.º, n.º 1, al. a) onde menciona que "O tratamento só é lícito se (…) o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;", tendo em consideração a oferta de serviços da sociedade da informação direcionada às crianças, sendo este lícito se possuírem pelo menos 16 anos. Caso estejamos a falar de uma criança com idade inferior a 16 anos, o tratamento só será lícito se o consentimento for dado ou autorizado pelos titulares das responsabilidades parentais da criança.[63] Neste último caso, o responsável pelo tratamento procura verificar que o consentimento foi prestado ou autorizado pelos titulares das responsabilidades parentais.[64]

3.1.8 Violação de Dados Pessoais

A violação de dados pessoais, consiste na "(…) violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou

[60] A. Barreto Menezes Cordeiro (Coordenação), *Comentários ao Regulamento geral de proteção de dados e á Lei n.º 58/2019*, Coimbra, Almedina, 2021, pág. 90 e 91.
[61] Conforme consta do art. 7.º, n.º 4 e do considerando (43) parte final - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[62] Ao abrigo do art. 7.º, n.º 3 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[63] Conforme consta do art. 8.º, n.º 1 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[64] Conforme consta do art. 8.º, n.º 2 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.", conforme consta do art. 4.º, n.º 12 do RGPD.

Quanto à segurança dos dados pessoais, devem ser aplicadas as medidas técnicas e organizativas adequadas,[65] pelo responsável pelo tratamento ou pelo subcontratante, de forma a assegurar a segurança dos dados.[66] Caso não sejam adotadas as medidas adequadas em caso de violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas.[67]

Caso o responsável pelo tratamento tenha conhecimento de alguma violação de dados pessoais, deverá proceder à notificação da autoridade de controlo, no prazo de 72 horas após ter tido conhecimento da violação. Caso não proceda à notificação no prazo referido, a notificação entregue fora de prazo deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases, sem demora injustificada.[68] Da mesma forma deve proceder o subcontratante, assim que este tome conhecimento de alguma violação, notificar o responsável pelo tratamento sem demora injustificada.[69]

O responsável pelo tratamento de dados pessoais, também deverá informar o titular dos dados da violação dos mesmos, isto no caso de essa violação ser suscetível de causar elevados riscos para os direitos e liberdades da pessoa singular, permitindo com esta comunicação que o titular tome as precauções necessárias.

---

[65] O art. 32.º, n.º 1 da al. a) a d) elenca algumas das medidas de segurança a ser tomadas, nomeadamente " (…) a) A pseudonimização e a cifragem dos dados pessoais; b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento." - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[66] Conforme se encontra previsto no art. 32.º, n.º 1 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[67] Como exemplos de possíveis dados causados, com a violação da segurança dos dados pessoais dos titulares, temos as seguintes situações: a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação de identidade, perdas financeiras, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social, conforme costa do considerando (85) – presente no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[68] Conforme consta do art. 33.º, n.ºs 1 e 4 e do considerando (85) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[69] Conforme consta do art. 33.º, n.º 2 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Por fim, é importante destacar que a violação de dados pessoais é diferente do tratamento ilícito de dados pessoais, sendo considerados conceitos distintos e independentes.[70]

3.1.9 Autoridade de Controlo

O art. 4.º, n.º 21 do RGPD, no seu conteúdo, apenas faz referência que a autoridade de controlo consiste "numa autoridade pública independente criada por um Estado-Membro (…)", remetendo-nos logo para o art. 51.º do mesmo regulamento, no qual é abordado com mais profundidade o conceito em análise.

Importa referir, que o facto de ser dito que estas autoridades de controlo são autoridades públicas que gozam de independência, não é sinónimo de que as mesmas não venham a ser sujeitas a procedimentos de controlo ou monitorização no que diz respeito às suas despesas nem a fiscalização judicial.[71] A constituição dessas autoridades de controlo, é fundamental para garantir a proteção das pessoas singulares no que diz respeito ao processamento dos seus dados pessoais.

Por referência do art. 51.º, n.º 1 do RGPD, é a cada Estado-Membro incumbida a tarefa de estabelecer uma ou mais autoridades de controlo, responsáveis por fiscalizar a correta e coerente aplicação do regulamento em estudo. Os Estados-Membros devem ter a possibilidade de criar mais do que uma autoridade de controlo, de modo a refletir a sua estrutura constitucional, organizacional e administrativa. A autoridade de controlo responsável pela correta aplicação do RGPD em Portugal é a Comissão Nacional de Proteção de Dados.[72]

[70] A. Barreto Menezes Cordeiro (Coordenação), *Comentários ao Regulamento geral de proteção de dados e á Lei n.º 58/2019*, Coimbra, Almedina, 2021, pág. 94.
[71] Conforme consta do considerando (118) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[72] Conforme consta do art. 3.º, da Lei n.º 58/2019, de 8 de agosto.

3.2 Princípios do RGPD

No art. 5.º do capítulo II do RGPD, encontram-se consagrados os princípios que devem ser observados no que diz respeito ao tratamento de dados pessoais, sendo esses princípios essenciais para garantir que o tratamento de dados pessoais seja realizado de maneira correta e segura, assegurando a proteção do titular dos dados e permitindo que este exerça todos os direitos previstos pelo RGPD. A aplicação desses princípios reflete-se tanto nos direitos dos titulares dos dados, consagrados nos art. 12.º e ss do RGPD, quanto nas obrigações do responsável pelo tratamento, previstas nos art. 24.º e ss do RGPD.

O disposto no n.º 2 do artigo acima mencionado, diz-nos que é ao responsável pelo tratamento que é incumbida a responsabilidade e obrigação de fazer cumprir os princípios constantes no regulamento, tendo de o comprovar, sendo possível aqui observar um deles, nomeadamente o da responsabilidade, do qual será feita posteriormente uma análise.

Neste sentido, seguindo a ordem constante no art. 5.º, encontram-se mencionados os seguintes princípios: o princípio da licitude, lealdade e transparência; o princípio da limitação das finalidades; o princípio da minimização; o princípio da exatidão; o princípio da limitação da conservação; o princípio da integridade e da confidencialidade e por fim o princípio referido no parágrafo anterior.

Caso se verifique o incumprimento destes princípios, o responsável pelo tratamento incorre numa contraordenação muito grave, segundo o previsto nos termos do art. 83.º, n.º 5 al. a) do RGPD e o art. 37, n.º 1 al. a) da Lei n.º 58/2019, de 8 de agosto.[73]

Deste modo, passarei a analisar cada um dos princípios mencionados:

[73] A Lei n.º 58/2019, assegura a execução, na ordem jurídica nacional, do RGPD.

3.2.1 Princípio da Livre Circulação

Inicialmente, irei começar por abordar o princípio da livre circulação, que não se encontra mencionado no art. 5.º, mas sim no art. 1.º do RGPD. Este princípio tem sido abordado desde o início desta dissertação, principalmente quando começamos a falar do RGPD, pelo facto, de este regulamento existir para proteger o tratamento de dados pessoais das pessoas singulares e a livre circulação desses dados.

Perante uma sociedade democrática, alicerçada na economia de mercado e cada vez mais assente na economia digital, a proteção da circulação da informação, e consequentemente dos dados pessoais, é crucial para assegurar os direitos e as liberdades das pessoas singulares.[74] A proteção dos dados pessoais é um pilar fundamental para garantir a confiança nas relações económicas e sociais, prevenindo abusos e assegurando que os direitos dos indivíduos são respeitados num ambiente digital em constante evolução.

3.2.2 Princípio da Licitude, Lealdade e Transparência

O Princípio da licitude, lealdade e transparência consubstancia-se num dos pilares fundamentais do RGPD, que visa proteger a privacidade e os direitos dos titulares dos dados. Podemos aferir que este princípio está associado às condições em que os dados pessoais podem ser tratados, definindo como esse tratamento deve ser realizado.

Assim sendo, no art. 5.º, mais precisamente no n.º 1, al. a), faz referência a este princípio, dizendo que os dados pessoais são "objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados". Este princípio é concretizado principalmente através de três aspetos, nomeadamente as condições de licitude, consagrado no art. 6.º, o tratamento das categorias especiais de dados pessoais, previsto no art. 9.º e o dever de informar, relacionado com os direitos do titular dos dados, plasmado no art. 12.º e ss, todos os artigos mencionados do RGPD.

[74] Nuno Saldanha, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 43.

De seguida irei abordar cada um dos conceitos que compõem o princípio em análise:

3.2.2.1 Licitude

O princípio da licitude determina que o tratamento de dados pessoais deve ser realizado de forma lícita, ou seja, no tratamento deve ser cumprida a lei, não estando só em causa o RGPD, mas sim todos os diplomas em concreto aplicáveis, que tenham origem europeia ou nacional.[75]

O regulamento, diz-nos que para o processamento de dados pessoais ser considerado lícito, o mesmo deve ter por base as situações elencadas no art. 6.º do RGPD, assim sendo, no tratamento deve estar incluído o **consentimento**, ou seja, o titular dos dados tem de ter dado o seu consentimento explícito para que os dados sejam processados; a **execução de contrato**, o tratamento tem de ser necessário para a execução de um contrato no qual o titular dos dados é parte ou, então, para diligências pré-contratuais a pedido do titular; o **cumprimento de uma obrigação legal** em que o tratamento seja necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; a **proteção de interesses vitais**, no qual o tratamento seja necessário para proteger interesses vitais do titular dos dados ou de outra pessoa; o **interesse público ou exercício de autoridade pública**, ou seja, o tratamento seja necessário para o exercício de funções de interesse público ou de autoridade pública atribuída ao responsável pelo tratamento; e os **interesses legítimos do responsável pelo tratamento ou de terceiros**, quando o tratamento é necessário para os interesses legítimos do responsável ou de terceiros, apenas e caso esses interesses não se sobreponham aos direitos e liberdades do titular dos dados.[76]

Do exposto, é de salientar, a situação constante na al. a) do n.º 1 do art. 6.º que refere que o tratamento só é considerado lícito se "o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais, para uma ou mais finalidades

[75] A. Barreto Menezes Cordeiro (Coordenação), *Comentários ao Regulamento geral de proteção de dados e á Lei n.º 58/2019*, Coimbra, Almedina, 2021, pág. 102.
[76] Conforme consta do art. 6.º, n.ºs 1 da al. a) a f) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

específicas;". Nesta alínea é feita a alusão ao consentimento, conceito esse fundamental no que toca à temática da proteção de dados, já devidamente explicado na página 22 e 23 desta dissertação. Reiterar que o consentimento tem de ser prestado de forma livre. específico, informado e inequívoco.[77]

A verificação das situações anteriormente explanadas, garantem que o tratamento dos dados pessoais tenha uma fundamentação clara e adequada.

3.2.2.2 Lealdade

O princípio da lealdade, na sua essência, impõe que o responsável pelo tratamento, aquando do tratamento de dados pessoais, realize o tratamento tendo por base os critérios equitativos.[78] Este princípio exige que o responsável pelo tratamento assuma uma postura de honestidade, retidão e lealdade perante o titular dos dados, não devendo fazer uso de práticas desleais ou ocultas, que possam colocar os dados dos titulares em risco.

Ao responsável pelo tratamento ainda é exigido que, face à relação que estabelece com os titulares dos dados, satisfaça a todo o tempo os interesses e expectativas legítimas dos titulares dos dados pessoais.

A fim de cumprir o exposto, o responsável pelo tratamento, deve tomar todas as medidas adequadas de forma a manter os titulares dos dados informados do modo como os seus dados são tratados, devendo ainda ser capaz de demonstrar a conformidade das operações de tratamento realizadas com o RGPD. Essas informações podem ser apresentadas juntamente com ícones padronizados, de modo a fornecer uma visão geral clara, visível e facilmente compreensível sobre o tratamento previsto. No caso de serem

[77] Ana Francisca Pinto Dias, *Revista de Direito da Responsabilidade - Responsabilidade Civil pelo Tratamento de Dados Pessoais: A Responsabilidade do Controller por Factos Próprios e por Factos de Outrem*, Coimbra, Ano 1, 2019, pág. 1263 e 1264, disponível in Responsabilidade civil pelo tratamento de dados pessoais: a responsabilidade do controller por factos próprios e por factos de outrem – Ana Francisca Pinto Dias – Revista de Direito da Responsabilidade (27 abril 2025).
[78] Conforme consta do considerando (39) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

disponibilizados eletronicamente, os ícones devem ser facilmente legíveis de forma automática.[79]

3.2.2.3 Transparência

O princípio da transparência está relacionado com o princípio da lealdade, anteriormente falado, em que o legislador ao longo dos artigos do regulamento, bem como dos seus considerandos, estabelece essa ligação.

Com este princípio, o legislador, pretende que seja fornecido aos titulares dos dados, por parte do responsável pelo tratamento de dados, informações e comunicações relativas ao tratamento, de forma concisa, transparente, inteligível de fácil acesso, recorrendo sempre a uma linguagem clara e simples.[80]

Segundo o RGPD, aquando da recolha dos dados pessoais, deve ser fornecido ao titular dos dados, as seguintes informações: a identidade e detalhes de contato do responsável pelo tratamento ou em caso de tal o contato do encarregado da proteção de dados; as finalidades do tratamento de dados; as bases legais tidas em conta para o tratamento; quais os dados pessoais que serão recolhidos; os destinatários dos dados; qual o prazo de conservação dos mesmos; quais os direitos dos titulares[81] e das transferências internacionais.[82]

Segundo o art. 12.º, n.º 1 parte final, a informação deve ser prestada aos titulares dos dados pessoais por escrito ou por meios eletrónicos, nos casos em que o titular solicitar pode ser prestada verbalmente, sendo que a identidade do mesmo seja comprovada por outros meios que não o verbal.

[79] Conforme consta dos considerandos (60) e (71) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[80] Conforme consta do art. 12.º, n.º 1 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[81] Aqui, por exemplo, falamos do direito de acesso, de retificação, de apagamento e de limitação do tratamento de dados, o direito de oposição ao tratamento bem como o direito à portabilidade dos dados pessoais. Falamos ainda do direito que o titular tem em retirar o consentimento anteriormente prestado e, por conseguinte, o direito de apresentar uma reclamação.
[82] Conforme consta do art. 13.º, n.ºs 1 e 2 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

3.2.3 Princípio da Limitação das Finalidades

O princípio da limitação das finalidades, é uma peça fundamental deste regulamento, uma vez que só depois de ser determinada a finalidade do tratamento é possível avaliar se os dados pessoais recolhidos são adequados e não excessivos.

Posto isto, o art. 5.º, n.º 1 al. b) do RGPD, diz que os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas e, não podem ser tratados posteriormente de uma forma incompatível com essas finalidades, embora se admita o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica, ou para fins estatísticos.[83]

Desta forma, podemos aferir, que o tratamento de dados pessoais, no que toca ao princípio analisado, encontra-se limitado a finalidades determinadas, explícitas e legítimas, passando a explicar cada um destes pressupostos:[84]

Relativamente às **finalidades determinadas,** estas devem ser determinadas antes do processo de tratamento começar, isto significa dizer que a identificação das finalidades não pode ser adiada ou condicionada a um evento futuro, certo ou incerto.

Por conseguinte, as **finalidades explícitas,** significam que o responsável pelo tratamento, determina as finalidades a prosseguir e, consequentemente, após isto, deve informar os titulares dos dados, as autoridades competentes e terceiros dessas finalidades eleitas.

Por fim, as **finalidades legítimas**, é exigido que sejam respeitadas todas as disposições legais, aplicáveis a este tema. Deste modo, se estiverem em causa finalidades que violem a lei, as mesmas devem ser tidas como ilegítimas.

[83] Conforme consta do art. 5.º, n.ºs 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 art. 89.º, n.º 1 («limitação das finalidades»)" - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[84] A. Barreto Menezes Cordeiro (Coordenação), *Comentários ao Regulamento geral de proteção de dados e á Lei n.º 58/2019*, Coimbra, Almedina, 2021, pág. 104.

No RGPD, designadamente no art. 30.º, n.º 1, é dito que o responsável pelo tratamento de dados pessoais, em determinados casos, deve criar um registo de todas as atividades de tratamento. Pela análise da al. b) do mesmo artigo, este princípio é um dos casos em que é exigido a criação de um registo de todas as atividades de tratamento, prevendo a finalidade do tratamento.

3.2.4 Princípio da Minimização dos Dados

Analisando a al. c) do n.º 1 do art. 5.º do RGPD, é percetível que este princípio defende que só devem ser tratados os dados pessoais que sejam "adequados, pertinentes e limitados, ao que é necessário relativamente às finalidades para as quais são tratados".

Do exposto, é possível aferir, que este princípio é composto por três requisitos, nomeadamente os dados, devem ser **adequados**, devendo o responsável pelo tratamento restringir a recolha e o respetivo tratamento dos dados pessoais apenas às finalidades para que vão ser tratados; devem ser **pertinentes**, ou seja, os dados devem ser pertinentes face à finalidade do tratamento; e por fim deve ser **limitado**, significa que só devem ser recolhidos e tratados os dados efetivamente necessários para concretizar a finalidade definida.[85]

Por último, é importante destacar que o princípio da minimização dos dados está diretamente ligado ao princípio da limitação da finalidade e da limitação da conservação, uma vez que, os dados recolhidos e armazenados, devem ser reduzidos ao mínimo necessário e mantidos apenas pelo tempo estritamente necessário.

Além disso, a minimização está fortemente conectada com a proteção de dados, conforme o art. 25.º do RGPD, especialmente o n.º 2, que detalha as obrigações relacionadas à minimização dos dados.

[85] A. Barreto Menezes Cordeiro, *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*, Reimpressão, Coimbra, Almedina, 2020, pág. 158 e 159.

3.2.5 Princípio da Exatidão

O princípio da exatidão, consagrado no art. 5.º, n.º 1 al. d) do RGPD, exige que os dados pessoais devem ser exatos e que devem estar devidamente atualizados, devendo ser aplicadas todas as medidas adequadas para que os dados inexatos, sejam apagados ou retificados sem demora.

Posto isto, é possível referir que este princípio se subdivide em três dimensões, [86] designadamente:

- Primeira dimensão, a proibição de recolher ou de armazenar dados incorretos - Esta proibição aplica-se, exclusivamente, aos dados objetivos e não aos dados subjetivos.
- Segunda dimensão, o dever de, sempre que necessário, atualizar os dados recolhidos - a inexatidão dos dados pode ter um impacto significativo na vida dos titulares. No entanto, nem todos os dados precisam estar atualizados constantemente, uma vez que determinados dados são relevantes, ainda que, desatualizados, como no caso das informações médicas que refletem condições passadas. A inexatidão dos dados pode ser irrelevante dependendo das finalidades, sem afetar o tratamento ou os resultados das análises.
- Por fim, a terceira dimensão, o dever de, à luz das finalidades prosseguidas, apagar ou retificar os dados incorretos - As obrigações de eliminar ou corrigir dados incorretos não se confundem com o direito de solicitar a eliminação de dados, sejam incorretos ou não. Ainda assim, este princípio está relacionado com o direito de retificação consagrado no art. 16.º e com o apagamento dos dados consagrado no art. 17.º, ambos previstos no RGPD.

Este princípio acarreta benefícios tanto para o responsável pelo tratamento de dados bem como para o titular dos dados. Para o responsável, garante que o processamento não seja prejudicado por informações incorretas ou desatualizadas, devendo ser adotadas medidas para corrigir ou apagar rapidamente esses dados. Quanto

[86] A. Barreto Menezes Cordeiro (Coordenação), *Comentários ao Regulamento geral de proteção de dados e á lei Nº58/2019*, Coimbra, Almedina, 2021, pág. 105 e 106.

ao titular, existe um reforço da segurança, assegurando o cumprimento dos direitos de retificação e de limitação do tratamento dos dados pessoais.[87]

3.2.6 Princípio da Limitação da Conservação

O princípio da limitação da conservação no seu teor, indica que os dados pessoais deverão ser conservados de forma a permitir a identificação dos respetivos titulares, só durante o período necessário para as finalidades para as quais são tratados.[88] Desde logo é possível depreender que o legislador com este regulamento, mais especificamente com este princípio, visou minimizar o período/prazo de conservação dos dados pessoais, devendo os mesmos ser, o quanto antes, apagados.[89]

Pelo que cabe ao responsável pelo tratamento de dados, fixar os prazos relativos ao apagamento ou à revisão periódica da conservação dos dados pessoais, a fim de assegurar que a conservação de dados fique limitada ao período estritamente necessário.[90]

Contudo, os dados pessoais, podem ser conservados por um período de tempo mais alargado, nomeadamente quando estejam em causa situações como o tratamento exclusivo para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, segundo o art. 89.º e art. 5.º, n.º 1 al. e) II parte do RGPD.

[87] Ana Francisca Pinto Dias, *Revista de Direito da Responsabilidade - Responsabilidade Civil pelo Tratamento de Dados Pessoais: A Responsabilidade do Controller por Factos Próprios e por Factos de Outrem*, Coimbra, Ano 1, 2019, pág. 1270, disponível in Responsabilidade civil pelo tratamento de dados pessoais: a responsabilidade do controller por factos próprios e por factos de outrem – Ana Francisca Pinto Dias – Revista de Direito da Responsabilidade (27 abril 2025).
[88] Conforme se encontra previsto nos art. 5.º, n.º 1 al. e) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[89] A. Barreto Menezes Cordeiro (Coordenação), *Comentários ao Regulamento geral de proteção de dados e á Lei n.º 58/2019*, Coimbra, Almedina, 2021, pág. 106.
[90] Conforme consta do considerando (39) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

3.2.7 Princípio da Integridade e da Confidencialidade

Este princípio encontra-se consagrado na al. f) do n.º 1 do art. 5.º do RGPD, que nos diz que os dados pessoais são "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 («integridade e confidencialidade»)", ou seja, com este principio, o legislador, procura promover a segurança face ao tratamento de dados, impondo, consequentemente, ao responsável pelo tratamento e ao subcontratante a aplicação de medidas técnicas e organizativas adequadas a fim de assegurar um nível de segurança adequado ao risco.[91]

A implementação destas medidas visa garantir que as informações tratadas estão devidamente autorizadas, além de prevenir a perda, destruição ou danos aos dados. Visam ainda proteger as informações fornecidas pelo titular, impedindo o acesso ou a divulgação não autorizados, promovendo assim a segurança durante o tratamento dos dados.

Conforme já mencionado anteriormente, no caso de estarmos perante a violação dos dados pessoais, cabe ao responsável pelo tratamento e ao subcontratante comunicar tal violação à autoridade de controlo e/ ou responsável pelo tratamento, respetivamente.[92]

3.2.8 Princípio da Responsabilidade

O princípio da responsabilidade encontra-se consagrado no art. 5.º, n.º 2 e no art. 24.º do RGPD. Este princípio, no seu teor, consubstancia dois deveres para o responsável pelo tratamento, nomeadamente o dever de atuar de acordo com o correto cumprimento dos princípios elencados no primeiro artigo, acima indicado, e, por conseguinte, o dever de poder comprovar à autoridade de controlo que adotou as medidas técnicas e

[91] No art. 32.º, n.º 1 al. a) a d), temos alguns exemplos de medidas técnicas e organizativas adequadas para assegurar a segurança no tratamento, nomeadamente: a pseudonimização e a cifragem dos dados pessoais; a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico e um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

[92] Conforme se encontra previsto no art. 33.º e 34.º - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

organizativas adequadas ao cumprimento de todos os princípios anteriormente mencionados.

O legislador coloca ao dispor do responsável pelo tratamento de dados, dois métodos de poder comprovar o cumprimento dos princípios estabelecidos por este regulamento, nomeadamente os códigos de conduta previstos no art.s 40.º e 41.º e os procedimentos de certificação previstos no art. 42.º, todos do RGPD.[93] Ambos os mecanismos, são facultativos, isto significa que é o responsável pelo tratamento que deve decidir a qual deles adotar, ou aderir a uma determinada conduta ou solicitar uma certificação.[94]

No caso de se verificar o incumprimento do princípio da responsabilidade, o responsável pelo tratamento estará a incorrer numa contraordenação muito grave, segundo o previsto e sancionado no art. 83.º, n.º 5, al. a) do RGPD e do art. 37.º, n.º 1, al. a) e n.º 2 da Lei n.º 58/2019.[95]

[93] Conforme se encontra previsto no art. 24.º, n.º 3 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[94] Ana Francisca Pinto Dias, *Revista de Direito da Responsabilidade - Responsabilidade Civil pelo Tratamento de Dados Pessoais: A Responsabilidade do Controller por Factos Próprios e por Factos de Outrem*, Coimbra, Ano 1, 2019, pág. 1274, disponível in Responsabilidade civil pelo tratamento de dados pessoais: a responsabilidade do controller por factos próprios e por factos de outrem – Ana Francisca Pinto Dias – Revista de Direito da Responsabilidade (27 abril 2025).

[95] As coimas podem ir até 20 milhões de euros, ou 4%, caso se fale de empresas.

3.3 Direitos dos Titulares dos Dados Pessoais

Ao longo do RGPD o legislador confere aos titulares dos dados pessoais um conjunto de direitos que lhes permitem controlar a forma como os seus dados são tratados. Os principais direitos incluem o **direito à informação**, deve ser informado sobre a recolha e uso dos seus dados; o **direito de acesso**, tem a faculdade de aceder aos dados pessoais que estão a ser tratados; o **direito de retificação**, pode corrigir os dados imprecisos ou incompletos; o **direito ao apagamento** (também conhecido como o direito a ser esquecido), pode solicitar a eliminação dos dados quando o tratamento seja considerado ilícito; o **direito à limitação do tratamento**, tem o direito de limitar o tratamento dos dados em determinadas circunstâncias; o **direito à portabilidade dos dados**, pode receber os dados num formato estruturado, de uso corrente e transmiti-los a outro responsável; o **direito de oposição**, pode opor-se ao tratamento dos dados, nomeadamente para fins de marketing direto; e o **direito de não sujeição a decisões automatizadas**, é lhe dado o direito de não ser sujeito a decisões baseadas unicamente no tratamento automatizado, incluindo a definição de perfis.

Estes direitos consubstanciam-se num conjunto de garantias fundamentais, que visam proteger a privacidade dos indivíduos. Permitem aos titulares terem controlo sobre os seus dados, podendo, entre outras ações, aceder, retificar, apagar ou restringir o tratamento dos seus dados. O principal objetivo é assegurar a transparência no processamento dos dados e garantir que sejam utilizados de forma justa, segura e lícita.

Deste modo, passarei a analisar os principais direitos dos titulares elencados no primeiro parágrafo.

3.3.1 Direito à Informação

O **direito à informação** consubstancia-se num dos pilares fundamentais do regulamento, desempenhando um papel central na salvaguarda dos demais direitos dos titulares. Uma comunicação que tenha por base a transparência, no que diz respeito ao tratamento dos dados pessoais, permite um exercício correto dos direitos de acesso, de retificação, de oposição e de portabilidade.

Nos termos do art. 12.º, n.º 1, bem como do considerando (39), a informação prestada ao titular deve obedecer a alguns critérios como **clareza, concisão e acessibilidade**, recorrendo a uma linguagem compreensível e adaptada ao público-alvo. Além disso, a comunicação deve ser realizada de forma **transparente e inteligível**, garantindo que os titulares compreendem plenamente o modo como os seus dados são tratados.

Relativamente a este direito, temos dois pontos de vista diferentes. Por um lado, temos os dados pessoais recolhidos junto do titular e por outro temos os dados que são obtidos por meios indiretos, ou seja, que não são recolhidos junto dos titulares. No art. 13.º, temos os casos em que o responsável recolhe os dados junto do titular, devendo este informar o titular, no momento da recolha, sobre a sua identidade, o contacto do EPD, a finalidade do tratamento e a base legal aplicável, os destinatários dos dados e os seus direitos. Por sua vez, no art. 14.º abordas os casos em que o responsável não recolhe os dados junto do titular sendo aqui impostas obrigações informativas similares, acrescendo a exigência de indicar a categoria dos dados em análise.

Existem ainda algumas exceções ao direito à informação, que permitem que hajam algumas restrições no seu uso, de acordo com a base legal atrás analisada, sendo que a informação a prestar ao titular pode ser dispensada quando este já tenha conhecimento das informações; quando a prestação da informação se revela impossível ou implica um esforço desproporcional; quando a obtenção ou divulgação dos dados esteja prevista pelo direito da União ou dos Estado-Membros; e nos casos em que os dados estejam sujeitos a obrigações de confidencialidade ou sigilo profissional.

Por fim, acresce dizer que para além do RGPD, existem outras bases legais que salvaguardam os indivíduos, no que toca ao direito à informação, nomeadamente a CRP, mais precisamente no art. 35.º, que estabelece garantias fundamentais no âmbito da proteção de dados pessoais e do acesso à informação,[96] visando assegurar que qualquer

[96] Este direito encontra-se ainda reforçado por outros artigos da CRP, nomeadamente o art. 26.º e o art. 37.º com a seguinte epigrafe, respetivamente, "outros direitos pessoais" e "liberdade de expressão e informação".

cidadão tem o direito de ser informado sobre o processamento dos seus dados e de exercer controlo sobre os mesmos.

3.3.2 Direito de Acesso

O **direito de acesso** encontra-se previsto no art. 15.º do RGPD, que nos diz que é atribuído ao titular dos dados o direito de obter, por parte do responsável pelo tratamento, a confirmação se os seus dados pessoais são ou não objeto de tratamento e, em caso disso, tem a faculdade de aceder aos seus dados pessoais e às informações elencadas da alínea a) à h) do art. em análise.

No caso de o titular dos dados pessoais, solicitar o acesso aos mesmos, cabe ao responsável pelo tratamento verificar a sua identidade.[97] É então após essa verificação, que o responsável pelo tratamento deve fornecer uma cópia dos dados pessoais em fase de tratamento.

Se o titular solicitar a cópia uma única vez a mesma deve ser gratuita,[98] excetuando-se os casos em que o titular solicitar mais do que uma cópia, aqui o responsável pelo tratamento pode exigir que o titular pague uma taxa razoável, atendendo aos custos administrativos, conforme o elencado no n.º 3 do art. 15.º do regulamento.

3.3.3 Direito de Retificação

Relativamente ao **direito à retificação**, este encontra-se consagrado no art. 16.º o qual pode ser dividido em duas partes, uma relacionada com os dados inexatos e outra relacionada com os dados incompletos. Relativamente aos dados pessoais inexatos é dito que "o titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento, a retificação dos dados pessoais inexatos", isto significa que o titular dos

[97] Conforme consta do considerando (64) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[98] Conforme se encontra previsto no art. 12.º, n.º 5 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

dados pessoais, caso verifique que os dados armazenados por uma determinada organização se encontram incorretos, pode solicitar que essa informação seja devidamente corrigida, essa correção deve ser feita pelo responsável pelo tratamento dos dados dentro de um prazo razoável, atendendo à complexidade do pedido. Ao proceder a esta correção, solicitada pelo titular, o responsável consegue garantir que os dados pessoais em tratamento se encontram exatos e atualizados.

Ainda no art. 16.º, na segunda parte, é dito que "o titular dos dados tem direito a que os dados pessoais incompletos sejam completados" ou seja, no caso de os dados pessoais de um determinado titular estarem incompletos, este tem o direito de solicitar que os dados sejam complementados, de forma a garantir que os mesmos estejam corretos e devidamente completos. Nestes casos pode estar em causa a adição de informações que estejam em falta, evitando assim possíveis erros ou interpretações erradas, por exemplo, se um registo contém apenas o primeiro nome de uma pessoa, isto pode causar confusões, uma vez que pode haver mais do que um titular com o mesmo nome, assim, o titular, pode solicitar que ao primeiro nome seja adicionado o seu sobrenome.

O titular dos dados, para dar início à correção ou complementação dos dados deve realizar o respetivo pedido nos termos do art. 12.º do RGPD,[99] mal seja rececionado este pedido o responsável pelo tratamento deve proceder à retificação ou à complementação dos dados pessoais do titular, sem demora injustificada, devendo ainda notificar cada destinatário a quem tenham sido transmitidos os dados da retificação de dados pessoais.[100]

[99] "O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os art.s 13.º e 14.º e qualquer comunicação prevista nos art.s 15.º a 22.º e 34.º a respeito do tratamento, 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. **As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos.** Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios." - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[100] Conforme se encontra previsto no art. 19.º - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

3.3.4 Direito ao Apagamento de Dados

O **direito ao apagamento dos dados** também conhecido como direito a ser esquecido encontra-se definido no art. 17.º do regulamento, aqui é estabelecido que "o titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada (...)" no caso de os dados pessoais deixarem de ser necessários para a finalidade para a qual foram obtidos; de retirar o consentimento; se oponha ao tratamento; se os dados pessoais forem tratados ilicitamente; se os dados tiverem de ser apagados para o cumprimento de alguma obrigação jurídica e se os dados forem recolhidos no contexto da oferta de serviços de sociedade da informação.[101]

Contudo, existem situações em que não é possível ao titular dos dados pessoais exercer o direito de apagamento, ou seja, existem dados pessoais que deverão continuar a ser tratados da forma licita sempre que se revele necessário para o exercício do direito de liberdade de expressão e informação; para o cumprimento de uma obrigação jurídica; para o exercício de funções de interesse público ou o exercício da autoridade pública; por razões de interesse público, no domínio da saúde pública; para fins de arquivo de interesse público; para fins de investigação científica ou histórica; para fins estatísticos e para efeitos de declaração, exercício ou defesa de um direito num processo judicial.[102]

3.3.5 Direito à Limitação do Tratamento

No presente regulamento encontra-se consagrado o **direito à limitação do tratamento**, conforme já foi anteriormente explicado,[103] depreende-se por limitação do tratamento de dados "a inserção de uma marca nos dados pessoais conservados com o

[101] Conforme se encontra previsto no art. 17.º, n.º 1 da al. a) a f) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[102] Conforme se encontra previsto no art. 17.º, n.º 3 da al. a) a e) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[103] Ver pág. 18 e19 desta dissertação.

objetivo de limitar o seu tratamento no futuro;" conforme plasmado no n.º 3 do art. 4.º do RGPD.

Este direito confere ao titular dos dados, a possibilidade de limitar durante um certo período de tempo a utilização dos seus dados pessoais. Durante este período, o tratamento dos dados fica como que "congelado", impedindo que sejam feitas determinadas coisas, como a comunicação a terceiros, a transferência internacional ou a sua eliminação.

O titular dos dados pessoais, pode invocar este direito perante o responsável pelo tratamento em diversas situações, designadamente: quando o titular contestar a exatidão dos dados pessoais;[104]quando estiver em causa um tratamento de dados ilícitos; nos casos em que os dados já não sejam necessários para o responsável;[105] e quando o titular realize o pedido de oposição ao tratamento,[106] constante no art. 21.º, n.º 1 do regulamento.[107]

Nesta situação, o titular deve ser informado pelo responsável pelo tratamento antes de ser anulada a limitação do tratamento, assegurando transparência em todo o processo e garantido que o direito à informação é respeitado. Durante o espaço de tempo em que o tratamento se encontra limitado, os dados pessoais apenas podem ser tratados quando o titular der o seu consentimento, quando seja para efeitos de exercício de um direito em processos judiciais, de defesa de direitos de terceiros ou por razões imperiosas de interesse público.

Pelo que, é possível concluir, que o direito à limitação do tratamento revela-se um instrumento essencial, no que toca à matéria da proteção de dados, uma vez que permite obter, por parte do titular dos dados um maior controlo sobre a utilização dos seus dados.

[104] Importa referir que a limitação ao tratamento irá manter-se até ao momento em que o responsável pelo tratamento de dados verifique a sua exatidão.
[105] Contudo o titular dos dados pessoais pode requerer na mesma a sua conservação para efeitos de exercício de um direito num processo judicial.
[106] Esta limitação acontece até ao momento em que se verifique que os motivos legítimos do responsável prevalecem sobre os do titular dos dados, conforme consta do n.º 1 al. d) do art. 18.º - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[107] Conforme se encontra previsto no art. 18.º, n.º 1 da al. a) a d) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

3.3.6 Direito de Portabilidade dos Dados

O **direito à portabilidade dos dados** é uma das novidades que o legislador incorporou no RGPD, que não se encontrava na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, encontrando-se explanado no art. 20.º do regulamento. Este direito representa uma inovação na proteção dos direitos dos titulares, permitindo que estes peçam a transferência dos seus dados pessoais entre diferentes serviços ou plataformas.

O exercício deste direito está condicionado a determinadas bases legais, nomeadamente quando o tratamento dos dados assenta no **consentimento** do titular dos dados, na **execução de um contrato** em que o titular é parte e em **diligências pré-contratuais** a pedido do titular. Assim, o titular dos dados, tem direito a receber os seus dados num formato estruturado, de uso corrente e de leitura automática, de forma que permitam a sua portabilidade, por exemplo para outra plataforma, a transmitir os seus dados diretamente entre responsáveis pelo tratamento, a exercer este direito apenas sobre os dados que forneceu.[108]

O RGPD impõe algumas restrições ao uso deste direito, especialmente em situações onde o tratamento dos dados seja necessário para o exercício de funções de interesse público e para o exercício da autoridade pública pelo responsável pelo tratamento. Este direito não se aplica a dados inferidos ou derivados, ou seja, não abrange informações criadas pelo responsável após tratar os dados fornecidos ou observados. A disponibilização dessas informações poderia comprometer a liberdade de iniciativa económica e a proteção de segredos de negócio, expondo algoritmos dos proprietários ou modelos preditivos a concorrentes.[109]

É importante enaltecer que o exercício do direito à portabilidade, pelo titular dos dados, não prejudica o exercício do direito ao apagamento, conforme o art. 20.º n.º 3.

[108] Conforme consta do considerando (68) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[109] Universidade de Coimbra - Direito de Portabilidade dos Dados, disponível in Direito de portabilidade dos dados (27 abril 2025).

3.3.7 Direito de Oposição

De acordo com o art. 21.º do regulamento, que consagra o **direito de oposição**, é conferido ao titular o direito de se opor, a qualquer momento e por razões relacionadas com a sua situação pessoal, ao tratamento dos seus dados. Este direito é aplicável quando a operação de tratamento se fundamenta no interesse público, nos interesses legítimos do responsável pelo tratamento ou de terceiros ou na reutilização de dados para uma finalidade diferente (mas compatível) da que motivou a recolha inicial, incluindo a definição de perfis.[110]

Assim que seja rececionado o pedido, o responsável deve cessar o tratamento dos dados pessoais, salvo se demonstrar razões imperiosas e legítimas que prevaleçam sobre os direitos, liberdades e interesses do titular, ou se o tratamento for necessário para o exercício de um direito num processo judicial, conforme a segunda parte do n.º 1 do art. 21.º do RGPD.

O exercício deste direito pode ser complementado com um pedido de apagamento, apresentado pelo titular dos dados, nos termos do art. 17.º, n.º 1, alínea c) do RGPD, ficando o responsável pelo tratamento obrigado a apagar os dados pessoais do titular.

3.3.8 Direito a não ficar sujeito a decisões individuais automatizadas

O **direito a não ficar sujeito a decisões individuais automatizadas** encontra-se consagrado no art. 22.º do RGPD, onde diz que "o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar."[111]

Entende-se por decisões individuais automatizadas, aquelas decisões resultantes exclusivamente do processamento automatizado de dados pessoais, sem que haja

[110] Conforme costa do art. 6.º, n.º 1 al. e) e f) e n.º 4, respetivamente - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[111] Conforme costa do art. 22.º, n.º 1 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

intervenção humana, utilizando meios tecnológicos para determinar um resultado que afeta diretamente o titular dos dados.[112]

No n.º 2, nas diversas alíneas que o compõem, encontram-se elencados três situações, nas quais não se aplica este conceito da não sujeição a decisões individuais automatizadas, nomeadamente quando as decisões forem necessárias para a celebração ou a execução de um contrato, entre o titular e o responsável; forem autorizadas pelo direito da União ou do Estado-Membro a que o responsável estiver sujeito ou se forem baseadas no consentimento explícito do titular dos dados pessoais, nestas situações o titular dos dados não consegue invocar este direito.

Em suma, os direitos dos titulares dos dados pessoais constituem um pilar essencial na proteção da privacidade e no reforço do controlo sobre as suas próprias informações. Garantem transparência no tratamento de dados, permitindo aos indivíduos conhecer, aceder, retificar, apagar, limitar ou transferir os seus dados, bem como opor-se ao seu tratamento em determinadas circunstâncias. Além disso, asseguram que decisões automatizadas que afetem significativamente os titulares sejam devidamente reguladas. A efetividade destes direitos é fundamental para equilibrar o avanço tecnológico, com a salvaguarda dos direitos e liberdade individuais, promovendo um tratamento de dados mais justo, seguro e responsável. Podemos ainda referir, que a cada um destes direitos, cabe uma obrigação, por parte do responsável, de tomar as devidas medidas técnicas ou organizativas, para corresponder às solicitações que lhe são dirigidas.[113]

[112] Conforme Diário da República, direito à não sujeição a decisões individuais automatizadas, disponível in Direito de não sujeição (a decisões individuais automatizadas) | DR (27 abril 2025).

[113] Nuno Saldanha, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 53.

4 O Responsável pelo Tratamento e o Subcontratante

É no decorrer do capítulo IV do RGPD, que o legislador, de forma detalhada, elenca quem é o responsável pelo tratamento e quem é o subcontratante, quais as suas obrigações perante os titulares dos dados pessoais e qual a relação estabelecida entre estas duas figuras, também denominadas por controller e processor, respetivamente, na terminologia inglesa. No que diz respeito à temática da proteção de dados, estes desempenham um papel fulcral no cumprimento das obrigações legais estabelecidas no regulamento da proteção de dados.

Conforme já referido nesta dissertação,[114] o r**esponsável pelo tratamento** é a entidade ou pessoa que determina as finalidades e os meios de tratamento dos dados pessoais, assumindo a responsabilidade direta pela conformidade legal. Por sua vez, o **subcontratante** é a entidade ou pessoa que realiza o tratamento dos dados em nome do responsável, seguindo as instruções deste e atuando sob a sua supervisão.

Ambos têm obrigações específicas e complementares no que diz respeito à proteção de dados, devendo a sua relação ser regulada por um contrato ou ato normativo que vincule o subcontratante ao responsável pelo tratamento, onde se encontre estabelecido o objeto e a duração, a natureza e finalidade do tratamento, o tipo de dados e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento.[115]

Posto isto, de seguida, irei abordar novamente os conceitos de responsável pelo tratamento e de subcontratante, mas de forma mais detalhada, seguindo-se a explanação das obrigações imputadas a cada um deles.

[114] Ver pág. 21 e 22 desta dissertação.
[115] Conforme consta do art. 28.º, n.º 3 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

4.1 Conceito de Responsável pelo Tratamento (Controller) e as suas obrigações

O **Responsável pelo Tratamento de Dados**, também designado por *Controller*, desempenha um papel central no contexto da proteção de dados pessoais, sendo a entidade que define os objetivos e os meios do tratamento dessas informações. De acordo com o RGPD, este, pode ser uma pessoa singular ou coletiva, autoridade pública, agência ou qualquer outro organismo que, de forma isolada ou em conjunto com outros, determina a forma como os dados pessoais são processados.[116]

A qualificação como *Controller* implica uma elevada responsabilidade no cumprimento das regras estabelecidas pelo RGPD, assegurando que todas as operações relacionadas ao tratamento de dados pessoais sejam realizadas de maneira transparente, segura e conforme os princípios legais, sendo este, efetivamente, quem controla os dados dos titulares dos dados pessoais.[117]

Ao longo do RGPD, o legislador estabeleceu diversas obrigações que devem ser cumpridas pelo responsável pelo tratamento de dados, de forma a garantir a proteção dos direitos e liberdades dos titulares dos dados. Neste sentido, **a primeira obrigação**, aparece elencada no art. 5.º, n.º 2 do regulamento, que determina ser responsabilidade do *Controller* **assegurar o cumprimento de todos os princípios do tratamento de dados pessoais**,[118] devendo este ser capaz de demonstrar a conformidade com o regulamento, ficando claro que o responsável pelo tratamento assume todas as obrigações definidas pelo legislador ao longo do regulamento, incorporando-se no chamado princípio da responsabilidade.[119]

[116] Conforme consta do art. 4.º, n.º 7 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[117] Nuno Saldanha, Novo Regulamento Geral de Proteção de Dados – *O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 73.
[118] Trata-se do princípio da licitude, da lealdade e transparência; da limitação da finalidade; da minimização dos dados; da exatidão; da limitação da conservação; da integridade e confidencialidade.
[119] Patrícia Andreia Batista Santos (2019) - "*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*" (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, disponível in RUN: A aplicação do novo regulamento geral de proteção de dados no contexto laboral (27 abril 2025).

Além da obrigação acima elencada, o legislador, ao longo do regulamento, enumera outras obrigações que o responsável pelo tratamento de dados deve ter em conta, nomeadamente:

- **Implementar medidas técnicas e organizativas** – Segundo o art. 24.º, n.º 1, o responsável pelo tratamento deve adotar medidas eficazes, com o objetivo de assegurar que o tratamento é realizado em conformidade com o regulamento;
- **Comprovar (*accountability*) que adotou as medidas adequadas –** Cabe ao responsável pelo tratamento implementar e demonstrar que adotou as medidas técnicas e organizativas necessárias a fim de garantir a conformidade com o regulamento. O princípio da **accountability**, além de exigir o cumprimento das regras do regulamento, também exige que esta entidade esteja em plenas capacidades de o comprovar, por meio de documentação, auditorias e monitoramento contínuo, isso inclui a implementação de políticas de privacidade e segurança, avaliação de riscos, registos de tratamento de dados, assegurando um tratamento de dados transparente e seguro, para além de que assim consegue evitar que lhe sejam aplicadas sanções e protege os direitos dos titulares dos dados;[120]
- **Definir políticas adequadas** – Esta obrigação encontra-se enumerada no art. acima referido, no seu n.º 2, devendo o responsável pelo tratamento adotar políticas internas proporcionais aos riscos associados ao processamento de dados pessoais, englobando a criação de diretrizes sobre a privacidade, a segurança da informação e os direitos dos titulares, bem como a realização de avaliações de risco. Além disso, é fundamental realizar revisões e atualizações contínuas das políticas, a fim de as adaptar a novas ameaças e

O princípio da responsabilidade encontra-se inserido no conceito de *accountability* (responsabilidade), ou seja, o responsável pelo tratamento para além de ser obrigado a executar todas as medidas necessárias, adequadas e eficazes de forma a garantir o cumprimento do RGPD, também está obrigado a comprovar que tomou essas medidas e que as mesmas são realmente eficazes ou que, pelo menos, reduzem os riscos para os direitos e liberdades dos titulares dos dados pessoais.

[120] Conforme se encontra previsto no art. 24.º, n.º 1 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

regulamentações, bem como implementar auditorias e avaliações periódicas. Em suma, o artigo reforça a importância de não só cumprir o RGPD, como de formalizar políticas claras, documentadas e adaptadas à realidade, assegurando um tratamento seguro e responsável dos dados pessoais.

Com fundamento no que foi dito é possível verificar que estas três obrigações se encontram interligadas e que se complementam em entre si, sendo fulcrais para garantir que os princípios salvaguardados pelo RGPD sejam devidamente cumpridos. É possível, ainda, verificar que estamos perante um ciclo contínuo, uma vez que, primeiramente, as medidas técnicas e organizativas são implementadas, posteriormente, estas devem ser comprovadas e sustentadas por políticas internas bem definidas que, consequentemente, garantem a revisão e a melhoria constante da conformidade com o RGPD**.**

Continuando a enumerar e a explicar as obrigações impostas ao responsável pelo tratamento de dados ao longo do regulamente, este deve:

- **Adotar medidas de proteção de dados desde a conceção e por defeito**[121] – Desmembrando esta obrigação em duas, começando por falar da proteção de dados desde a conceção, isto significa, que o responsável pelo tratamento, deve integrar medidas de segurança e privacidade, logo desde a fase inicial, ou seja, antes de dar início ao tratamento de dados, devem ser avaliados os riscos e adotadas medidas técnicas e organizativas para minimizar tais riscos, como por exemplo, a anonimização, pseudonimização e o controlo de acessos. Passando para a proteção de dados por defeito, assegura que, por definição, apenas os dados pessoais estritamente necessários para a finalidade pretendida sejam tratados. Com esta medida, o legislador procura limitar a quantidade de dados recolhidos, o tempo de conservação e o acesso aos

[121] Conforme se encontra previsto no art. 25.º, n.º 1 e 2, respetivamente- do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

dados, garantindo que apenas as pessoas autorizadas tenham acesso à informação.[122]

- **Proceder ao registo das atividades de tratamento –** De forma a atestar a correta aplicação do presente regulamento, de acordo com o art. 30.º, o responsável pelo tratamento deve conservar um registo de todas as atividades de tratamento realizadas sob a sua responsabilidade. Esses registos, podem ser efetuados por escrito ou em formato eletrónico, devendo ser disponibilizados à Autoridade de Controlo, quando esta os requisitar.[123] Os registos das atividades de tratamento de dados pessoais devem conter vários elementos, nomeadamente a identificação do responsável; os objetivos do tratamento; as categorias dos dados recolhidos e os seus destinatários; no caso de os dados serem enviados para países fora da UE, deve constar a identificação desses países terceiros e das garantias de proteção aplicadas; os prazos previstos para o apagamento e sendo possível a descrição das medidas de seguranças.[124]

  Desta obrigação é possível depreender que o responsável deve **cooperar com as Autoridades de Controlo**, conforme o art. 31.º do RGPD, no desempenho das suas funções, facultando-lhe todas as informações pedidas, bem como os documentos que comprovem a conformidade com o regulamento. Esta obrigação, visa garantir que haja uma supervisão eficaz da aplicação do regulamento, promovendo a transparência, a proteção dos dados pessoais e a responsabilização das organizações no cumprimento das normas de privacidade e segurança da informação.

[122] Comissão Europeia - *"O que significa a proteção de dados «desde a conceção» e «por defeito»?"*, disponível in O que significa a proteção de dados «desde a conceção» e «por defeito»? - Comissão Europeia (27 abril 2025).
[123] Conforme consta do considerando (82) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
Acresce mencionar, que as obrigações mencionadas no n.º 1 e 2 do art. 30.º não se aplicam quando estejam em causa empresas com um número de trabalhadores inferior a 250, salvo exceção se o tratamento for suscetível de causar um certo risco face aos direitos e liberdades dos titulares dos dados pessoais, segundo o n.º 5 do art. mencionado.
[124] Conforme se encontra previsto no art. 30.º, n.º 1 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Seguindo o raciocínio e a orientação do RGPD, irei agora abordar três obrigações que se encontram interligadas, e que estão relacionadas com a segurança dos dados pessoais, assim sendo, o responsável, deve:

- **Adotar medidas técnicas e organizativas a fim de assegurar um nível de segurança adequado ao risco** – Atendendo ao art. 4.º, n.º 12 uma possível violação da segurança pode causar "de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento", assim, com esta obrigação, o legislador pretende assegurar um nível de segurança adequado ao risco, evitando possíveis violações de segurança. Pelo que, cabe ao responsável adotar todas as medidas necessárias e proporcionais aos riscos inerentes ao respetivo tratamento, devendo ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como a probabilidade e gravidade de uma possível violação de dados.[125] Quanto às **medidas técnicas**, o legislador no regulamento, faz referência, por exemplo, à utilização da pseudonimização[126] e da cifragem. Por sua vez, quanto às **medidas organizativas**, o legislador refere-se à definição de políticas de segurança da informação, à formação e sensibilização dos colaboradores, à implementação de procedimentos para resposta a incidentes de segurança e à realização de auditorias regulares para avaliar a eficácia das medidas aplicadas. A implementação destes dois tipos de medidas, garante a confidencialidade, a integridade e a disponibilidade dos dados pessoais, assegurando a proteção dos direitos e liberdades dos titulares e reforçando a conformidade da organização com o RGPD.
- **Notificar a Autoridade de Controlo, caso sejam violados os dados pessoais** - Esta obrigação encontra-se prevista ao longo do art. 33.º do RGPD e tem como finalidade garantir uma resposta rápida e transparente face a incidentes que comprometam a segurança dos dados pessoais. Caso ocorra

[125] Conforme se encontra previsto no art. 32.º, n.º 1 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[126] Ver explicação na pág. 20 desta dissertação.

uma violação de dados, cabe ao responsável, notificar a Autoridade de Controlo competente,[127] no prazo máximo de 72 horas após ter tido conhecimento do incidente, exceto se a violação não representar quaisquer riscos para os direitos e liberdades dos titulares dos dados. Essa notificação deve conter uma descrição simples e clara da violação, incluindo a natureza dos dados afetados, o número aproximado de titulares envolvidos e os potenciais impactos para os mesmos. Deve ainda apresentar as medidas adotadas para mitigar os efeitos da violação e fornecer os contactos do EPD, se existir, para esclarecimentos adicionais. Esta obrigação assegura que a Autoridade de Controlo possa monitorizar a situação, orientar o responsável pelo tratamento na mitigação dos riscos e reforçar a proteção dos dados pessoais, promovendo a transparência e a salvaguarda dos direitos dos titulares.

- **Comunicar, a violação de dados pessoais ao titular dos dados**[128] – Esta obrigação alerta-nos que o responsável pelo tratamento, não se encontra apenas obrigado a notificar a Autoridade de Controlo, este deve, em caso de violação dos dados, comunicar aos titulares dos dados, sempre que essa violação representar um grave risco para os direitos e liberdades destes, permitindo-lhes tomar as devidas precauções. Essa comunicação deverá descrever a natureza da violação dos dados de forma clara e simples, devendo ser efetuada logo que seja possível, em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia.[129]

[127] Cada país da UE tem uma Autoridade de controlo responsável por garantir o cumprimento das regras de proteção de dados, por exemplo no caso de Portugal é a CNPD a autoridade competente por fiscalizar, aplicar sanções e garantir o cumprimento das normas estabelecidas no regulamento. Acresce dizer que a Autoridade de Controlo só tem jurisdição dentro do seu próprio território, ou seja, não pode atuar diretamente noutro país, conforme consta do art. 55.º - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[128] Conforme se encontra previsto no art. 34.º - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[129] Tanto a notificação feita à Autoridade de Controlo como a notificação feita aos titulares dos dados, o responsável pelo tratamento de dados, deve fazê-lo sem demora injustificada - conforme consta do considerando (86) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Tendo em conta que alguns tratamentos de dados são suscetíveis de implicar um elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto ou finalidade, o responsável pelo tratamento está obrigado proceder, a uma avaliação do impacto dessas operações de tratamento e à consulta prévia. Assim, o responsável pelo tratamento, deve:

- **Proceder à AIPD e à Consulta Prévia** - Sempre que a operação de tratamento de dados apresente um elevado risco para os direitos e liberdades dos titulares dos dados, é obrigatório realizar uma AIPD prévia ao tratamento de dados, conforme previsto n.º 1 do art. 35.º do RGPD. A avaliação de impacto é um processo que ajuda as organizações a identificar e a minimizar os riscos, a avaliar as necessidades do tratamento, a gerir os riscos para os direitos e liberdades das pessoas e a determinar as medidas necessárias para fazer face a esses riscos.[130] Esta avaliação é obrigatória quando o tratamento de dados for suscetível de representar um alto risco para os titulares; quando há uma análise detalhada e automatizada dos dados pessoais para avaliar ou prever aspetos como trabalho, situação financeira, saúde, preferências e localização, podendo impactar legalmente a pessoa; quando são tratados dados sensíveis, como informações de saúde ou antecedentes criminais, em grande escala e quando existe uma monitorização constante de espaços públicos em grande escala.[131] A avaliação deverá incluir, as medidas, garantias e procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância do RGPD.[132] Neste seguimento, o responsável, deve recorrer à **consulta prévia** da Autoridade de Controlo, antes de proceder ao tratamento, nos casos em que AIPD indique que desse tratamento resultaria num elevado risco na ausência de medidas tomadas a fim de atenuar o risco, conforme consta do art. 36.º, n.º 1. A consulta prévia à Autoridade de Controlo obriga a uma conjunto de

[130] Nuno Saldanha, Novo Regulamento Geral de Proteção de Dados – *O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 103.
[131] Ibidem
[132] Conforme consta do considerando (90) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

procedimentos e comunicações, nomeadamente a indicação da repartição de responsabilidades entre o responsável e o subcontratante, das finalidades e dos meios previstos para o tratamento, das medidas e garantias previstas para a defesa dos direitos e liberdades dos titulares, a comunicação do EPD, apresentação da AIPD e disponibilizar informações adicionais.[133]

- **Designar um Encarregado de Proteção de Dados** – O EPD desempenha um papel essencial no cumprimento do regulamento, auxiliando na aplicação das suas normas. Contudo, ainda que seja nomeado um encarregado, a responsabilidade pelo cumprimento continua a ser do responsável pelo tratamento ou do subcontratante. Além disso, o EPD atua como intermediário entre a Autoridade de Controlo, os titulares dos dados e as organizações.[134] Em alguns, casos é obrigatório designar um encarregado, pois, segundo o art. 37.º do regulamento, todas as entidades públicas,[135] independentemente da natureza de dados tratados, estão obrigadas a nomear um EPD.[136] O responsável pelo tratamento e o subcontratante asseguram que o EPD é envolvido nas questões relacionadas com a proteção de dados, conforme menciona o art. 38.º do regulamento.
- **Adotar códigos de conduta e procedimentos de certificação** – Sempre que for possível, as associações ou outras entidades que representem os responsáveis pelo tratamento ou os subcontratantes, devem **criar ou adotar códigos de conduta,** a fim de respeitar o regulamento e facilitar a sua aplicação efetiva,[137] tendo em atenção as características específicas do tratamento efetuado em determinados setores e as necessidades específicas

[133] Nuno Saldanha, Novo Regulamento Geral de Proteção de Dados – *O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 109 e 110
[134] Disponível in Encarregado de Proteção de Dados (27 abril 2025).
[135] Por entidades publicas entende-se, o Estado; as regiões autónomas; as autarquias locais e as entidades supranacionais previstas na lei; as entidades administrativas independentes e o Banco de Portugal; os institutos públicos; as instituições de ensino superior, independente da sua natureza; as empresas do setor empresarial do Estado e dos setores empresariais regionais e locais e as associações públicas, conforme a al. a), do n.º 2 do art. 12.º – da Lei n.º 58/2019 de 8 de agosto.
[136] Os tribunais no exercício da sua função jurisdicional não estão abrangidos por esta obrigatoriedade de designar um EPD, segundo a al. a), do n.º 1 do art. 37.º - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[137] Conforme consta do considerando (98) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

das empresas, consoante a dimensão das empresas, adequar essas realidades ao RGPD.[138] O regulamento, no n.º2 do art. 40.º, enumera várias coisas que podem e devem constar nos códigos de conduta, nomeadamente o que consta da al. a) à k). Estes códigos poderão regular as obrigações do responsável e do subcontratante, tendo sempre em conta o risco que poderá resultar do tratamento dos dados no que diz respeito aos direitos e às liberdades dos titulares dos dados, conforme consta no considerando (98) do regulamento. Acresce dizer, que durante a elaboração/alteração destes códigos, as organizações acima mencionadas devem consultar os respetivos titulares dos dados em tratamento e, sempre que for possível, ter em conta os contributos recebidos e as opiniões expressas em resposta a essas consultas.[139]

Com o mesmo objetivo dos códigos de conduta, deverão ser criados **procedimentos de certificação**, selos e marcas de proteção de dados, de forma a reforçar a transparência e o cumprimento do presente regulamento, permitindo aos titulares avaliar de forma célere o nível de proteção de dados assegurado pelos produtos e serviços em causa, conforme plasmado no art. 42.º, n.º 1 do RGPD.

Diante do exposto, é possível aferir que o responsável pelo tratamento de dados desempenha um papel imprescindível no que diz respeito à proteção de dados pessoais, assumindo diversas obrigações previstas ao longo do RGPD com o objetivo de garantir a conformidade e a segurança no tratamento dessas informações e o controller deve assegurar a transparência e a proteção dos direitos dos titulares dos dados.

Os diversos deveres imputados ao responsável interligam-se entre si, demostrando a necessidade de ter uma abordagem contínua e estruturada no que toca à gestão da privacidade e segurança dos dados. A adoção de medidas técnicas e organizativas de proteção desde a conceção, a realização de avaliações de impacto e a consulta prévia às

[138] Nuno Saldanha, op. cit, pág. 123.
[139] Conforme consta do considerando (99) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

autoridades competentes, demonstram a importância da prevenção e mitigação de riscos no tratamento de dados pessoais.

Em caso de incumprimento das obrigações referidas ao longo deste tópico, pode levar à aplicação de sanções, conforme previsto no art. 83.º, que estabelece um quadro rigoroso para a aplicação de sanções, procurando garantir que o responsável pelo tratamento de dados adote práticas adequadas de proteção e segurança. Neste artigo está determinado que as coimas sejam aplicadas de forma eficaz, proporcional e dissuasiva, tendo em conta diversos fatores, tais como a natureza, a gravidade e a duração da infração, o grau de responsabilidade do infrator, as eventuais medidas corretivas adotadas, o nível de cooperação com as autoridades de controlo e eventuais violações anteriores.

4.2 Conceito de Subcontratante (Processor) e as suas obrigações

Nos termos do art. 28.º do RGPD, o subcontratante surge como uma figura relevante no regulamento, sendo a entidade à qual o responsável pelo tratamento de dados pode recorrer para realizar o tratamento de dados em seu nome.

Quando o responsável pelo tratamento faz uso desse recurso, está, na prática, a optar por delegar total ou parcialmente as atividades de tratamento de dados para uma entidade externa.[140] No entanto, é fundamental que essa delegação seja realizada com cautela, uma vez que o responsável pelo tratamento tem a obrigação de contratar apenas subcontratantes que ofereçam garantias suficientes, especialmente em termos de conhecimentos especializados, fiabilidade e recursos, no que diz respeito à implementação de medidas técnicas e organizativas adequadas,[141] medidas essas que

[140] Ana Francisca Pinto dias, *Revista de Direito da Responsabilidade - Responsabilidade Civil pelo Tratamento de Dados Pessoais: A Responsabilidade do Controller por Factos Próprios e por Factos de Outrem*, Coimbra, Ano 1, 2019, pág. 1280, disponível in Responsabilidade civil pelo tratamento de dados pessoais: a responsabilidade do controller por factos próprios e por factos de outrem – Ana Francisca Pinto Dias – Revista de Direito da Responsabilidade (27 abril 2025).
[141] Conforme consta do considerando (81) primeira parte - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

devem assegurar que o tratamento atenda aos requisitos do regulamento e que os direitos dos titulares dos dados sejam devidamente protegidos.

Conforme já redigido nesta dissertação,[142] o subcontratante é "(...) uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes"[143], isto significa, que o subcontratante é como se fosse um mandatário do responsável pelo tratamento de dados, que trata os dados pessoais por conta do responsável pelo tratamento.

Importa referir, que o subcontratante, devidamente autorizado, pode subcontratar. Neste caso ao subcontratante subcontratado é lhe imputado as mesmas obrigações relativas à proteção de dados.[144]

O legislador no decorrer do regulamento, enuncia algumas obrigações que o subcontratante deve ter em conta, essas obrigações vão encontrar-se estipuladas no contrato redigido entre o responsável e o subcontratante. Pelo que, segundo as diversas alíneas do n.º 3 do art. 28.º o subcontratante deve:

- **Tratar os dados pessoais com base nas instruções documentadas pelo responsável pelo tratamento** – Nesta obrigação estão incluídas as transferências de dados para países terceiros ou organizações internacionais, salvo se estiver obrigado a fazê-lo pelo direito da UE ou do Estado-Membro a que está sujeito, sendo que, nestes casos, **o subcontratante deverá informar** o responsável pelo tratamento dos dados pessoais desse requisito jurídico antes do tratamento, excetuando-se as situações em que a lei proibir essa informação por motivos importantes de interesse público;
- **Garantir a confidencialidade** – Significa dizer que o subcontratante deve assegurar que, as pessoas autorizadas a tratar os dados pessoais assumem um

[142] Ver pág. 22 desta dissertação.
[143] Conforme consta do art. 4.º, n.º 8 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[144] Nuno Saldanha, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 79.

compromisso de confidencialidade ou que estão sujeitas a obrigações legais de confidencialidade adequadas ao contexto;

- **Adotar todas as medidas de segurança necessárias** – Com esta obrigação o legislador pretende proteger os dados pessoais, pelo que segundo o art. 32.º do RGPD, o subcontratante deve adotar as medidas de segurança essenciais à proteção do tratamento de dados, a fim de evitar possíveis violações aos dados pessoais que causem grandes danos aos titulares desses dados;
- **Obter autorização prévia e por escrito** – O subcontratante quando decidir subcontratar, deve comunicá-lo, previamente e por escrito, ao responsável pelo tratamento. Deve ainda exigir ao novo subcontratante, por contrato, a apresentação de garantias suficientes de execução de medidas técnicas e organizativas adequadas à realização desse tratamento;
- **Prestar assistência ao responsável pelo tratamento** – Atendendo à natureza do tratamento e à informação disponibilizada ao subcontratante, este, deve auxiliar o responsável, recorrendo a medidas técnicas e organizativas adequadas, a fim de permitir que o segundo cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos e no sentido de assegurar o cumprimento das obrigações consagradas do art. 32.º ao 36.º do RGPD.
- **Apagar ou devolver-lhe todos os dados pessoais depois de concluída a prestação de serviços** – Significa que o subcontratante assim que concluir a sua prestação de serviços, deve apagar ou devolver as cópias existentes relativamente ao tratamento de dados pessoais, excetuando-se os casos em que a conservação dos dados seja exigida ao abrigo do direito da UE ou dos Estados-Membros;
- **Disponibilizar todas as informações necessárias** – O subcontratante deve demonstrar, ao responsável pelo tratamento, o cumprimento das obrigações previstas no art. 28.º, procurando facilitar e contribuir para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outra entidade mandatada pelo último.

- **Colaborar com a Autoridade de Controlo** – Segundo o art. 31.º do regulamento, tal como o responsável pelo tratamento, o subcontratante está obrigado a colaborar com a CNPD.
- **Notificar o responsável caso ocorra uma violação dos dados** – Nestes casos, assim que o subcontratante tenha conhecimento de algum tipo de violação de dados pessoais, deve notificar, sem demora injustificada, o responsável e não a Autoridade de Controlo, conforme consta no n.º 2 do art. 33.º do RGPD.

Em suma, ainda que o responsável pelo tratamento dos dados continue a ser o responsável pelo cumprimento das regras de proteção de dados pessoais, o subcontratante, assim que começar a trabalhar para o responsável, encontra-se sujeito a diversas obrigações, nomeadamente as atrás enunciadas.

Após a análise destas figuras, é possível concluir que a ambas lhes é imposta uma variedade de obrigações, face ao tratamento e aos titulares dos dados, sendo que alguns desses deveres aplicam-se tanto ao responsável pelo tratamento como ao subcontratante, por exemplo, a obrigatoriedade de registo das atividades de tratamento mencionada no art. 30.º, n.º 1 e 2, o cumprimento da segurança no tratamento dos dados presente no art. 32.º e a nomeação de EPD consagrado no art. 37.º.

Tal como para o responsável, o regulamento preceitua que se o subcontratante não cumprir as obrigações decorrentes do RGPD, dirigidas especificamente ao subcontratante ou se não tiver seguido as instruções lícitas dadas pelo responsável pelo tratamento, é responsabilizado pelo incumprimento das normas impostas pelo RGPD e pelos danos causados aos titulares pelo tratamento, segundo o art. 82.º, n.º 2.

4.3 Relação entre o Responsável pelo Tratamento e o Subcontratante

A relação estabelecida entre o responsável pelo tratamento e o subcontratante, deve reger-se por um contrato ou por outro ato jurídico, escrito, que vincule o

subcontratante ao responsável pelo tratamento.[145] Nesse contrato, devem constar tanto as responsabilidades e obrigações do responsável pelo tratamento como do subcontratante, procurando desta maneira assegurar que o processamento dos dados pessoais se dê de forma segura e em conformidade com o RGPD.

No contrato, para além do mencionada atrás, deve ainda constar mais um conjunto de informações, designadamente o **objeto**, ou seja, define o propósito geral do contrato e o que está a ser estabelecido; a **duração**, encontra-se definido o período durante o qual o tratamento de dados será realizado; a **natureza** e a **finalidade** do tratamento, deve explicar a razão pela qual os dados serão tratados e de que forma isso será feito; o **tipo de dados pessoais**[146] a tratar, nele deve especificar quais categorias de informações serão tratadas; e a **categoria dos titulares dos dados**,[147] significa que deve indicar a quem pertencem os dados tratados.[148] A especificação destas informações, assegura que todas as partes envolvidas compreendem quais são as suas obrigações e consequentemente leva a que o tratamento de dados seja realizado de forma licita e segura.

Quando falamos do contrato, importa referir que entre o responsável e o subcontratante tanto pode ser redigido um contrato individual ou um contrato com cláusulas contratuais-tipo. Neste último modelo de contrato, as cláusulas podem ser estabelecidas quer pela Comissão quer pela Autoridade de Controlo em conformidade com o procedimento de controlo da coerência, conforme mencionado do n.º 6 a 8 do art. 28.º do RGPD.

Este contrato deve obrigar o subcontratante a algumas coisas, nomeadamente tratar os dados pessoais com base nas instruções dadas pelo responsável pelo tratamento, garantir a confidencialidade, adotar todas as medidas de segurança necessárias, obter autorização prévia e por escrito, prestar assistência ao responsável pelo tratamento, a

[145]Conforme consta do art. 28.º, n.º 3 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[146] Quanto ao tipo de dados pessoais em tratamento, pode estar em causa por exemplo o nome ou o endereço do respetivo titular.
[147] Para a categoria dos titulares dos dados temos como exemplos os clientes, os funcionários ou até mesmo os fornecedores de uma determinada empresa.
[148] Conforme consta do art. 28.º, n.º 3 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

apagar ou devolver-lhe todos os dados pessoais depois de concluída a prestação de serviços e a disponibilizar todas as informações necessárias, estas obrigações encontram-se melhor explicadas no subtópico anterior.

Enaltecendo que o subcontratante só pode tratar os dados pessoais de acordo com as instruções documentadas do responsável pelo tratamento, é possível aferir que esta obrigação significa que o subcontratante não tem autonomia no tratamento de dados e que não pode usar os dados para finalidades que não estejam previamente autorizadas pelo responsável. Assim, é possível perceber que esta é uma das diferenças entre o responsável pelo tratamento e o subcontratante, uma vez que o primeiro tem controlo sobre as finalidades do tratamento e por sua vez o segundo não tem qualquer controlo sobre isso, apenas realiza o tratamento de acordo com as instruções fornecidas pelo responsável. Contudo, apesar de o subcontratante realizar as suas tarefas sob a alçada do responsável, se este "em violação do presente regulamento, determinar as finalidades e os meios de tratamento, é considerado responsável pelo tratamento no que respeita ao tratamento em questão." segundo o n.º 10 do art. atrás mencionado.

Sucintamente, a relação entre o responsável pelo tratamento e o subcontratante deve ser clara, transparente e baseada na confiança, regularizada por um contrato ou outro instrumento jurídico escrito. Esse documento não só define as responsabilidades de cada parte, como também assegura que o tratamento dos dados pessoais ocorra de forma segura e em conformidade com o regulamento. Caso exista um subcontratante, este atua sempre sob as instruções do responsável, sem autonomia sobre as finalidades do tratamento, o que reforça a importância de uma comunicação eficaz e de regras bem estabelecidas. Com a elaboração deste contrato, é possível assegurar que todos saibam exatamente qual é o seu papel, contribuindo assim para um tratamento de dados justo, seguro e responsável.

5 A Responsabilidade Civil no Tratamento de Dados

5.1 Enquadramento

A temática responsabilidade civil, ganhou bastante relevância na era digital, no que diz respeito ao tratamento de dados pessoais, uma vez que o volume de informações trocadas e armazenadas alcançou níveis nunca vistos, pelo que se tornou inevitável a criação de diretrizes que salvaguardassem os direito e liberdades dos titulares. A crescente e célere evolução das NTIC, trouxe consigo diversas questões cruciais sobre o tratamento e proteção de dados pessoais, como por exemplo "**até que ponto a evolução tecnológica pode dificultar a fiscalização e a respetiva responsabilização?**", ou nos casos em que estejamos perante uma violação dos dados pessoais, "**quem responde por essa violação?**" e "**quais serão os danos indemnizáveis e as sanções aplicadas?",** caso se comprove que houve violação do regulamento**.**

Neste ponto, o RGPD exerce um papel fundamental, com ele é possível responder a algumas dessas questões que vão surgindo, e como já referido diversas vezes, nesta dissertação, com a criação deste regulamento, o legislador procurou reforçar a importância de estabelecer regras claras e transparentes, que visassem proteger os direitos e liberdades dos titulares dos dados em tratamento, garantindo, consequentemente, que os responsáveis pelo tratamento ou os subcontratantes fossem devidamente responsabilizados pelos danos causados nos dados pessoais, por uma eventual violação, nos casos em que a culpa possa ser imputada aos mesmos.

É no capítulo VIII do RGPD, mais precisamente do art. 77.º ao art. 84.º, que se encontra consagrado as **vias de recurso**, a **responsabilidade** e as **sanções** no que diz respeito à proteção de dados pessoais. Este capítulo, estabelece as regras relativas às reclamações, às responsabilidades e às respetivas sanções aplicáveis em caso de violação do regulamento, permitindo com elas que o tratamento de dados pessoais seja conduzido de forma responsável e em conformidade com os direitos fundamentais dos indivíduos.

Segundo o considerando (141) os titulares dos dados têm direito a apresentar reclamação à Autoridade de Controlo, principalmente no Estado-Membro da sua residência habitual, do seu local de trabalho ou do local onde foi alegadamente praticada

a infração, e direito a uma ação judicial efetiva, nos termos do art. 47.º da Carta,[149] nas situações em que considerem que os seus direitos conferidos pelo presente regulamento foram violados ou quando a Autoridade de Controlo não responder a uma reclamação, a recusar ou rejeitar, total ou parcialmente, ou se esta não proceder às intervenções necessárias para proteger os direitos dos titulares. A Autoridade de Controlo, deverá informar o autor da reclamação sobre o andamento e o resultado da mesma, informando-o ainda que tem direito de intentar uma ação judicial,[150] podendo esta ser contra a Autoridade de Controlo, nos casos em que não trate da reclamação ou não informe os titulares dos dados sobre o andamento e resultado no prazo de três meses, ou pode ser contra o responsável pelo tratamento ou o subcontratante nos casos em que se considere que houve um tratamento incorreto, infringindo o regulamento e, consequentemente, levando à violação dos direito dos titulares referidos no mesmo.[151]

Segundo o regulamento, a responsabilidade civil pelo tratamento de dados, é imputada ao responsável pelo tratamento e ao subcontratante, segundo os art. 82.º a 84.º do RGPD. Por exemplo, o art. 82.º, para além de abordar a responsabilidade de quem processa os dados, também prevê o direito à indemnização a quem tenha sofrido danos quer materiais ou imateriais, resultantes da violação do regulamento. É neste grupo de artigos, que se encontram previstas as coimas, as sanções e as respetivas indemnizações, pelo que o RGPD estabelece a base para que os titulares de dados possam ser indemnizados sempre que houver danos decorrentes do tratamento ilícito dos seus dados pessoais.

[149] O art. 47.º com a epigrafe *direito à ação e a um tribunal imparcial*, diz que "Toda a pessoa cujos direitos e liberdades garantidos pelo direito da União tenham sido violados tem direito a uma ação perante um tribunal nos termos previstos no presente artigo. Toda a pessoa tem direito a que a sua causa seja julgada de forma equitativa, publicamente e num prazo razoável, por um tribunal independente e imparcial, previamente estabelecido por lei. Toda a pessoa tem a possibilidade de se fazer aconselhar, defender e representar em juízo. É concedida assistência judiciária a quem não disponha de recursos suficientes, na medida em que essa assistência seja necessária para garantir a efetividade do acesso à justiça."
[150] Conforme consta do art. 77.º, n.º 3 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[151] Conforme consta do art. 78.º e 79.º - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

5.2 Medidas de segurança implementadas no tratamento de dados

Nas situações em que se observe uma rutura da segurança que conduza à destruição, à perda, à alteração, à divulgação não autorizada ou ao acesso de dados pessoais de forma acidental ou ilícita, conforme já referido nesta dissertação, estaremos perante uma violação de dados pessoais.[152] Neste sentido, o RGPD obriga o responsável a notificar a Autoridade de Controlo, sendo que, em alguns casos, também deve notificar os titulares dos dados alvo da violação.[153] Assim, nas situações em que aconteça uma violação e que a mesma suceda de uma adoção de medidas preventivas inadequadas por parte do responsável, sobre este recairá a responsabilidade civil.

Desde logo, atendendo ao exposto, é possível aferir que a responsabilidade civil se encontra diretamente relacionada com a implementação de medidas de segurança adequadas no tratamento de dados pessoais. O legislador reforça esta ideia, com o art. 32.º, o qual obriga quer o responsável, quer o subcontratante a implementar medidas técnicas e organizativas adequadas a fim de garantir um nível de segurança apropriado ao risco apresentado pelo tratamento. Estas medidas incluem a pseudonimização e a cifragem de dados, a garantia de confidencialidade, integridade, disponibilidade e a resiliência dos sistemas utilizados no tratamento.

As medidas técnicas de pseudonimização e de anonimização são recomendadas pelo RGPD com o objetivo de minimizar os riscos associados ao tratamento de dados pessoais. Posto isto, a pseudonimização passa pela separação dos dados pessoais de elementos identificadores, o que reduz o risco de que os dados possam ser associados a um titular de dados específico. Quanto à anonimização, esta medida implica a eliminação de todos os elementos que possam identificar uma determinada pessoa, tornando os dados irreversíveis.[154] A aplicação das medidas técnicas e organizativas, nomeadamente as

[152] Ver pág. 25 desta dissertação.
[153] Conforme consta do art. 33.º, nº 1 e art. 34.º, nº 1 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[154] Ver a explicação constante na pág. 20 e 21 desta dissertação. Sendo ainda visível in Anonimização e Pseudonimização (27 abril 2025).

mencionadas atrás, levam à diminuição dos danos causados por uma eventual violação e como tal reduzir o impacto da responsabilidade civil imputada aos responsáveis.

5.3 Conceito de Responsabilidade Civil

O conceito geral de responsabilidade civil, encontra-se previsto no art. 483.º, n.º 1 do CC, onde menciona que "aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação", assim, a responsabilidade civil refere-se à obrigação de reparar os danos causados a um terceiro, em virtude da prática de atos ilícitos.

Existe um conjunto de responsabilidades que podem ser aplicadas a esta temática do tratamento de dados, designadamente as responsabilidades criminais, as responsabilidades contraordenacionais, a responsabilidade civil, a responsabilidade de foro disciplinar e a responsabilidade social.[155] Deste conjunto de responsabilidades, a que se salienta, face ao tema proteção de dados, é a responsabilidade civil. Para estarmos perante uma responsabilidade civil é necessário observar três requisitos, nomeadamente a **existência de dano**; a **ação ou omissão ilícita**; e o **nexo de causalidade** entre a ação ou omissão e o dano causado. No caso do tratamento de dados pessoais, esses requisitos também se aplicam, mas de maneira específica, conforme a natureza dos dados e as regras estabelecidas pelo RGPD, mais acresce dizer que são estes requisitos que validam ou não o exercício do direito de indemnização facultado aos titulares.

Tendo em conta o contexto da proteção de dados pessoais e analisando os três requisitos acima referidos, podemos dizer que:

- Quanto à **existência de dano**, este, é um elemento essencial no que diz respeito à definição da responsabilidade civil, o regulamento no n.º 1 do art. 82.º, reconhece que o dano tanto pode ser material ou imaterial. Os danos

[155] Nuno Saldanha, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 163.

materiais, também considerados por danos patrimoniais, são aqueles dados que se podem ver ou tocar, ou seja, que podem ser sentidos em bens corpóreos ou incorpóreos, por exemplo, podemos estar a falar de prejuízos financeiros, em que a indemnização visa reparar /atenuar essa perda financeira. Quanto ao dano imaterial, este está relacionado com lesões sofridas à sua condição humana, podem ser causados danos a bens como a honra, a imagem, a intimidade ou a vida privada, podemos falar de danos morais, danos estéticos e danos existenciais, por exemplo, caso sejam divulgados dados sensíveis, como informações sobre saúde ou dados financeiros, sem que o titular tenha previamente autorizado, podendo causar sérios danos imateriais, ainda que não haja um prejuízo económico direto.

- No que diz respeito ao segundo requisito a **ação ou omissão ilícita,** a ilicitude pode dar-se de diversas situações, como a recolha de dados sem consentimento do titular, o tratamento de dados ser para finalidades distintas das originalmente previstas, ou a falha na implementação de medidas de segurança adequadas. O regulamento especifica que o tratamento de dados deve estar sempre sustentado por uma base legal, não sendo permitido o tratamento sem justificação clara e legalmente permitida.[156]
- Por fim, relativamente ao último requisito, para que se fale de responsabilidade civil, é necessário que se demonstre **o nexo de causalidade** entre o tratamento ilícito de dados e o dano causado ao titular. Podemos aferir que este é um ponto delicado em muitos casos, visto que pode ser difícil provar que o dano sofrido pelo titular foi causado diretamente pela ação ou omissão por parte do responsável pelo tratamento ou do subcontratante, tanto que neste sentido, o regulamento, prevê a possibilidade de o responsável ou o subcontratante ficarem exonerados da responsabilidade, nos casos em que consigam provar que não são de forma alguma responsáveis pelo facto que levou ao dano, segundo o art. 82.º, n.º 3 e considerando (146) do RGPD.

[156] Conforme consta do art. 6.º e considerando (40) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Considerando o exposto, é de salientar que o responsável pelo tratamento e o subcontratante exercem um papel fundamental face ao tratamento de dados, a eles é incumbido o dever de garantir que todas as operações de tratamento sejam realizadas em conformidade e de encontro com as normas estabelecidas no RGPD, assegurando que os dados sejam tratados de maneira lícita, transparente e segura, e que ao adotar medidas adequadas consigam evitar possíveis violações. Ainda que o subcontratante processe os dados em nome do responsável pelo tratamento e sob as instruções dadas por este, o subcontratante pode ser responsabilizado diretamente pelos danos que provenham do incumprimento das suas obrigações, significa isto, que ambos podem ser responsabilizados civilmente pelos danos causados aos titulares dos dados que ocorram de um processamento de dados ilícito.

5.3.1 Exemplo Prático: O Caso C-340/21 do TJUE[157]

Podemos dar como exemplo elucidativo do que foi explicado anteriormente, e até utilizar de elo de ligação com o que vai ser explicado a seguir, o **Acórdão do TJUE no Processo C-340/21**, proferido em 14 de dezembro de 2023. O caso em questão envolveu a Agência Nacional de Receitas Fiscais da Bulgária (NAP), cuja base de dados foi alvo de um ataque informático, levando à divulgação de dados pessoais de diversos cidadãos. A lesada, na ação que propôs no tribunal, solicitou uma indemnização por danos imateriais, ao abrigo do art. 82.º do regulamento, motivada pelo receio de uma futura utilização abusiva dos seus dados, como por exemplo chantagem ou ser alvo de rapto.[158]

O tribunal administrativo decidiu que não se verificaram falhas nas medidas de segurança adotadas pela NAP, e, consequentemente, não existiria nexo de causalidade suficiente para justificar aquele pedido de indemnização. A lesada, descontente com a

[157] Ac. do Tribunal de Justiça (Terceira Secção) de 14 de dezembro de 2023 – Proc. n.º C-340/21, disponível in CURIA - Documents (27 abril 2025).
[158] Mafalda Miranda Barbosa, *Revista de Direito da Responsabilidade – Proteção de Dados e Causalidade: Reflexões a Propósito do AC. TJUE C-340/21, de Dezembro de 2023*, Coimbra, Ano 6, 2024, disponível in Proteção de dados e causalidade: reflexões a propósito do Ac. TJUE C-340/21, de 14 de dezembro de 2023 – Mafalda Miranda Barbosa – Revista de Direito da Responsabilidade (27 abril 2025).

decisão, interpôs recurso para o Supremo Tribunal Administrativo, perante diversas questões levantadas pelo mesmo, decidiu formular, em sede de reenvio prejudicial,[159] essas questões para o TJUE que veio esclarecer que a violação de dados pessoais, sozinha, não leva automaticamente à conclusão de que houve incumprimento das obrigações do responsável pelo tratamento e do subcontratante; que o responsável tem o ónus de provar que adotou todas as medidas técnicas e organizativas adequadas a fim de prevenir a violação, contudo, a isenção de responsabilidade de ambos só se dá se se provar a inexistência de nexo de causalidade entre a violação e o alegado dano; e que o receio fundado numa futura utilização abusiva dos dados pode, mesmo sem concretização efetiva de prejuízo, constituir um dano imaterial indemnizável, nos termos do art. 82.º, n.º 1 do RGPD.

Após a leitura deste acórdão, é possível aferir que o mesmo assume particular relevância para a discussão do nexo de causalidade no que toca à responsabilidade civil face à proteção de dados, sobretudo quando se trata de uma violação resultante da atuação de terceiros. Neste sentido o TJUE esclareceu que, nestes casos, a responsabilidade do responsável pelo tratamento ou do subcontratante não se afasta automaticamente, sendo exigido que demonstrem a ausência de culpa ou nexo causal com o dano sofrido.

No âmbito do RGPD, e em relação ao acórdão supramencionado, a responsabilidade civil é objetiva, contudo, é exigido que seja provado o nexo de causalidade entre a violação e o dano sofrido, ou seja, para falarmos em responsabilidade civil tem de estar em causa uma violação do regulamento e essa violação tem de ter causado danos aos titulares dos dados, podendo esses danos ser materiais ou imateriais. Neste sentido, o acórdão reforça os direitos dos titulares dos dados, reconhecendo legalmente os danos imateriais, os considerados danos subjetivos, como por exemplo o medo e a ansiedade. Com isto, o TJUE concluiu que o receio de uma eventual utilização

[159] O reenvio prejudicial "encontra-se previsto no art. 267.º do Tratado sobre o Funcionamento da União Europeia e constitui um mecanismo contencioso que visa garantir a uniformidade na interpretação e aplicação do Direito da União Europeia. Caracteriza-se como um incidente de instância de um processo judicial nacional, ou seja, quando a resolução de um litígio nacional dependa do esclarecimento sobre uma norma de DUE, o órgão jurisdicional nacional solicita ao Tribunal de Justiça da União Europeia (TJUE) pronúncia sobre essa questão. O processo judicial nacional suspende-se enquanto o TJUE não responder à questão prejudicial.", disponível in Processo das questões prejudiciais (Direito da União Europeia) | DR (27 abril 2025).

abusiva de dados pessoais, mesmo sem que tal tenha ocorrido, pode constituir um dano imaterial indemnizável no âmbito do art. 82.º do RGPD, acreditando que excluir tais situações do direito à indemnização não seria compatível com o elevado nível de proteção que o RGPD visa assegurar.

Importa ainda abordar a inversão do ónus da prova, ou seja, normalmente quem alega ter sofrido um determinado dano, é quem tem de provar o prejuízo sofrido pelo mesmo, a negligência de quem o provocou e o respetivo nexo de causalidade, contudo, o TJUE veio reforçar a ideia implementada no regulamento, em que não é o titular dos dados que tem de provar que o responsável não atuou de forma lícita no tratamento de dados, mas sim o contrário, o responsável pelo tratamento é que tem de provar que agiu com diligência, adotando todas as medidas técnicas e organizativas adequadas para evitar a violação dos dados. Com esta inversão, o legislador procura proteger os titulares e consequentemente obrigar os responsáveis a cumprir as suas responsabilidades e a atuar em conformidade com o RGPD.

Ainda que esteja em causa uma violação praticada por terceiro, por exemplo um hacker como fala o caso prático em análise, a causalidade não é afastada, excetuando-se os casos em que o responsável consiga demonstrar que durante todo o tratamento tomou todas as medidas possíveis para evitar que tal dano acontecesse. Neste sentido, o TJUE concluiu que o responsável não pode ficar automaticamente isento da responsabilidade quando se trata de uma violação cometida por um terceiro, para tal, deve demonstrar que implementou as medidas técnicas e organizativas adequadas para garantir a segurança dos dados, conforme o disposto no art. 24.º e no art. 32.º do RGPD.[160]

O acórdão do TJUE no processo C-340/21 proferido em 14 de dezembro de 2023, contribuiu para uma leitura mais exigente da causalidade no domínio digital, reforçando o papel da diligência preventiva e da prova positiva das medidas de proteção, como

[160] Conforme mencionado no art. 24.º "(…) 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. (…)", no art. 32.º é reforçada a ideia de que o responsável terá sempre de implementar medidas técnicas e organizativas adequadas a fim de cumprir o estabelecido no regulamento, no qual se encontram elencadas algumas medidas a adotar, ambos se encontram consagrados – no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

fatores determinantes na atribuição de responsabilidade. Também foi fundamental para clarificar a responsabilidade civil face à violação de dados, para reconhecer os danos imateriais subjetivos, para reforçar o ónus da prova do responsável pelo tratamento e para enquadrar o nexo de causalidade face a ataques externos. Este acórdão reconhece que o receio de uso indevido dos dados pessoais, por si só, pode justificar uma indemnização proporcional ao dano causado.

5.4 Direito de Indemnização

De acordo com o art. 82.º do RGPD, **qualquer pessoa que tenha sofrido danos** provenientes da violação das normas de proteção de dados, **tem o direito a ser indemnizado por esses danos**. Segundo o art. 564.º do CC, "o dever de indemnizar compreende não só o prejuízo causado, como os benefícios que o lesado deixou de obter em consequência da lesão", isto significa que, no âmbito da proteção de dados, quando o responsável tiver o dever de indemnizar o titular dos dados afetados, essa indemnização deve cobrir o prejuízo causado pela violação, bem como compensar pelos benefícios que deixou de obter por causa dos danos.

Relativamente à imputação da responsabilidade civil, entre o responsável pelo tratamento e o subcontratante, primeiramente será responsabilizado o responsável pelo tratamento, tendo de responder por esses danos, contudo, o subcontratante, também será responsabilizado caso não tenha cumprido as suas obrigações presentes no regulamento ou se não tiver seguido as indicações dadas pelo responsável pelo tratamento.[161]

Quando o titular dos dados afetados pretender intentar uma ação contra o responsável pelo tratamento e/ou contra o subcontratante, para solicitar uma indemnização, a mesma deve ser apresentada perante os tribunais competentes nos termos

[161] Conforme consta do art. 82.º, n.º 2 segunda parte - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

do direito do Estado-Membro em que tenham estabelecimento ou, em alternativa, do Estado-Membro em que o titular dos dados tenha a sua residência habitual.[162]

De forma a analisar corretamente este tópico e de o abordar com maior clareza, irei analisar um acórdão que retrata um pouco acerca do direito de indemnização, designadamente o **Acórdão do TJUE no Processo C-300/21**, proferido em 4 de maio de 2023.

Este acórdão envolveu a Österreichische Post AG, uma empresa austríaca, que utilizou algoritmos para inferir as afinidades partidárias dos cidadãos com base em critérios sociodemográficos. Um cidadão identificado como UI, descobriu que os seus dados foram utilizados para esse tratamento sem o respetivo consentimento, sendo-lhe atribuída uma afinidade política específica, o que o deixou indignado e ofendido, levando-o a solicitar uma indemnização pelos danos não patrimoniais, alegando "inquietação interior".[163]

Com este caso foram levantadas algumas questões cruciais quanto à interpretação do art. 82.º do RGPD, nomeadamente se a simples violação do regulamento confere automaticamente o direito a indemnização, independentemente de ter ou não originado um dano, se o dano imaterial necessita de atingir um certo grau de gravidade para justificar a indemnização, e se os tribunais nacionais podem estabelecer critérios próprios para quantificar esses danos.

O TJUE entende que o direito de indemnização depende da verificação, cumulativa, de três requisitos, designadamente a existência de um dano, a ocorrência de uma violação do RGPD e a existência de um nexo de causalidade entre o dano e a violação.[164] Desde logo, é percetível que estes requisitos são o elo entre o direito de indemnização e a responsabilidade civil. Conforme explicado anteriormente, a violação do regulamento prende-se com a ação ou omissão ilícita do mesmo, por sua vez, o dano

[162] Conforme consta do art. 82.º, n.º 6, que remete para o art. 79.º, n.º 2 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[163] Ac. do TJUE de 4 de maio de 2023 – Proc. n.º C-300/21, disponível in CURIA - Documents (27 abril 2025).
[164] Disponível in A indemnização de danos imateriais: A insuficiência da violação do Regulamento Geral sobre a Proteção de Dados e a desnecessidade de um limiar mínimo de gravidade, Sérvulo Publications, Knowledge - Sérvulo & Associados – Law firm, Portugal (27 abril 2025).

pode ser de natureza material ou imaterial e, por fim, o nexo de causalidade está relacionado com o facto de ser necessário demonstrar que o dano decorreu dessa violação. Aqui podem surgir alguns obstáculos práticos significativos à efetivação do direito à indemnização, especialmente quando se fala de danos imateriais, uma vez que não é fácil quantificar, por exemplo, a angústia ou a ansiedade sentida.

Podemos constatar que os três requisitos mencionados se encontram presentes no caso em análise, começando pelo requisito da violação, sendo evidente que a empresa ao proceder ao estudo das "preferências políticas" dos cidadãos, violou claramente o regulamento, uma vez que analisou dados sensíveis, conforme disposto no art. 9.º,[165] sem o consentimento e conhecimento do titular dos dados, violando desde logo princípios fundamentais do regulamento como o princípio da licitude, da lealdade e da transparência no tratamento de dados.

Quanto ao requisito do dano, o UI alegou sentir-se afetado por uma "inquietação interior", levanta-se aqui a questão se o dano imaterial (o ligeiro desconforto emocional) é suscetível de ser indemnizado. Neste sentido, o tribunal aferiu que o dano imaterial, ainda que seja leve, não deve ser de todo excluído, devendo ser afastada a ideia de um limite mínimo de gravidade. Esta interpretação feita pelo TJUE vai de encontro com o que o RGPD defende, que é garantir uma proteção efetiva dos direitos fundamentais dos titulares dos dados pessoais.

Por último, o requisito do nexo de causalidade entre a atribuição da afinidade política e o estado de inquietação alegado pelo lesado, em que o TJUE confirmou que este elemento deve ser demonstrado tendo por base critérios objetivos, ou seja, não pode o simples desconforto subjetivo justificar, por si só, a compensação, sem essa ligação causal concreta.

[165] Art. 9.º - *Tratamento de categorias especiais de dados pessoais* "É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa." - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

O regulamento, no seu teor, não faz propriamente uma distinção entre os tipos de danos indemnizáveis, o que faz com que tanto os danos materiais quanto os danos imateriais possam vir a ser indemnizados. O legislador ao não fazer essa restrição procurou proteger os titulares de dados contra qualquer tipo de lesão proveniente de um tratamento ilícito dos seus dados pessoais. Contudo, é importante e imprescindível a prova do dano sofrido, isto porque, o dano imaterial, devido à sua natureza subjetiva, torna-se difícil de quantificar, exigindo que por parte dos tribunais seja feita uma abordagem mais subjetiva, não obstante, uma vez provado o nexo de causalidade entre o ato ilícito e o dano, a indemnização deve ser deferida, ainda que proporcional ao dano sofrido.

Em suma, face ao caso prático em apreso e às questões levantadas, o TJUE concluiu que a simples violação do RGPD não é suficiente para conferir ao titular dos dados o direito a ser indemnizado, tendo este de provar a existência de um dano quer seja material ou imaterial e comprovar que existe nexo de causalidade entre a violação e o dano sofrido. Ainda reitera a ideia que, no caso de danos imateriais, para ter direito à indemnização, não terá de atingir um determinado limite de gravidade. Com este parecer do TJUE é possível uniformizar a interpretação do art. 82.º do RGPD, assegurando que os titulares de dados disponham de um nível de proteção semelhante em todos os Estados-Membros, evitando desigualdades injustificadas na aplicação do direito à indemnização.

5.5 Sanções

Com o objetivo de acautelar a efetiva observância e execução das regras estabelecidas no RGPD, o legislador procurou estabelecer um regime sancionatório eficaz, prevendo por exemplo a aplicação de **coimas**, a serem aplicadas em caso de incumprimento do previsto no regulamento, segundo o art. 83.º. Mais acrescenta o legislador no art. 84.º onde atribui aos Estados-Membros a competência de estabelecer as regras referentes a outras sanções, que não sejam as coimas, como por exemplo sanções penais ou administrativas, igualmente aplicáveis em caso de violação do regulamento,

sendo que, posteriormente, deverão comunicar à Comissão o teor das normas internas adotadas.[166]

Na aplicação das **sanções** devem ter-se em conta três pressupostos, designadamente, devem ser: efetivas, ou seja, devem produzir realmente um efeito prático; proporcionais, isto significa que a sanção deve corresponder à gravidade da infração; e dissuasivas, isto é, as sanções devem ser caracterizadas pela sua natureza preventiva, evitando futuras violações. Para a correta aplicação das sanções, atendendo aos aludidos pressupostos, é essencial que sejam considerados alguns aspetos, como a natureza, a gravidade e duração da infração, o seu caráter doloso, as medidas tomadas para atenuar os danos causados, o nível de responsabilidade ou eventuais infrações anteriores, o meio pelo qual a autoridade de controlo tomou conhecimento da infração, o cumprimento do código de conduta, bem como quaisquer outros elementos que possam agravar ou atenuar a violação.[167]

No regulamento podem ser encontrados três tipos de sanções:[168]

- as **sanções pecuniárias** – É o mesmo que falar em coimas, sendo estas aplicadas nos casos em que se dê uma violação do disposto no regulamento. No art. 83.º encontra-se estabelecido os valores aplicados nas coimas;
- as **sanções penais** – Estas devem ser, segundo o art. 84.º, definidas pelos Estados-Membros a fim de punir as violações ao RGPD e à legislação nacional, podendo incluir, por exemplo, a perda dos lucros auferidos com a violação, não obstante, é necessário ter em atenção o preceito de que ninguém deve ser punido mais do que uma vez pelo mesmo crime;[169]

[166] Conforme consta do art. 84.º, n.º 1 e 2 - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[167] Conforme consta do considerando (148) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[168] Nuno Saldanha, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?* Lisboa, FCA – Editora de Informática, 2018, pág. 169.
[169] Conforme consta do considerando (149) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

- as **sanções administrativas** – São as sanções aplicadas pela Autoridade de Controlo no exercício dos seus poderes de correção, como por exemplo, o poder de advertir, de repreender, de emitir ordens ou exigir determinadas ações por parte dos responsáveis.[170]

Relativamente às sanções pecuniárias, o mesmo que dizer as coimas, o regulamento divide-as em dois tipos de valores, segundo o previsto nos n.ºs 4 e 5 do art. 83.º, assim temos situações em que as coimas podem chegar até 10 000 000 milhões de euros ou 2% do volume de negócios anual mundial, consoante o que for maior, sendo aplicável, por exemplo, na falta de manutenção dos registos de atividades de tratamento, quando não seja comunicado à Autoridade de Controlo a violação de dados e nos casos em que o tratamento seja suscetível de implicar um elevado risco e não procedam AIPD. Ou, por sua vez, as coimas, podem ir até ao valor de 20 000 000 milhões de euros ou 4% do volume de negócios anual mundial, conforme o que for maior, sendo aplicável, nos casos em que se constate violações graves, como por exemplo, seja feito um tratamento de dados ilícito ou quando sejam violados os princípios básicos implícitos ao tratamento de dados ou dos direitos dos titulares.[171]

A título de exemplo da aplicação das coimas, mencionadas acima, podemos analisar a Deliberação n.º 2021/1569 da CNPD,[172] da qual resultou a aplicação de uma coima no valor de 1.250.000 euros ao Município de Lisboa, pela Autoridade de Controlo com fundamento na divulgação indevida de dados pessoais de determinados impulsionadores das manifestações a terceiros, como por exemplo à Embaixada da Rússia e à Embaixada da India.[173] A partir do momento em que os titulares dos dados pessoais partilhados sem autorização remeteram uma queixa à Autoridade de Controlo, a mesma deu inicio ao procedimento de averiguação do qual resultou que o Município de Lisboa

[170] Segundo o art. 58.º, n.º 2, al. a) a j) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[171] Segundo o art, 83.º n.º 4 e 5) - do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[172] Disponível in https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-aplica-sancao-ao-municipio-de-lisboa/ (30.04.2025).
[173] Segundo o exposto nos pontos 62 e 48 das pág. 38 e 34, respetivamente, da deliberação, disponível in https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-aplica-sancao-ao-municipio-de-lisboa/ (30.04.2025).

realmente tinha violado um conjunto de normas previstas no RGPD, nomeadamente o princípio da licitude, lealdade e transparência, uma vez que o Município procedeu ao tratamento de dados pessoais sem recorrer a uma base legal adequada e o princípio da minimização de dados, visto que coletou dados a mais do que os necessários para a finalidade do tratamento em causa, previstos no art. 5.º, n.º 1, al. a) e c), respetivamente. Violou ainda o direito de informação dos titulares dos dados, consagrado no art. 13.º, uma vez que não comunicaram de forma clara aos titulares dos dados pessoais sobre o tratamento desses dados. Por fim, a CNPD, ainda constatou que o Município não procedeu previamente à AIPD antes de dar início ao tratamento de dados, algo que é imposto sempre que determinado tratamento seja suscetível de implicar um elevado risco face aos direitos e liberdades das pessoas singulares, segundo o plasmando no art. 35.º, n.º1.

Tendo em conta o exposto, a CNPD considerou que se justificava a aplicação de uma coima, considerando a natureza sensível dos dados envolvidos e a possível perda de confiança nas instituições públicas. A corroborar a medida implementada pela CNPD, a 21.07.2024, o TAC, confirmou que o Município violou o regulamento ao divulgar dados pessoais dos impulsionadores das manifestações, mantendo a decisão tomada pela CNPD referente à aplicação da coima. Contudo, reduziu o valor da coima para 1.027.500 euros, visto que haviam infrações prescritas desde 21.12.2021, data em que a CNPD tomou a decisão, até à sentença judicial.[174]

Em suma, da breve análise feita à Deliberação n.º 2021/1569 da CNPD, conclui-se, que a aplicação de um regime sancionatório rigoroso, sempre que ocorra uma violação das disposições previstas no regulamento decorrente de um tratamento ilícito de dados, constitui uma medida eficaz para a correção, visto que desencoraja ou inibe uma determinada conduta indesejada, por meio da intimidação ou da advertência**.** No caso em apreço, é evidente que o Município de Lisboa caiu em incumprimento quanto a algumas obrigações legais previstas para o tratamento de dados pessoais, levando à aplicação de

[174] Disponível in https://www.cnpd.pt/comunicacao-publica/noticias/tribunal-confirma-violacao-do-rgpd-pela-autarquia-de-lisboa/?utm_source=chatgpt.com (30.04.2025).

uma sanção por parte da CNPD e o facto de o TAC reforçar a legitimidade da atuação da Autoridade de Controlo evidenciando que a medida foi legal, proporcional e adequada às infrações cometidas. Convém salientar que o ajuste feito, pelo Tribunal, à coima aplicada, enalteceu que este regime sancionatório não só tem um caráter punitivo, mas também um caráter dissuasor e proporcional.

Conclusão

Ao longo da realização da presente dissertação, foi possível perceber o quão complexa é a temática do tratamento de dados pessoais e tudo o que a envolve, principalmente quando se fala da responsabilidade civil nos casos em que ocorram violações aos dados pessoais por incumprimento das disposições do regulamento. À medida que os dados pessoais se destacam na era digital como um recurso fundamental para a sua expansão, torna-se inevitável questionar como o direito pode responder eficazmente às ameaças que surgem do uso ilícito dos dados pessoais.

Ao longo do estudo deste tema, foi possível comprovar que o RGPD simboliza uma evolução significativa na regulamentação do processamento dos dados pessoais, tanto na sua abrangência territorial e material, como pela estipulação de deveres concretos quer ao responsável pelo tratamento, quer ao subcontratante e, consequentemente, pelo reconhecimento dos direitos inerentes aos titulares dos dados pessoais. Outro ponto fundamental da criação do regulamento, foi a estipulação de princípios fundamentais como por exemplo a licitude, a transparência, a minimização, a exatidão e a limitação da conservação, que aparecem como pilares centrais de um sistema que visa garantir um tratamento lícito, seguro e transparente dos dados.

Com a elaboração desta dissertação, foi possível constatar que, apesar de o responsável pelo tratamento continuar a ser o principal responsável pelo cumprimento das obrigações legais, o regulamento acentuou significativamente a responsabilidade do subcontratante, impondo-lhe deveres próprios e responsabilizando-o diretamente em caso de incumprimento. Nos casos em que hajam falhas no tratamento de dados pessoais, decorrentes da violação do RGPD, é fundamental analisar a responsabilidade civil com base no regime jurídico em vigor. É essencial garantir que existam formas eficazes de indemnizar os titulares que tenham sofrido prejuízos e que o responsável e/ou o subcontratante adotem uma postura proativa, ética e preventiva no processamento dos dados, reforçando a confiança dos cidadãos e a credibilidade das instituições.

Em resumo, a responsabilidade civil, no que diz respeito à proteção de dados, é um fator fundamental para garantir que as regras são cumpridas. A responsabilização por

uma prática ilícita, face ao tratamento de dados, não versa apenas na aplicação de sanções, procura também incentivar uma cultura de responsabilidade e respeito pela privacidade dos titulares dos dados. Um grande desafio que se coloca para o futuro, é assegurar que estas normas sejam aplicadas de forma eficaz e harmonizada, tanto a nível nacional como europeu, num mundo cada vez mais tecnológico e em constante modernização.

Bibliografia

Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa - *Manual da Legislação Europeia sobre Proteção de Dados*, Luxemburgo: Serviço das Publicações da União Europeia, 2022, edição 2018, disponível in Manual da Legislação Europeia sobre Proteção de Dados — Edição de 2018 (27.04.2025);

Assembleia da República, Tratado de Lisboa, disponível in Tratado de Lisboa (27.04.2025);

Barbosa, Mafalda Miranda, *Revista de Direito da Responsabilidade – Proteção de Dados e Causalidade: Reflexões a Propósito do AC. TJUE C-340/21, de dezembro de 2023*, Coimbra, Ano 6, 2024, disponível in Proteção de dados e causalidade: reflexões a propósito do Ac. TJUE C-340/21, de 14 de dezembro de 2023 – Mafalda Miranda Barbosa – Revista de Direito da Responsabilidade (27.04.2025);

Comissão Europeia - O que significa a proteção de dados «desde a conceção» e «por defeito»?, disponível in O que significa a proteção de dados «desde a conceção» e «por defeito»? - Comissão Europeia (27.04.2025);

Comissão Nacional de Proteção de Dados, de 13 de dezembro de 2021, Deliberação n.º 2021/1569 – *Violação do RGPD pelo Município de Lisboa*, disponível in https://www.cnpd.pt/comunicacao-publica/noticias/tribunal-confirma-violacao-do-rgpd-pela-autarquia-de-lisboa/?utm_source=chatgpt.com (30.04.2025);

Comissão Nacional de Proteção de Dados, de 13 de dezembro de 2021, Deliberação n.º 2021/1569 – *Violação do RGPD pelo Município de Lisboa*, disponível in https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-aplica-sancao-ao-municipio-de-lisboa/ (30.04.2025);

Conselho da Europa, Estados-Membros - O Conselho da Europa em resumo, disponível in Estados-Membros - O Conselho da Europa em resumo (27.04.2025);

Cordeiro, A. Barreto Menezes (Coordenação), *Comentários ao Regulamento geral de proteção de dados e á Lei n.º 58/2019*, Coimbra, Almedina, 2021.

Cordeiro, A. Barreto Menezes, *Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*, Reimpressão, Coimbra, Almedina, 2020.

Dias, Ana Francisca Pinto, *Revista de Direito da Responsabilidade - Responsabilidade Civil pelo Tratamento de Dados Pessoais: A Responsabilidade do Controller por Factos Próprios e por Factos de Outrem*, Coimbra, Ano 1, 2019, disponível in Responsabilidade civil pelo tratamento de dados pessoais: a responsabilidade do controller por factos próprios e por factos de outrem – Ana Francisca Pinto Dias – Revista de Direito da Responsabilidade (27.04.2025);

Diário da República, direito à não sujeição a decisões individuais automatizadas, disponível in Direito de não sujeição (a decisões individuais automatizadas) | DR (27.04.2025);

Diário da República, Processo de questões prejudiciais em Direito da União Europeia, disponível in Processo das questões prejudiciais (Direito da União Europeia) | DR (27.04.2025);

Instituto de Gestão Financeira e Equipamentos da Justiça, Encarregado de Proteção de dados, disponível in Encarregado de Proteção de Dados (27.04.2025);

Portal do DPO, Encarregado de Proteção de dados - Avaliação de Impacto sobre Proteção de Dados (AIPD), disponível in Avaliação de Impacto sobre Proteção de Dados - Portal do DPO - Encarregado de Protecção de Dados (27.04.2025);

Saldanha, Nuno, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica?* Como implementar? Lisboa, FCA – Editora de Informática, 2018.

Saldanha, Nuno, *RGPD – Guia para uma auditoria de conformidade, dados, privacidade, implementação, controlo, compliance*, Lisboa, FCA – Editora de Informática, 2018.

Santos, Patrícia Andreia Batista (2019) - "*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*" (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, disponível in RUN: A aplicação do novo regulamento geral de proteção de dados no contexto laboral (27.04.2025);

Sérvulo & Associados - *A indemnização de danos imateriais: A insuficiência da violação do Regulamento Geral sobre a Proteção de Dados e a desnecessidade de um limiar mínimo de gravidade*. Sérvulo Publications (11.05.2023), disponível in A indemnização de danos imateriais: A insuficiência da violação do Regulamento Geral sobre a Proteção de Dados e a desnecessidade de um limiar mínimo de gravidade, Sérvulo Publications, Knowledge - Sérvulo & Associados – Law firm, Portugal (27.04.2025);

União Europeia - História da União Europeia – 1945-59, disponível in História da União Europeia – 1945-59 | União Europeia (27.04.2025);

Universidade de Coimbra - Anonimização e Pseudonimização, disponível in Anonimização e Pseudonimização (27.04.2025);

Universidade de Coimbra - Princípios do Tratamento de Dados Pessoais, disponível in Princípios do Tratamento Dados (27.04.2025);

Universidade de Coimbra - Direito de Portabilidade dos Dados, disponível in Direito de portabilidade dos dados (27.04.2025);

Jurisprudência

Ac. do Tribunal de Justiça (Terceira Secção) de 14 de dezembro de 2023 – Proc. n.º C-340/21, disponível in CURIA - Documents (27.04.2025);

Ac. do TJUE de 4 de maio de 2023 – Proc. n.º C-300/21, disponível in CURIA - Documents (27.04.2025);

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

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 dos dados pessoais e à livre circulação desses dados.

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 aos tratamentos de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).