COIMBRA
BUSINESS
SCHOOL
iscac
100 ANOS
Politécnico de Coimbra

COIMBRA BUSINESS SCHOOL
iscac
100 ANOS
O tratamento de dados pessoais de saúde à luz do RGPD
Helena Santos
ISCAC | 2024

COIMBRA
BUSINESS
SCHOOL
iscac
100 ANOS
Politécnico de Coimbra

Helena Beatriz da Silva Santos

# O TRATAMENTO DE DADOS PESSOAIS DE SAÚDE À LUZ DO REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

Coimbra, setembro de 2024

Helena Beatriz da Silva Santos

# O TRATAMENTO DE DADOS PESSOAIS DE SAÚDE À LUZ DO REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

Coimbra, setembro de 2024

# 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

**"Artigo 12.º**

Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."

Declaração Universal dos Direitos Humanos

## AGRADECIMENTOS

A mim, por todo o esforço e dedicação que depositei em mim própria que me tornou numa mulher independente e com os pés bem assentes na terra.

À minha mãe que move mundos por mim, por ter o melhor colo do mundo, por tentar sempre compreender-me e por ensinar-me todos os dias a ser a melhor versão de mim.

Ao meu superpai, que ao longo da vida fez escolhas duras para me dar o futuro que ele não teve, por me ensinar que com trabalho, dedicação e sobretudo amor, chegamos onde queremos.

Ao meu irmão, que desde sempre foi o meu exemplo a seguir, que se tornou o meu ídolo e me ensinou que com poucas palavras dizemos muito.

À minha avó Rosa, que partiu a meio deste projeto, por ter rezado por mim até ao último dia, não há palavras para a descrever.

Por fim, a todos os meus amigos que fizeram o meu percurso ser mais leve e, hoje, celebram esta vitória como se fosse deles. Em especial, à minha amiga Xana que amparou todos os meus receios.

## RESUMO

O primeiro capítulo, tende a focar-se na evolução do direito à privacidade, isto é, quais os primeiros passos dados, em contexto internacional e europeu, com vista à proteção do direito à privacidade e o surgimento do direito à proteção de dados pessoais. Neste capítulo falamos de documentos internacionais que, se revelaram imprescindíveis, à forma como encaramos hoje, a urgência da proteção de dados pessoais e, que serviram de base ao RGPD, que são exemplo a Declaração Universal dos Direitos do Homem, a Carta dos Direitos Fundamentais da União Europeia e a respetiva importância do Tratado de Lisboa, a Convenção n.º 108 e a Diretiva n.º 92/1995. Ainda neste capítulo, abordaremos a transposição das normas legislativas internacionais para o ordenamento jurídico português, surgindo então a Lei n.º 58/2019.

O segundo capítulo dedica-se exclusivamente ao RGPD, onde é discutida a sua aplicação direta nos Estados-Membros da União Europeia, assentando na profunda análise das suas disposições, explorando as suas finalidades, bem como o impacto e os desafios da sua implementação.

Posteriormente, o terceiro capítulo discute o conceito de dados pessoais, distinguindo-os dos dados pessoais sensíveis, e os princípios que orientam seu tratamento, como a licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, conservação, integridade e confidencialidade e responsabilidade, destacando o papel central e imperativo do consentimento informado e livre.

O capítulo quarto explora o conceito de titular dos dados, estudando, ao detalhe quais os direitos destes, que surgiram com a implementação do RGPD, sendo eles o direito de acesso, que terá especial interesse para a análise do capítulo seguinte, o direito à retificação, ao apagamento, à limitação do tratamento, à portabilidade e à oposição.

Finalmente, no quinto e último capítulo, apresentamos um estudo de caso que explora a aplicação prática dos princípios estabelecidos pelo RGPD e pela Lei n.º 58/2019. Este estudo de caso tem como objetivo analisar o equilíbrio entre a necessidade de proteger dados pessoais sensíveis e outros direitos fundamentais igualmente garantidos por lei. É dado um foco particular ao direito de acesso em situações em que o titular dos dados já faleceu, estudando de que forma pode este proteger o acesso às suas informações e, do mesmo modo, quais as situações que a lei permite o acesso de terceiros às mesmas.

**Palavras-chave**: dados pessoais, dados pessoais sensíveis, proteção de dados, RGPD, consentimento, direito de acesso, princípio da administração aberta.

## ABSTRACT

The first chapter focuses on the evolution of the right to privacy, specifically the initial steps taken in the international and European contexts towards the protection of the right to privacy and the emergence of the right to personal data protection. In this chapter, we discuss international documents that have proven to be essential in shaping our current understanding of the urgency of personal data protection and which served as the foundation for the GDPR, such as the Universal Declaration of Human Rights, the Charter of Fundamental Rights of the European Union and the importance of the Treaty of Lisbon, Convention No. 108, and Directive No. 92/1995. Additionally, in this chapter, we will address the transposition of international legislative norms into the portuguese legal framework, leading to the emergence of Lei n.º 58/2019.

The second chapter is exclusively dedicated to the GDPR, where its direct application in the Member States of the European Union is discussed, focusing on an in-depth analysis of its provisions, exploring its purposes, as well as the impact and challenges of its implementation.

Subsequently, the third chapter discusses the concept of personal data, distinguishing it from sensitive personal data, and the principles guiding their processing, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability, highlighting the central and imperative role of informed and free consent.

The fourth chapter explores the concept of data subjects, examining in detail the rights that have emerged with the implementation of the GDPR, such as the right of access, which will be of particular interest for the analysis in the following chapter, as well as the right to rectification, erasure, restriction of processing, data portability, and the right to object.

Finally, in the fifth and last chapter, we present a case study that explores the practical application of the principles established by the GDPR and Law No. 58/2019. This case study aims to analyze the balance between the need to protect sensitive personal data and other fundamental rights equally guaranteed by law. Particular focus is given to the right of access in situations where the data subject is deceased, examining how this right can protect access to their information, and similarly, the situations in which the law allows third-party access to that information.

**Keywords**: personal data, sensitive personal data, data protection, GDPR, consent, right of access, open administration principle.

# ÍNDICE GERAL

TERMO DE RESPONSABILIDADE ..... 1

PENSAMENTO ..... 2

AGRADECIMENTOS ..... 3

RESUMO ..... 4

ABSTRACT ..... 6

ÍNDICE GERAL ..... 8

LISTA DE ABREVIATURAS, ACRÓNIMOS E SIGLAS ..... 12

INTRODUÇÃO ..... 13

CAPÍTULO I – A EVOLUÇÃO DO DIREITO À PRIVACIDADE ..... 15

1.1 Direito Internacional ..... 16

1.2 Direito da União Europeia ..... 18

1.3 Direito Nacional ..... 22

CAPÍTULO II – O REGULAMENTO GERAL DA PROTEÇÃO DE DADOS ..... 26

2.1. Enquadramento histórico ..... 26

2.2. As finalidades do RGPD ..... 27

2.3. A aplicação direta do RGPD ..... 29

2.4. O impacto do RGPD ..... 31

CAPÍTULO III – DADOS PESSOAIS ..... 33

3.1. O conceito de dados pessoais ..... 33

3.2. Dados sensíveis ..... 35

3.3. O tratamento de dados pessoais ..... 38

3.3.1. Princípios relativos ao tratamento de dados pessoais ..... 38

3.3.1.1. Princípio da licitude ..... 38

3.3.1.2. Princípio da lealdade ..... 40

3.3.1.3. Princípio da transparência ..... 42

1.3.1.1 Princípio da limitação das finalidades ..... 43

3.3.1.4. Princípio da minimização dos dados ..... 44

3.3.1.5. Princípio da exatidão ..... 44

3.3.1.6. Princípio da conservação ..... 45

3.3.1.7. Princípio da integridade e confidencialidade ..... 46

3.3.1.8. Princípio da responsabilidade ..... 46

3.3.2. O consentimento ..... 47

3.3.2.1. Manifestação da vontade ..... 49

3.3.2.2. Livre ..... 50

3.3.2.3. Específica ..... 51

3.3.2.4. Informada ..... 53

3.3.2.5. Inequívoca ..... 55

3.3.3. Condições de licitude do tratamento de dados sensíveis ..... 55

3.3.3.1. Consentimento ..... 56

3.3.3.2. Obrigações laborais ..... 57

3.3.3.3. Interesses vitais ..... 57

3.3.3.4. Fundações e associações ..... 58

3.3.3.5. Dados tornados públicos pelo próprio titular ..... 59

3.3.3.6. Processo judicial ..... 60

3.3.3.7. Interesses públicos ..... 60

3.3.3.8. Cuidados de saúde ..... 61

3.3.3.9. Saúde pública ..... 62

3.3.3.10. Arquivo, investigação científica ou histórica e fins estatísticos . 63

CAPÍTULO IV – OS DIREITOS DO TITULAR DOS DADOS PESSOAIS ..... 64

4.1. Direito de Acesso ..... 64

4.1.1. O princípio da administração aberta ..... 66

4.1.2. Direito de acesso aos documentos administrativos ..... 69

4.1.2.1. Acesso ao processo clínico ..... 73

4.2. Direito à retificação ..... 75

4.3. Direito ao apagamento (direito ao esquecimento) ..... 76

4.4. Direito à limitação do tratamento ..... 79

4.5. Direito de Portabilidade ..... 80

4.6. Direito de Oposição ..... 81

CAPÍTULO V – ESTUDO DE CASO ..... 83

CONCLUSÃO ..... 89

REFERÊNCIAS BIBLIOGRÁFICAS ..... 92

LEGISLAÇÃO ..... 94

JURISPRUDÊNCIA ..... 95

NETOGRAFIA ..... 96

# LISTA DE ABREVIATURAS, ACRÓNIMOS E SIGLAS

Al. – alínea;

CADA – Comissão de Acesso aos Documentos Administrativos;

CC. – Código Civil;

CEDH - Convenção Europeia dos Direitos Humanos;

CDOM – Código Deontológico da Ordem dos Médicos;

Cfr. – Conforme;

CNPD – Comissão Nacional da Proteção de Dados;

CPA – Código do Procedimento Administrativo.

CPC – Código de Processo Civil;

CRP – Constituição da República Portuguesa;

DUDH – Declaração Universal dos Direitos Humanos;

EOM – Estatuto da Ordem dos Médicos;

LADA – Lei de Acesso aos Documentos Administrativos;

N.º - número;

ONU – Organização das Nações Unidas;

Pág. – página.

RGPD – Regulamento Geral da Proteção de Dados Pessoais;

SS. – Seguintes;

TEDH - Tribunal Europeu dos Direitos do Homem;

TFUE – Tratado sobre o Funcionamento da União Europeia;

TUE – Tratado da União Europeia;

UE – União Europeia;

# INTRODUÇÃO

O tratamento de dados pessoais tornou-se numa questão central no mundo contemporâneo, muito devido às profundas transformações trazidas pelo fenómeno da Globalização e pela evolução tecnológica. A ascensão da nova Era Digital revolucionou a maneira como vivemos, trabalhamos e nos relacionamos, centralizando os dados pessoais e elevando-os a um patamar sem precedentes e nunca antes visto. No entanto, esta centralização dos dados coloca-nos a todos numa posição de vulnerabilidade, especialmente tendo em conta as consequências da modernização tecnológica, que ampliou consideravelmente o volume e a profundidade das informações pessoais recolhidas.

Atualmente, com a proliferação de dispositivos conectados à internet e o feroz crescimento das redes sociais, a recolha de dados pessoais intensificou-se de forma bastante considerável. Informações básicas, como o nome e a morada e, até detalhes mais sensíveis, como o histórico de navegação e os padrões de consumo, são constantemente recolhidos e armazenados em servidores espalhados por todo o mundo, acessíveis remotamente com extrema facilidade. Este processo, embora impulsionado pela procura de maior eficiência e inovação, traz consigo sérios desafios, especialmente no que toca à privacidade e à segurança dos titulares dos dados.

Até 2018, especialmente num contexto europeu, não havia um consenso legislativo a nível internacional que acompanhasse a crescente evolução tecnológica e, portanto, mostrou-se insuficiente para proteger e salvaguardar os interesses e direitos dos titulares dos dados. Ainda que a consciencialização dos indivíduos sobre a proteção das suas informações pessoais tenha aumentado com o passar dos anos, o risco de segurança associado à recolha de dados pessoais continua a crescer e, por isso, assistimos a episódios frequentes de *hackers* e *cyber* criminosos que exploram as vulnerabilidades dos sistemas de armazenamento de dados, o que ressalta a gravidade da situação que se vive. Esta lacuna legislativa reforçou a necessidade urgente de uma abordagem global mais coesa e atualizada para enfrentar os desafios emergentes na proteção de dados pessoais num cenário digital em constante transformação.

Em resposta a estas preocupações, muitos países têm vindo a adotar legislações mais rigorosas para proteger a privacidade dos cidadãos e a segurança dos seus dados. Entre estes esforços, destaca-se o Regulamento Geral de Proteção de Dados (RGPD) da

União Europeia, que entrou em vigor em 2018. O RGPD estabeleceu um conjunto abrangente de regras que visam garantir que os dados pessoais são tratados de forma segura, transparente e conforme os direitos dos seus titulares, impondo requisitos rigorosos para a recolha, armazenamento e tratamento, além de prever sanções significativas para o seu incumprimento.

Dentro deste vasto campo da proteção de dados, os dados de saúde merecem uma atenção especial devido à sua natureza extremamente sensível. Estes dados, que incluem informações sobre o estado físico e mental dos indivíduos, bem como aspetos íntimos como o histórico médico e predisposições genéticas, são particularmente vulneráveis a abusos. A proteção destes dados é crucial, uma vez que qualquer comprometimento pode ter consequências graves, desde a discriminação até riscos à integridade física e psicológica dos seus titulares. O RGPD, consciente destas peculiaridades, veio impor requisitos e princípios imperativos ao tratamento de dados pessoais, inclusive aos dados de saúde, assegurando que estes sejam objeto de tratamento com o máximo cuidado e proteção.

Assim sendo, a presente dissertação propõe uma análise detalhada sobre o tratamento de dados pessoais à luz do RGPD, com especial atenção às implicações legais e práticas deste Regulamento. O estudo aborda a evolução histórica do direito à privacidade, as complexidades do tratamento de dados sensíveis, como os de saúde, e os desafios enfrentados pelas organizações na aplicação prática destas normas. Além disso, a dissertação procura compreender de que forma o RGPD equilibra a necessidade de proteção de dados com outros direitos fundamentais igualmente protegidos, como é o caso do direito de acesso.

# CAPÍTULO I – A EVOLUÇÃO DO DIREITO À PRIVACIDADE

Atualmente, muito tendo em conta ao fenómeno da Globalização, é nos manifestamente percetível que a evolução tecnológica tem desempenhado um papel significativo na maneira como lidamos com a privacidade e a proteção dos nossos dados pessoais.

A centralização dos dados pessoais e a crescente importância a eles associada, levou-nos ao surgimento de uma nova Era: a Era Digital[1], trazendo consigo profundas transformações na história contemporânea, que revolucionaram a forma como vivemos, trabalhamos e nos relacionamos. Esta matéria assume uma importância incontestável no quotidiano das pessoas comuns, colocando-nos, a todos, numa posição de fragilidade face às consequências da modernização tecnológica.

Com o avanço da tecnologia, especialmente com a proliferação de dispositivos ligados à internet e o crescimento das redes sociais, a recolha de dados pessoais viu-se cada vez mais intensificada. Isto traduz-se numa maior disponibilização de informações básicas e pessoais por parte do utilizador, como o nome, morada, número de telefone e detalhes mais sensíveis como o histórico de navegação na internet e padrões de compra. Desta forma, as entidades capacitadas da recolha de dados podem armazenar este tipo de informações nos seus servidores, em qualquer parte do mundo e, aceder remotamente às mesmas com extrema facilidade. Tal facto pode comprometer a proteção e segurança destes dados de cariz tão pessoal, especialmente tendo em conta que o regime de proteção de dados pessoais não é uniforme em todos os países, gerando assim, um legítimo clima de insegurança por parte dos utilizadores.

Embora os indivíduos estejam, cada vez mais, a tornar-se conscientes em relação às informações pessoais que disponibilizam na *internet*, suscetíveis de recolha por parte das entidades responsáveis para o efeito, a crescente recolha de dados pessoais pode refletir-se num progressivo risco de segurança. Infelizmente, cada vez mais assistimos a episódios de *hackers* e *cyber* – criminosos que, de forma constante, exploram as

[1] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 27, pode ler-se "A emergência do Direito da proteção de dados consubstancia mais um reflexo do advento de uma nova Era: a Era Digital. Esta nova fase da evolução da nossa Sociedade encontra nos progressos tecnológicos a sua fonte de rotura com o passado recente. As transformações fazem-se sentir a todos os níveis e em todas as ordens normativas: a moral, religiosa, do trato social e jurídica".

vulnerabilidades dos sistemas de armazenamento de dados, a fim de obter informações pessoais e até financeiras.

Face a estas questões, atualmente, muitos países têm vindo a implementar legislação mais rigorosa com vista à proteção da privacidade dos cidadãos e dos seus dados. Estes regulamentos impõem requisitos rigorosos para a recolha de dados pessoais, bem como, para armazenamento e tratamento, ao mesmo tempo que, estipulam sanções significativas para o seu não cumprimento. É o caso da União Europeia que adotou o Regulamento Geral de Proteção de Dados (RGPD), que estudaremos adiante.

Contudo, importa-nos refletir, como chegamos até aqui e quais os primeiros passos dados, em contexto internacional, com vista à proteção quer do direito à privacidade como o direito da proteção dos dados pessoais e a sua respetiva evolução[2].

## 1.1 Direito Internacional

O mundo enfrentou um período negro de duras batalhas e destruições culturais, físicas e humanas, durante a II Guerra Mundial, que terminou em 1945 após seis penosos anos. Face ao débil cenário que o mundo todo enfrentava, surgiu a necessidade de precaver conflitos como este e, criar mecanismos que protegessem os direitos humanos que, até aqui, eram violados constantemente. Foi então que, a 24 de outubro de 1945, sensivelmente dois meses após o termo do conflito, foi criada a Organização das Nações Unidas (ONU), com o propósito de reconstruir os direitos humanos e dar relevo à dignidade humana[3]. À época composta por 51 Estados-membros[4], a ONU dá a oportunidade aos países pertencentes de procurarem soluções em conjunto para os problemas do mundo, preservando a soberania e os interesses nacionais em prol do desenvolvimento e paz mundial, com base nos princípios da justiça, dignidade humana e

[2] NETO, Eugênio Facchini & DEMOLINER, Karine Silva, Direito À Privacidade Na Era Digital – Uma Releitura Do ART. XII Da Declaração Universal Dos Direitos Humanos (DUDH) NA Sociedade Do Espetáculo, *Revista Internacional Consinter De Direito*, ANO V – NÚMERO IX, 2º Semestre, 2019, pág, 120, a propósito da evolução histórica da proteção de dados pessoais – "(…) a evolução do conceito de privacidade, tal como conhecido no final do século XIX e na primeira metade do século XX, para uma noção de proteção de dados, em razão da perceção de que a violação da privacidade atualmente se dá através do acesso e manipulação de nossos dados pessoais – dados esses obtidos muitas vezes com a nossa própria ingênua colaboração".

[3] CUNHA, Sílvia Maria Duarte, *Eliminação dos dados de Saúde: Um Direito do Paciente?* Dissertação de mestrado integrado em Medicina, Faculdade de Medicina, Universidade do Porto, Porto, 2018, pág. 5.

[4] Atualmente é composta por 193 Estados-membros.

no bem-estar de todos[5]. Assim, os objetivos desta instituição passam por: manter a paz mundial; incentivar à segurança e desenvolvimento económico e progresso social; proteger os direitos humanos; proteger o meio ambiente; e despender de ajuda humanitária em caso de catástrofes naturais e conflitos armados.

Três anos após a sua criação, em 1948, surgiu a Declaração Universal dos Direitos Humanos (DUDH), como consequência das atrocidades provocadas pelo conflito mundial e que conduziram a um desconhecimento e desprezo total dos direitos do Homem. Trata-se de um texto jurídico, com mais de 70 anos, que tem como fundamento a liberdade, a justiça e a paz do mundo e zela pela proteção dos direitos do homem através de um regime de direito, mediante respeito universal e efetivo destes direitos e das liberdades fundamentais – pode ler-se no seu preâmbulo.

Este diploma consagra 30 artigos que visam proteger os direitos humanos básicos, como os princípios da dignidade, liberdade e fraternidade humana – contemplada nos seus 2 primeiros artigos. Seguem-se os artigos 12.º a 17.º, onde são elencados direitos cívicos como o direito à privacidade, à honra, à nacionalidade e à propriedade privada. Nos artigos seguintes, 18.º a 20.º, podemos constatar liberdades imprescindíveis ao ser humano para viver em comunidade, como o direito à liberdade de pensamento, opinião e de expressão bem como a liberdade religiosa e o seu respetivo culto. São ainda considerados direitos económicos, sociais e culturais, nos artigos 21.º a 27.º, isto é, direito ao trabalho bem como às suas boas condições e ainda o direito à educação. Por fim, os três últimos artigos, 28.º a 30.º, solidificam os ideais e o propósito da DUDH, reforçando a sua aplicação tanto no panorama nacional como internacional, devendo a sua interpretação ser unânime em todos os cenários e, ainda destacam os deveres que cada indivíduo tem para com a comunidade e, portanto, no exercício destes direitos e no gozo destas liberdades, ninguém está sujeito senão às limitações estabelecidas pela lei.

No que concerne ao estudo da presente dissertação, destacamos o artigo 12.º que consagra, pioneiramente, a tutela da vida privada:

> Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua

[5] ONU, acedido e consultado a 12/08/2024, disponível em https://unric.org/pt/historia-da-onu/.

> honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.
> (Artigo 12.º da Declaração Universal dos Direitos do Homem, 1948).

O artigo 12.º da DUDH, serviu de base sólida para a evolução dos conceitos de privacidade e proteção de dados, sendo este um dos primeiros documentos internacionais a consagrar explicitamente o direito à privacidade como um direito fundamental[6]. Como tal, a tutela da vida privada neste diploma, teve influência direta em todas as legislações que se seguiram, baseando-se nos princípios convencionados na DUDH, como é exemplo a Convenção Europeia dos Direitos Humanos de 1953.

## 1.2 Direito da União Europeia

Em 1953, entrou em vigor a Convenção Europeia dos Direitos Humanos (CEDH), inspirada na DUDH, cujo nome oficial é "Convenção para a proteção dos Direitos do Homem e das liberdades fundamentais".

Através deste diploma jurídico nasceu o Conselho da Europa – composto pelos Estados-membros, tendo como finalidade realizar uma união mais estreita entre os seus Membros, visando a proteção e desenvolvimento dos direitos do Homem e das liberdades fundamentais[7]. Neste sentido, surgiu o Tribunal Europeu dos Direitos do Homem (TEDH)[8], uma entidade internacional com vigência nos Estados-membros, e que garante a eficácia da proteção destes direitos.

A par da DUDH, na Convenção encontramos liberdades fundamentais que constituem verdadeiras bases da justiça e da paz no mundo, como é o caso do direito à liberdade e à segurança (artigo 5.º) e o direito ao respeito pela vida privada e familiar

[6] MIRANDA, Jorge, *Direitos Fundamentais: Introdução Geral*, Diversos, Lisboa, 1999, pág. 11, o autor entende os direitos fundamentais como "direitos ou posições subjetivas das pessoas enquanto tais, individual ou institucionalmente consideradas, assentes na Constituição". Quer isto dizer que, este tipo de direitos são inerentes à existência humana e representam uma natureza de necessidade que garantem aspetos fulcrais à autonomia e vida humana, como direitos básicos das pessoas com a finalidade de assegurar a igualdade e liberdade entre indivíduos. Por essa razão, os direitos fundamentais são matéria jurídica de extrema complexidade e, portanto, carecem de alguma cautela na sua análise.

[7] Pode ler-se no preâmbulo da Convenção Europeia dos Direitos Humanos.

[8] Artigo 19.º da CEDH, pode ler-se: "A fim de assegurar o respeito dos compromissos que resultam, para as Altas Partes Contratantes, da presente Convenção e dos seus protocolos, é criado um Tribunal Europeu dos Direitos do Homem, a seguir designado "o Tribunal", o qual funcionará a título permanente".

(artigo 8.º), profundamente influenciado pelo disposto no artigo 12.º da DUDH – matéria a destacar no presente trabalho.

A década de 1980, foi importante para a consolidação em matéria de dados pessoais, conceito recente para a época. A Convenção n.º 108[9], foi decisiva para o efeito, sendo esta a primeira convenção internacional juridicamente vinculativa dedicada exclusivamente à proteção de dados pessoais. Aqui surgiram novos termos, conceitos e princípios que moldaram a proteção dos dados pessoais para o futuro, vejamos o artigo 2.º, que refere, taxativamente definições imprescindíveis ao tema, como o conceito de dados pessoais[10] e o tratamento de dados[11], bem como a sua aplicação transversal ao direito público e privado[12]. Já no artigo 5.º, reparemos nos respetivos princípios[13] pelos quais estes conceitos se devem fazer reger e, que ainda hoje, são a base de legislações modernas sobre proteção de dados, criando assim, uma base comum que influenciou diretamente o desenvolvimento das políticas de privacidade no contexto nacional e internacional.

Nesta Convenção, como referido e, à semelhança do que acontece nos anteriores diplomas, reitera-se o direito ao respeito pela vida privada, procurando conciliá-lo com o fenómeno da Globalização e a liberdade de informação. Assim, pode ler-se no seu preâmbulo,

> Considerando que é necessário garantir a dignidade humana e a proteção dos direitos humanos e das liberdades fundamentais de todas as pessoas e, dada a diversificação, intensificação e globalização do tratamento de

[9] Convenção n.º 108 para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal do Conselho da Europa, de 28 de janeiro de 1981.

[10] Artigo 2.º n.º 1 al. a) da Convenção n.º 108 esclarece o conceito de "dados pessoais": "refere-se a qualquer informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados")";

[11] Artigo 2.º n.º 1 al. b) da Convenção n.º 108 esclarece o conceito de "tratamento de dados": "refere-se a qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, tais como a recolha, armazenamento, preservação, alteração, recuperação, divulgação, disponibilização, supressão, destruição ou execução de operações lógicas e/ou aritméticas sobre esses dados;"

[12] Artigo 3.º n.º 1 da Convenção n.º 108, pode ler-se "Cada Parte compromete-se a aplicar a presente Convenção ao tratamento de dados sob a sua jurisdição nos setores público e privado, garantindo assim o direito de todas as pessoas à proteção dos seus dados pessoais".

[13] Artigo 5.º n.º 4 da Convenção n.º 108, "4. Os dados pessoais sujeitos a tratamento deverão ser: a) tratados de forma justa e transparente; b) recolhidos para finalidades explícitas, específicas e legítimas e não tratados de forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos é, sob reserva de salvaguardas apropriadas, compatível com esses fins; c) adequados, pertinentes e não excessivos relativamente às finalidades para as quais são tratados".

> dados e dos fluxos de dados pessoais, a autonomia pessoal com base no direito de uma pessoa ao controlo dos seus dados pessoais e do tratamento desses dados;
> (Preâmbulo da Convenção n.º 108 para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal do Conselho da Europa, de 28 de janeiro de 1981).

Para além disso, a Convenção n.º 108, reconhece também no seu preâmbulo que é "necessário promover, a nível mundial, os valores fundamentais, do respeito pela primazia e pela proteção dos dados pessoais, comprometendo-se assim à livre circulação de informação entre as pessoas". Neste sentido, a Convenção tem como finalidade, proteger todas as pessoas no que toca ao tratamento dos seus dados pessoais, por forma a contribuir para o respeito dos seus direitos humanos e liberdades fundamentais, especialmente, no que toca ao direito à vida privada, cfr. o artigo 1.º do presente diploma.

Em 1995 surgiu a Diretiva n.º 95/46/CE[14], relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que teve um impacto profundo e duradouro na forma como a proteção de dados pessoais foi abordada na União Europeia. Antes da Diretiva n.º 95/46/CE, os diplomas que regulavam a proteção de dados variavam amplamente entre os Estados-Membros da União Europeia, pelo que, um dos principais objetivos desta Diretiva foi, precisamente, harmonizar a regulamentação no âmbito da proteção dos dados pessoais, estabelecendo um quadro uniforme em todos os países da UE. Contudo, este diploma foi, posteriormente, revogado com a entrada em vigor do Regulamento Geral da Proteção de Dados Pessoais (RGPD), em 2018.

Ainda no contexto da União Europeia, destacamos a Carta dos Direitos Fundamentais da União Europeia[15], da qual sublinhamos, desde já, o artigo 8.º[16],

[14] Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

[15] Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, com as necessárias adaptações em 12 de dezembro de 2007;

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

profundamente inspirado nas disposições da Diretiva n.º 95/46/CE, pelo artigo 8.º da CEDH e ainda pelas considerações do Tratado sobre o Funcionamento da União Europeia (TFUE)[17]. O artigo 8.º, é inovador, já que, não só reconhece o interesse e a natureza fundamental e universal do direito à proteção de dados pessoais, no seu n.º 1 a par com o disposto no artigo 16.º n.º 1 do TFUE, como também, elenca taxativamente no n.º 2, a forma como estes dados devem ser recolhidos, armazenados e tratados, devendo para o efeito, reger-se pelos princípios fundamentais da proteção de dados que, hoje, podemos encontrar ao longo do artigo 5.º do RGPD, que estudaremos, posteriormente, com mais detalhe. Ademais, entendemos ainda do n.º 2, o consentimento como condição imperativa para o respetivo tratamento dos dados, pelo que, deve o titular, gozar do direito de acesso e retificação dos mesmos. Para tal facto, dispõem a Carta no n.º 3 do artigo 8.º que, a fiscalização de todos estes preceitos deve ser efetuada por uma entidade independente, regulada por cada Estado-Membro.

Não menos importante é o artigo 7.º[18], em harmonia com o disposto no artigo 8.º da CEDH, e intimamente ligado ao artigo 8.º da Carta, garante o direito ao respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, criando limites legais à interferência de entidades públicas e privadas. A Carta foi pioneira na distinção destes dois direitos, igualmente fundamentais, o direito à vida privada e familiar e o direito à proteção de dados. No entanto, é fundamental, consciencializarmo-nos da sua distinção, pelo que, o direito à vida privada e familiar é mais amplo e cobra a proteção da intimidade pessoal e familiar, enquanto o direito à proteção de dados pessoais trata especificamente do tratamento de informações pessoais. Ambos os direitos são complementares e essenciais para assegurar a dignidade e a privacidade dos indivíduos na Nova Era.

A propósito do valor jurídico e moral da Carta, Gomes Canotilho (2001)[19], diz-nos que "a elaboração de uma carta europeia de direitos fundamentais pretende recortar um conjunto de direitos juridicamente vinculativos das instituições da União Europeia. O

[17] Para melhor compreensão do TFUE, destacamos o artigo 1.º do diploma, onde se pode ler "1. O presente Tratado organiza o funcionamento da União e determina os domínios, a delimitação e as regras de exercício das suas competências. 2. O presente Tratado e o Tratado da União Europeia constituem os Tratados em que se funda a União. Estes dois Tratados, que têm o mesmo valor jurídico, são designados pelos termos "os Tratados".".

[18] Artigo 7.º da Carta, pode ler-se: "Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações".

[19] RIQUINHO, Ana Luísa, VENTURA, Catarina Sampaio, ANDRADE, J. C. Vieira de, CANOTILHO, J. J. Gomes, GORJÃO-HENRIQUES, Miguel, RAMOS, R. M. Moura, e, MOREIRA, Vital, *Carta de Direitos Fundamentais da União Europeia*, Coimbra Editora, 2001, pág. 13.

seu primeiro objetivo é, assim, a positivação de direitos através da sua incorporação jurídica no ordenamento da União. Em segundo lugar, pretende-se positivar os direitos conferindo-lhes um valor de *Fundamental Rights* e atribuindo-lhes uma hierarquia materialmente superior no quadro das fontes de direito da União Europeia. Significa isto a fundamentalização formal e material desses direitos. Fundamentalização formal porque as normas da carta deverão ser incluídas no tratado e aí colocadas no grau hierarquicamente superior da ordem jurídica e comunitária".

Por fim, importa considerar o valor jurídico da Carta. A Carta dos Direitos Fundamentais da UE, só passou a ser vinculativa com a entrada em vigor do Tratado de Lisboa (2009)[20] que, atribuiu caráter jurídico à mesma. Até então, a Carta tinha um mero caráter político e declarativo, sem qualquer força jurídica vinculativa. Pode ler-se no artigo 6.º n.º 1 do Tratado da União Europeia (TUE), "a União reconhece os direitos, as liberdades e os princípios enunciados na Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, com as adaptações que lhe foram introduzidas em 12 de dezembro de 2007, em Estrasburgo, e que tem o mesmo valor jurídico que os Tratados. (…)". A partir daqui, União Europeia reconhece os direitos, liberdades e princípios estabelecidos na Carta, conferindo-lhe um papel central no sistema jurídico da UE. Quer isto dizer que, o Tratado de Lisboa converteu o caráter declarativo da Carta dos Direitos Fundamentais da UE num instrumento jurídico de aplicação obrigatória, integrando-a no tecido normativo da UE, por forma a assegurar que, os direitos nela previstos sejam respeitados em todas as ações e políticas da UE[21].

## 1.3 Direito Nacional

O artigo 16.º da Constituição da República Portuguesa (CRP) dita no n.º 1 que "os direitos fundamentais consagrados na Constituição não excluem quaisquer outros

[20] PARLAMENTO EUROPEU, *Trado de Lisboa*, acedido e consultado em 13/08/2024, disponível em https://www.parlamento.pt/europa/Paginas/TratadodeLisboa.aspx, pode ler-se "O Tratado de Lisboa, entrou em vigor a 1 de dezembro de 2009, foi assinado em Lisboa, a 13 de dezembro de 2007, no culminar da terceira Presidência portuguesa do Conselho da União Europeia. É um Tratado composto pelos dois principais Tratados da UE revistos: o Tratado da União Europeia (TUE) e o Tratado que institui a Comunidade Europeia (agora designado Tratado sobre o Funcionamento da União Europeia - TFUE), bem como por vários protocolos e declarações, que se encontram em anexo e dele fazem parte integrante.".

[21] Artigo 51.º da Carta, pode ler-se "As disposições da presente Carta têm por destinatários as instituições, órgãos e organismos da União, na observância do princípio da subsidiariedade, bem como os Estados-Membros, apenas quando apliquem o direito da União. Assim sendo, devem respeitar os direitos, observar os princípios e promover a sua aplicação, de acordo com as respetivas competências e observando os limites das competências conferidas à União pelos Tratados.".

constantes das leis e das regras aplicáveis de direito internacional", o que quer dizer que, os direitos previstos e legislados na CRP, são complementares aos dispostos na legislação internacional, "os preceitos constitucionais e legais relativos aos direitos fundamentais devem ser interpretados e integrados de harmonia com a Declaração Universal dos Direitos do Homem", n.º 2. Mais acrescenta o artigo 8.º n.º 1 e 2 que "as normas e os princípios de direito internacional geral ou comum fazem parte integrante do direito português; as normas constantes de convenções internacionais regularmente ratificadas ou aprovadas vigoram na ordem interna após a sua publicação oficial e enquanto vincularem internacionalmente o Estado Português.".

Assim, no ordenamento jurídico português, o direito à proteção de dados pessoais encontra-se previsto no artigo 35.º da Constituição da República Portuguesa (CRP), que no entender de Gomes Canotilho e Vital Moreira (2010)[22], traduz-se num tratamento de dados pessoais informatizados que abrange não "apenas a individualização, fixação e recolha de dados, mas também a sua conexão, transmissão, utilização e publicação". Doutrina esta que servirá de base ao estudo dos preceitos elencados no artigo 35.º.

Ao longo dos anos temos vindo a assistir a um grande e crescente desenvolvimento tecnológico que têm como consequência a "pegada digital", isto é, um rasto informático que é deixado por toda e qualquer utilização da *internet*, falamos por exemplo de movimentação de contas bancárias, compras *on-line*, portagens eletrónicas, redes sociais e visita de sites na *internet*. Neste sentido, foi essencial determinar este direito como um direito fundamental, tendo sempre por base a proteção do indivíduo neste meio.

O direito à proteção de dados provem de certos "direitos-mãe"[23], sendo eles o desenvolvimento da personalidade, a dignidade humana e a intimidade da vida privada. Existe uma estreita relação entre o direito da proteção de dados pessoais e o seu respetivo tratamento informático que, por sua vez, está intimamente relacionado com os "direitos-mãe" acima mencionados. Quer isto dizer que, quanto mais o conteúdo dos dados em causa se relaciona com a dignidade, autodeterminação e personalidade do indivíduo, ou

[22] CANOTILHO, José Gomes & MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, 4.ª Edição, Vol. I, Coimbra, Coimbra Editora 2010, pág. 548.

[23] CANOTILHO, José Gomes & MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, pág. 549, pode ler-se "O conjunto de direitos fundamentais relacionados com o tratamento informático de dados pessoais (…) arranca de alguns «direitos-mãe» em sede de direitos, liberdades e garantias. (…) O enunciado «dados pessoais» exprime logo a estreita conexão entre estes direitos e o respetivo tratamento informático;".

seja, quanto mais pessoais forem, mais restrições são impostas quer à sua recolha quer à sua utilização, como é o caso de dados bancários e dados de saúde que, se revestem de um extremo caráter pessoal e, portanto, carecem de um tratamento delicado e limitado.

Acontece que o direito à proteção de dados pessoais figura-se como um direito base, que se desdobra em tantos outros. Neste sentido, ao longo do artigo 35.º da CRP, podemos verificar alguns direitos fundamentais implícitos no âmbito da proteção de dados, com o objetivo de reafirmar o direito à autodeterminação informacional[24], ou seja, ao controlo da informação disponibilizada. No seu n.º 1, presenciamos o direito de acesso aos dados informatizados que digam respeito ao indivíduo, ou seja, existe um direito ao conhecimento dos dados pessoais existentes nos registos informáticos público ou privados e o direito de obter informações relativas à sua finalidade; o direito à contestação e atualização, que se traduz na faculdade de retificar, complementar ou atualizar os dados constantes no sistema. O n.º 2 e a parte final do n.º 4 limitam este direito de acesso, concedendo autorizam a terceiros em casos muito específicos e previstos na lei[25]. A acrescentar que o n.º 3 prevê a proibição, em regra, dos dados pessoais sensíveis, que estudaremos com mais detalhe no Capítulo III.

A presente dissertação tende a focar-se nos dados de saúde que se caracterizam como dados sensíveis, por se tratarem de dados com extremo caráter pessoal e, por isso, estão intimamente ligados aos dados pessoais, já que dizem respeito à intimidade da vida privada de cada um e, portanto, devem ser respeitados e limitados neste sentido, tal como previsto no artigo 26.º n.º 1 da CRP. Quer isto dizer, que os dados de saúde são tutelados como direitos fundamentais, sendo, por isso, o artigo 35.º n.º 3 do presente diploma, uma garantia adicional ao artigo 26.º. Para Gomes Canotilho e Vital Moreira (2010)[26], o artigo 35.º n.º 3, oferece uma proteção ampla e concreta do direito à privacidade e à intimidade estipulado no artigo 26.º. Esta garantia concretiza e assegura a proteção do direito à

[24] BOTELHO, Catarina Santos, *Novo ou velho direito? – O Direito ao esquecimento e o princípio da proporcionalidade no constitucionalismo global*, AB INSTANTIA, V (7), 2017, pág 5, https://papers.ssrn.com/sol3/results.cfm, "O direito à autodeterminação informativa, consagrado no artigo 35.º da Constituição portuguesa, visa impedir a instrumentalização da pessoa a mero objeto de informações. O n.º 1 do artigo 35.º procura obstar a intromissões abusivas na esfera privada das pessoas mediante a recolha e tratamento de dados pessoais informatizados. (…) O n.º 2 e a parte final do n.º 4 do artigo 35.º autorizam o legislador a restringir este direito, concedendo excecionalmente acesso de terceiros e interconexão de dados".

[25] Cfr. a Lei de Execução do RGPD, Lei n.º 58/2019, 8 de agosto, versão em vigor.

[26] CANOTILHO, José Gomes & MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, pág. 553

privacidade e à intimidade no contexto da era digital e da informática, assegurando que os direitos fundamentais sejam respeitados no âmbito da proteção de dados.

O Código Civil prevê também os direitos de personalidade já que "consagra o direito à reserva sobre a intimidade da vida privada, incluindo-o entre os chamados "direitos de personalidade", nos termos do artigo 70.º a 80.º do CC.

Por último e, ainda no ordenamento jurídico português, existe legislação ordinária que regulam a matéria da proteção de dados pessoais, como é o caso da Lei n.º 58/2019 de 8 de agosto, a Lei de Proteção de Dados Pessoais (LPD[27]), que veio revogar a Lei n.º 67/98 de 26 de outubro, que resultou da transposição da Diretiva 95/46/CE, que por sua vez, foi revogada pela entrada em vigor do RGPD. Esta disposição legal visa a proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais e à livre circulação dos mesmos.

Não menos importante, importa referir que, no sentido de assegurar a regulamentação e a proteção dos dados pessoais, elencados nos artigos 35.º e 268.º n.º 2 da CRP, surgiram algumas entidades cujo objetivo passa, essencialmente, por garantir a eficácia da preservação dos dados pessoais – a CADA e a CNPD. A Comissão de Acesso aos Documentos Administrativos (CADA) é uma entidade pública independente e o seu objetivo passa, essencialmente, por assegurar o cumprimento das disposições legais no que toca ao acesso a informação administrativa, previstas na LADA.[28] A Comissão Nacional da Proteção de Dados (CNPD), é igualmente uma entidade independente que tem poderes para controlar e fiscalizar todo o processo de tratamento de dados pessoais, isto é, é a entidade nacional responsável por salvaguardar o cumprimento das disposições do RGPD e da Lei n.º 58/2019, que estudaremos ao detalhe a seguir.[29] É de salientar que a CNPD coopera com outras entidades estrangeiras, sempre com o objetivo de preservar os direitos dos indivíduos de pessoas residentes no estrangeiro.

[27] Artigo 1.º n.º 1 da Lei n.º 58/2019, pode ler-se: "A presente lei aplica-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante, mesmo que o tratamento de dados pessoais seja efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público, aplicando-se todas as exclusões previstas no artigo 2.º do RGPD.".

[28] Lei de acesso aos documentos administrativos, Lei n.º 26/2016, 22 de agosto. Ver Capítulo IV, Ponto 4.1.

[29] Artigo 3.º n.º 1 al. q) e artigo 43.º e ss da Lei 58/2019.

# CAPÍTULO II – O REGULAMENTO GERAL DA PROTEÇÃO DE DADOS (RGPD)

## 2.1. Enquadramento histórico

Todas as normas legislativas, quer a nível nacional ou europeu, estudadas no Capítulo I, refletem a preocupação atual e crescente em relação à proteção da privacidade dos cidadãos no contexto da evolução tecnológica e da Globalização. A integração dos dados pessoais nas bases de dados, juntamente com o progresso tecnológico, tornou-se uma realidade cada vez mais presente no nosso dia-a-dia. E, portanto, levanta preocupações legítimas sobre como os dados são recolhidos, armazenados, processados e partilhados, e de que forma estes podem afetar a privacidade e os direitos individuais.

Esta incerteza jurídica, resulta do facto de que a legislações até então existentes e, estudadas no Capítulo I, não conseguiam acompanhar o ritmo acelerado da evolução tecnológica no âmbito da recolha de dados e o seu respetivo tratamento. Tal facto pode levar à existência de lacunas da lei no que toca à proteção da privacidade dos cidadãos e, consequentemente, resultar em abusos por parte das entidades e organizações responsáveis pelo tratamento deste tipo de dados.

Quer isto dizer que, à medida a que assistimos ao fugaz crescimento tecnológico, tornou-se crucial estabelecer um ponto de equilíbrio entre as entidades capacitadas e responsáveis pela recolha de dados, a legislação e os próprios indivíduos[30].

Para o efeito, a Comissão Europeia propôs implementar o Regulamento Geral da Proteção de Dados Pessoais (RGPD)[31] que representa um claro esforço dos Estados-Membros em abordar estas questões e fortalecer os direitos dos cidadãos europeus em relação à proteção dos seus dados pessoais. Esta é uma legislação robusta assente na proteção e tratamento dos dados pessoais, que por muitos foi encarada como a primeira

[30] KPMG, *O Impacto do Regulamento Geral de Proteção de Dados em Portugal*, Estudo, março 2017, pág. 2, acedido e consultado em 13/08/2024, disponível em https://www.centromarca.pt/folder/conteudo/1722_7_pt-2017-rgpd.pdf, identifica que o grande desafio em fazer face ao progresso tecnológico "está em garantir o controlo sobre a privacidade dos dados nesta nossa sociedade […] onde a crescente adoção da internet, das redes sociais e de modelos de negócio digitais criam uma equação de resolução difícil: por um lado, as pessoas sentem-se atraídas e partilham (às vezes voluntariamente, outras de forma pessoas sentem-se atraídas e partilham (às vezes voluntariamente, outras de forma inconsciente) dados da sua vida pessoal, frequentemente sem considerarem os potenciais efeitos colaterais; por outro, as Organizações capturam cada vez mais informação sobre os seus clientes, geralmente com o objetivo de fornecer mais e melhores serviços, ou como forma de monetizar a informação".

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

reforma em matéria de dados pessoais na Europa, que entrou em vigor a 25 de maio de 2018, com aplicação em todos os Estados-Membros da UE, substituindo em Portugal a Lei n.º 67/98, que transpõe para a ordem jurídica portuguesa a anterior Diretiva 95/46/CE[32], entrando em vigor, mais tarde, a Lei n.º 58/2019 de 8 de agosto, que se alinha diretamente ao Regulamento aplicável uniformemente em todos os Estados-Membros, o RGPD[33].

## 2.2. As finalidades do RGPD

Assim sendo, entendemos a extrema responsabilidade da União Europeia, enquanto união económica e política[34], em relação à preservação e garantia dos direitos fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia (CDFUE) e na consolidação de um Mercado Único Digital [35]. Neste contexto, especialmente numa era de modernização, mudanças tecnológicas e crescimento da consciência individual numa "*aldeia global informatizada*", é crucial assegurar a proteção de dados pessoais e a aplicação da lei para prevenir a criminalidade[36].

A implementação do RGPD não teve como principal objetivo a proteção dos interesses individuais dos titulares dos dados, mas sim, regular o tratamento dos dados

[32] Considerando (3) do RGPD, "A Diretiva 95/46/CE do Parlamento Europeu e do Conselho (4) visa harmonizar a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros".

[33] Considerando (9) do RGPD, "Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE.".

[34] COMISSÃO EUROPEIA, *A União Europeia*, acedido e consultado em 14/08/2024, disponível em *https://portugal.representation.ec.europa.eu/quem-somos/uniao-europeia_pt*, pode ler-se "A União Europeia é uma união económica e política de características únicas, constituída por 27 países europeus que, em conjunto, abarcam grande parte do continente europeu.".

[35] COMISSÃO EUROPEIA, *Mercado Único Digital*, acedido e consultado em 14/08/2024, disponível em https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_pt#policy-areas.

[36] MOREIRA, Tiago Filipe Monteiro, *O Impacto do Regulamento Geral da Proteção de Dados Pessoais nas Organizações: Um Novo Paradigma*, Dissertação de mestrado em Solicitadoria, Instituto Superior de Contabilidade e Administração de Coimbra, Instituto Politécnico de Coimbra, 2018, pág. 3.

pessoais. Quando falamos em interesses individuais dos titulares, referimo-nos, inevitavelmente, aos direitos fundamentais que protegem aspetos essenciais à vida humana, como o direito à privacidade. Acontece que, este tipo de direitos, os chamados direitos de personalidade, já se encontram previstos e regulados noutras normas gerais e, por isso, a essência do Regulamento, não passa por proteger estes direitos diretamente, mas sim, por estabelecer um quadro legal, uniforme e abrangente para o tratamento de dados pessoais em toda a União Europeia, cfr. o artigo 1.º do Regulamento. O foco do RGPD está na regulamentação do tratamento dos dados, por forma a assegurar que as empresas, organizações e autoridades públicas que lidam com os dados pessoais e o seu tratamento, o façam de forma legal, ética e transparente[37].

Embora o RGPD tenha como principal função a regulamentação do tratamento de dados, não quer isto dizer que, não protege ou defende os direitos fundamentais, pelo contrário, o RGPD é uma peça central na proteção dos direitos fundamentais das pessoas no que diz respeito ao tratamento dos seus dados[38]. Isto porque, o Regulamento foi concebido precisamente para assegurar que o tratamento de dados pessoais respeite e proteja os direitos fundamentais dos indivíduos, em particular o direito à privacidade e à proteção dos dados pessoais[39].

Posto isto, consideramos como os dois propósitos do RGPD, a defesa pelos direitos e liberdades fundamentais das pessoas singulares, com especial atenção ao direito à proteção de dados e o seu tratamento devido, previsto e regulado no seu artigo 1.º n.º 2 e, a promoção da livre circulação dos dados pessoais na União Europeia, por meio de um Mercado Único, com tratamento uniforme em todos os seus Estados-Membros, artigo 1.º n.º 3[40].

---

[37] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 33, do ponto de vista dogmático do RGPD, considera que "O RGPD não nasceu para acautelar os interesses individuais dos titulares dos dados – esses seriam sempre protegidos através da invocação de normas gerais relativas aos direitos de personalidade – mas sim para regular o seu tratamento".

[38] Aliás, o Considerando (1) do RGPD diz que "A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental".

[39] Artigo 1.º n.º 1 e 2 do RGPD, "1. "O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados 2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.".

[40] Considerando (2) do RGPD, "Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo

Assim sendo, CORDEIRO, Menezes (2020)[41] define o RGPD como "um conjunto sistematizado de princípios, normas e institutos que regula os dados pessoais das pessoas singulares e o seu tratamento". Esta última parte revela-se essencial na compreensão e aplicação do Regulamento, uma vez que este, trata exclusivamente a proteção de dados pessoais de pessoas singulares, ou seja, dos indivíduos, pelo que não se aplica, diretamente, aos dados das pessoas coletivas.[42]

O RGPD implementa diretrizes para o processamento de dados pessoais, impondo às entidades responsáveis: transparência, consentimento, segurança e responsabilidade no tratamento de dados pessoais. Assim, o objetivo do RGPD e de iniciativas semelhantes, passa por equilibrar a necessidade legítima das entidades de recolher e utilizar dados pessoais para diversos fins com o direito fundamental à privacidade e à proteção dos seus dados pessoais. Estas medidas visam proporcionar maior segurança jurídica e promover a confiança dos cidadãos na economia digital, ao mesmo tempo que preserva o respeito pelos direitos individuais.

## 2.3. A aplicação direta do RGPD

Antes da entrada em vigor do RGPD, que veio revogar a Diretiva n.º 95/46/CE, cada país da UE era autónomo na regulamentação do tratamento dos dados pessoais e, por isso, existiam várias leis próprias de proteção de dados. Esta autonomia refletiu-se em grandes divergências legislativas no que toca à aplicação da matéria da proteção de dados, comprometendo por isso, o Mercado Único Digital[43].

É importante percebermos que, a revogação da Diretiva n.º 95/46/CE, foi um passo importante neste sentido[44]. A adoção de um Regulamento em vez de uma nova

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 singulares."

[41] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 35.

[42] No Considerando (14) do RGPD, pode ler-se "A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais. O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva.

[43] Ver Ponto 2.2.

[44] É importante consolidar a ideia de que o RGPD não veio substituir os ideais implementados pela Diretiva, veio sim, colmatar a divisão entre os Estados-Membros na aplicação da matéria da proteção de dados e, consolidar a ideia de um Mercado Único, tal como se pode ler no Considerando (9) do RGPD: "Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação

Diretiva deve-se ao facto de que, as diretivas, por sua natureza, são instrumentos legislativos que estabelecem objetivos que os Estados-Membros devem prosseguir e alcançar, permitindo, no entanto, que cada país escolha a forma e os meios para praticar e implementar esses objetivos[45]. Tal facto, resultou numa fragmentação significativa dos Estados-Membros, ao adotar mecanismos distintos na aplicação desta matéria que, contribuía, eficazmente, para o retrocesso do Mercado Único.

Por sua vez, a implementação do RGPD, teve por isso mesmo, como um dos principais objetivos colmatar estas barreiras e zelar por harmonização legislativa das normas relativas à proteção de dados já existentes, em todos os Estados-Membros. Isto porque, nos termos do artigo 288.º do TFUE, os regulamentos têm carater geral, sendo por isso, obrigatoriamente aplicáveis de igual forma em todos os Estados-Membros[46]. Ou seja, o RGPD contribuiu ferozmente para o funcionamento pleno e eficaz do Mercado Único ao estabelecer um conjunto uniforme de regras para a urgência da proteção de dados pessoais em toda a UE.

A responsabilidade em garantir a conformidade entre todos os países da União Europeia no âmbito da aplicação do disposto deste Regulamento e, salvaguardar o Direito Comunitário, recai sobre os tribunais nacionais[47], sendo por isso, inadmissível que, um Estado-Membro aplique de forma incompleta ou em sentido diverso as disposições adotadas no Regulamento.[48].

---

da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE.".

[45] Artigo 288.º do TFUE, pode ler-se "Para exercerem as competências da União, as instituições adotam regulamentos, diretivas, decisões, recomendações e pareceres. (…) A diretiva vincula o Estado-Membro destinatário quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios.".

[46] Artigo 288.º do TFUE, pode ler-se "O regulamento tem caráter geral. É obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros."

[47] Ac. do TJUE, de 20/09/2001, n.º de processo C-453/99, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:61999CJ0453, pode ler-se "(…) como resulta de jurisprudência constante, aos tribunais nacionais encarregados de aplicar, no quadro das suas competências, as disposições do direito comunitário cabe garantir a plena eficácia destas normas e proteger os direitos que as mesmas conferem aos particulares (…)".

[48] Ac. do TJUE de 07/02/1973, n.º de processo 39/72 (Comissão Itália), https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A1973%3A13, pode ler-se "É, pois, inadmissível que um Estado-membro aplique de forma incompleta ou seletiva as disposições de um

Concluímos assim que a aplicação direta do RGPD desempenha um papel vital no fortalecimento do Mercado Único Europeu, promovendo a harmonização legislativa, enquanto cria condições equitativas para a competitividade. Ao garantir que a proteção de dados pessoais é uniforme em toda a UE, o RGPD não só protege os direitos dos cidadãos, mas também apoia o crescimento económico e a inovação dentro do Mercado Único.

## 2.4. O impacto do RGPD

A entrada em vigor e a subsequente aplicação do RGPD, transformou o modo como as entidades públicas ou privadas tratam os dados pessoais. Podemos considerar que este Regulamento assenta em três pilares que visam garantir uma proteção mais eficaz dos dados pessoais, bem como, promover a transparência, a confiança e a responsabilidade no seu tratamento, sendo eles: novas obrigações e responsabilidades para as empresas/entidades, na medida em que o RGPD, impõe às empresas que tratam dados pessoais uma série de obrigações e responsabilidades mais robustas em relação à sua recolha, armazenamento, tratamento e proteção desses dados, como por exemplo, a exigência do consentimento explícito[49] por parte do utilizador para o uso dos seus dados; novos direitos para os titulares dos dados, o Regulamento vem fortalecer os direitos dos cidadãos neste âmbito, concedendo a faculdade de acesso aos seus dados pessoais, o direito de os corrigir, o direito de ver os seus dados apagados (direito ao esquecimento) e o direito à portabilidade dos dados, isto é, de os transferir de uma entidade para outra;[50] e ainda, novos poderes para as autoridades nacionais de proteção de dados, - no âmbito do ordenamento jurídico português, falamos da CNPD, que previamente se preparou para a entrada em vigor do RGPD[51], passando a partir de então, a ter poderes para supervisionar

regulamento comunitário, de modo a prejudicar a aplicação de certos elementos da legislação comunitária a respeito dos quais tenha manifestado a sua oposição ou que julgue contrários a certos interesses nacionais.".

[49] Considerando (32) do RGPD, "O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. (…)"

[50] Ver Capítulo IV.

[51] COMISSÃO NACIONAL DA PROPETÇÃO DE DADOS (CNPD), *O que somos e quem somos*, acedido e consultado em 14/08/2024, disponível em https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/, pode ler-se, "A Comissão Nacional de Proteção de Dados (CNPD) é uma entidade administrativa independente, com personalidade jurídica de direito público e com poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República. A CNPD controla e fiscaliza o cumprimento do RGPD, da Lei 58/2019, da Lei 59/2019 e da Lei 41/2004, bem como

e fazer cumprir o Regulamento, bem como aplicar multas aquando do não cumprimento e ainda investigar eventuais queixas dos utilizadores.

Assim, pode ler-se no Considerando (2), que um dos objetivos da implementação do RGPD passa por "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 singulares".

Contudo, há a salientar que o tratamento de dados pessoais não é um direito absoluto[52] e deve ser equilibrado com outros interesses legítimos da sociedade bem como os restantes direitos fundamentais, mediante o critério da proporcionalidade. Quer isto dizer que, as restrições do tratamento de dados devem ser proporcionais ao objetivo pretendido e não devem ir além do necessário para atingir o seu fim.

O conceito de proteção de dados pessoais, que anteriormente não era tido como imperativo, passou a ser, no contexto jurídico-legal, uma questão primordial merecendo especial atenção. Tal decorre, em parte, de uma crescente consciencialização pública sobre a importância da privacidade e da segurança dos dados pessoais, consequente do RGPD, que trouxe consigo, o surgimento de outros novos conceitos como "violação de dados pessoais"[53] e "limitação do tratamento"[54].

das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos dos seus dados pessoais.".

[52] Considerando (4) do RGPD, "O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdades e e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística."

[53] Artigo 4.º n.º 12 do RGPD, pode ler-se "«Violação de dados pessoais», uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;"

[54] Artigo 4.º n.º 3 do RGPD, pode ler-se "«Limitação do tratamento», a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro;".

# CAPÍTULO III – DADOS PESSOAIS

## 3.1. O conceito de dados pessoais

O artigo 4.º n.º 1 do RGPD define dados pessoais como "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)"[55], mais à frente, é esclarecido que "é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador".

Este é um conceito bem estruturado não só no contexto europeu, mas também no contexto internacional[56], que se subdivide em quatro elementos distintivos: i) qualquer informação; ii) relativa; iii) pessoa singular; e iv) identificada ou identificável[57].

A parte final do mesmo artigo esclarece que "é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular". Quer isto dizer que, uma pessoa é considerada identificada quando uma informação específica permite reconhecê-la diretamente, sem necessidade de cruzamento com outros dados e, identificável[58] quando certas informações não permitem a identificação direta de uma pessoa, mas, quando combinadas com outros dados, identificam, embora indiretamente, alguém[59].

---

[55] Esta é a mesma definição de "dados pessoais" que constava na Diretiva n.º 95/46/CE no artigo 2.º al. a), comprovando que, os preceitos elencados na Diretiva permanecem válidos, conforme disposto no Considerando (9);

[56] No mesmo sentido, a OCDE, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*, 23 de setembro de 1980, define dados pessoais com as exatas palavras utilizadas pelo legislador europeu: *"personal data" means any information relating to an identified or identifiable individual (data subject)".*

[57] Estes preceitos devem ser analisados em detalhe em conformidade com o disposto no Parecer n.º 4/2007 do Grupo de Trabalho de Proteção de Dados do Artigo 29.º, sobre o conceito de dados pessoais, de 20/06/2007, pág. 6 e ss.

[58] Considerando (26) do RGPD, "Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica.".

[59] É importante salientar que, a Lei n.º 58/2019 no artigo 17.º, *a contrario sensu* do disposto no RGPD, refere que os dados pessoais das pessoas falecidas integram a categoria de dados pessoais.

Francisco, D., & Francisco, S. (2019)[60], entendem que "o teste decisivo para decidir se são dados pessoais para o RGPD ou não, consiste em avaliar se esses dados podem ser usados direta ou indiretamente para identificar uma pessoa. Enquanto o nome de uma pessoa identifica obviamente a mesma, a verdade é que algumas combinações de identificadores indiretos também permitem essa identificação".

De facto, qualquer informação, relativa à nossa pessoa pode se enquadrar no conceito de "dados pessoais", independentemente da sua natureza. Existem informações que, desde logo, são identificáveis, como é o caso do nome, idade, número de identificação do cartão de cidadão, morada, endereços eletrónicos, estado civil, situação patrimonial, profissão, características físicas e mentais. Por outro lado, existem outras informações que, ligadas num todo, podem igualmente incluir-se neste conceito, como é o caso de considerações íntimas como a religião ou posição política, dados genéticos, biométricos e informações relativas à saúde[61], origem racial e ética e ainda, a orientação sexual[62].

Para o efeito, estas informações só são "dados pessoais" quando "relativas a uma pessoa singular, identificada ou identificável", desde logo porque, a proteção conferida pelo RGPD apenas inclui pessoas singulares[63]. Pelo que, o RGPD aplica-se a todas as situações em que estas informações possam constar, como é o caso de imagens relativas a pessoas, recolhidas através dos sistemas de videovigilância[64], a gravação de chamadas telefónicas, os endereços de IP[65], os dados de tráfego e dados de localização recolhidos no âmbito das comunicações eletrónicas e ainda a informação relativa à localização de determinadas pessoas (por exemplo através de sistemas de geolocalização) também constituem dados pessoais.

Importa referir ainda que, os dados pseudonimizados são também dados pessoais nos termos do artigo 4.º n.º 5 do RGPD, por pseudonimizados, entende-se "o tratamento

---

[60] FRANCISCO, Daniel, & Francisco, Sandra, *Regulamento Geral de Proteção de Dados: 7 passos para uma metodologia de implementação do RGPD na Administração Pública*, Edições Sílabo, Lisboa, 2019, pág. 29.

[61] Artigo 4.º n.º 13, 14 e 15 do RGPD;

[62] Artigo 9.º do RGPD.

[63] Considerando (14) do RGPD.

[64] Artigo 19.º n.º 1 da Lei nº 58/2019, 8 de agosto, a par do GT 29, *Parecere 4/2007*, pág. 8, "*Images of individuals captured by a video surveillance system can be personal data to the extent that the individuals are recognizable".*

[65] Ac. do TJUE, de 19/10/2016, n.º de processo C-582/14, disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62014CJ0582, sustenta a ideia de que o IP é um dado pessoal de uma pessoa identificável.

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", fazem parte da proteção conferida pelo RGPD.[66]

## 3.2. Dados sensíveis

Embora o RGPD não apresente uma definição exata para "dados sensíveis" ou especiais [67], ao longo do Regulamento percebemos uma clara distinção deste conceito, em relação aos demais dados pessoais, desde logo pelo seu tratamento.

Como estudamos no ponto anterior, dados pessoais dizem respeito qualquer informação que possa identificar direta ou indiretamente alguém e que, geralmente, a sua divulgação geralmente não traz consequências graves para os titulares dos dados. Por outro lado, os dados sensíveis dizem respeito a informações, como o próprio nome indica, de caráter sensível, o que significa que requerem de um nível de proteção muito mais rigoroso, já que, do ponto de vista dos direitos e liberdades fundamentais, implicam sérios riscos para os seus titulares,[68] podendo gerar vulnerabilidade, discriminação ou provocar algum dano na esfera jurídica do indivíduo.

---

[66] Artigo 4.º n.º 5 do RGPD.

[67] O RGPD adota a expressão "dados especiais", tendo ambos o mesmo significado, tal como consta no Considerando (10), "(…) O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»)".

[68] Podemos ler no Considerando (51), "Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em

Importa referir que a categorização de dados pessoais especiais não é nova, a Convenção n.º 108, já estudada, dedicava o artigo 6.º a estes dados, bem como a revogada Diretiva n.º 95/46/CE, no artigo 8.º.

Assim, ainda que não haja uma definição exata deste conceito no RGPD, este apresenta três categorias de dados especiais, sendo elas os dados genéticos[69], dados biométricos[70] e dados relativos à saúde[71]. Neste sentido, no artigo 9.º[72], estão elencados, taxativamente, os dados que, para todos os efeitos são considerados especiais: i) os tratamentos que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou a filiação sindical; ii) os tratamentos de dados genéticos, dados biométricos para identificarem uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa[73].

Por assim ser, o tratamento de dados sensíveis é, em regra, proibido. Contudo, o tratamento destes dados é autorizado em situações muito específicas: quando tiver sido dado o consentimento pelo titular dos dados para o tratamento desses mesmos dados; quando o tratamento se revele indispensável para o cumprimento de obrigações em matéria de legislação laboral, segurança social e de proteção social; caso o tratamento seja necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, estando o titular impedido de fornecer o seu consentimento; quando o tratamento for realizado por uma associação, fundação ou outro organismo sem fins lucrativos, sendo esse tratamento referente a membros ou ex-membros dessas instituições; por motivos de interesse público importante, nomeadamente, no domínio da saúde pública; caso o

conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais.".

[69] Artigo 4.º n.º 13 do RGPD, "«Dados genéticos», os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa;"

[70] Artigo 4.º n.º 14 do RGPD, "«Dados biométricos», dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;"

[71] Artigo 4.º n.º 15 do RGPD, "«Dados relativos à saúde», dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde;".

[72] Importa referir que o disposto neste artigo difere dos preceitos da Convenção n.º 108 e da Diretiva n.º 95/46/CE, o que mostra, desde logo, a urgência de fazer face à evolução histórica e tecnológica.

[73] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 133.

tratamento seja indispensável para efeitos de medicina do trabalho; e finalmente, para efeitos de arquivo de interesse público ou investigação científica, nos termos do artigo 9.º n.º 1 e 2.

Além do artigo 9.º, o RGPD apresenta um conjunto variado de preceitos com um campo de aplicação material circunscrito a esta categoria de dados pessoais especiais, como o artigo 6.º n.º 4 – licitude do tratamento e das cláusulas de abertura, o artigo 22.º n.º 4 – decisões individuais automatizadas, artigo 35.º n.º 3 – avaliação de impacto sobre a proteção de dados e, artigo 37.º n.º 1 al. c) – designação do encarregado dados.[74]

A presente dissertação tende a estudar, com especial detalhe, os dados relativos à saúde, pelo que, torna-se necessário compreender melhor a proteção especial conferida pelo legislador europeu a este tipo de dados.

Ora, por dados de saúde devemos entender "e todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro" o que inclui "qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro", Considerando (35) a par com o disposto no artigo 4.º n.º 15.

A saúde de uma pessoa é uma parte fundamental da sua privacidade. A exposição de informações sobre a sua condição médica, tratamentos, diagnósticos ou qualquer outro dado médico, tem um caráter profundamente pessoal. E, portanto, é crucial que cada indivíduo tenha o controlo sobre quem pode, ou não, ter acesso a essas informações e em que contexto, sendo por isso, exigível uma especial atenção e proteção nesse sentido.

[74] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 135.

## 3.3. O tratamento de dados pessoais

O artigo 4.º n.º 2 do RGPD, apresenta-nos o conceito basilar do tratamento de dados pessoais, sendo este "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;".[75]

Por tratamento automatizado, devemos entender qualquer operação ou conjunto de operações realizadas no âmbito dos dados pessoais de forma automatizada, ou seja, sem intervenção humana direta.[76]

Não podemos deixar de referir que, assim como vimos no Ponto anterior, o tratamento de dados pessoais sensíveis é, em regra, proibido, salvo as exceções previstas no n.º 2 do artigo 9.º.[77]

Assim sendo, o tratamento de dados pessoais está intimamente relacionado com os princípios previstos no artigo 5.º do RGPD, que orientam a forma como os dados pessoais devem ser tratados. Estes princípios estabelecem diretrizes que asseguram que o tratamento de dados seja efetuado de forma responsável, lícita e em conformidade com os direitos dos titulares dos dados, que estudaremos com mais detalhe a seguir.

### 3.3.1. Princípios relativos ao tratamento de dados pessoais

#### *3.3.1.1. Princípio da licitude*

O artigo 5.º n.º 1 al. a) do RGPD diz que os dados pessoais são "objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados". O n.º 2 do artigo 8.º da Carta refere ainda que os dados pessoais são "objeto de um tratamento legal, para fins

[75] Nos termos do artigo 2.º n.º 1 do RGPD, "O presente regulamento não se aplica ao tratamento de dados pessoais: a)Efetuado no exercício de atividades não sujeitas à aplicação do direito da União: b)Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; c)Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; d)Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.".

[76] Tomamos como exemplo as *cookies* - pequenos arquivos de texto que os *sites* armazenam no dispositivo dos usuários enquanto navegam na *internet.*

[77] Ver Ponto 3.3.3.

específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei."

Mais acrescenta o Considerando (40) que "para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar.".

Quer isto dizer que, o consentimento[78], constitui uma base sólida e imperativa para a licitude do tratamento dos dados pessoais, uma vez que, constitui uma causa para a licitude nos termos do artigo 6.º n.º 1 al. a).

Fazer cumprir com o princípio da licitude exige um esforço por parte das entidades responsáveis pelo tratamento dos dados em fundamentar legalmente o seu tratamento com base nas disposições legais previstas no Regulamento. Para além disso, é igualmente exigível que, o tratamento seja devidamente comunicado ao titular dos dados, de forma clara e transparente, garantindo, principalmente, que o mesmo dá o seu consentimento[79] voluntário para os devidos efeitos, sob pena de violação do Regulamento nos termos do artigo 83.º n.º 5.

Mais se acrescenta, que o tratamento de dados só é lícito quando respeitar a uma das alíneas previstas no artigo 6.º n.º 1 do RGPD, isto é, nas situações em que "a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma

[78] Estudaremos ao detalhe a importância do consentimento no âmbito do tratamento dos dados pessoais no Ponto 3.3.2.

[79] O titular dos dados tem a possibilidade de retirar o seu consentimento ou retificar os dados para os quais deu consentimento a qualquer momento, tal como resulta do artigo 7.º n.º 3 do RGPD, "O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar" a par com o disposto no artigo 13.º n.º 2 al. c), artigo 14.º n.º 2 al. d) e ainda na parte final do artigo 8.º n.º 2 da Carta "(…) Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.".

obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica".

#### *3.3.1.2. Princípio da lealdade*

O artigo 5.º n.º 1 al. a) elenca três dos princípios pelos quais o tratamento de dados pessoais se deve fazer reger, uma vez que estão intimamente ligados, sendo um deles a lealdade.

Fazer cumprir com este princípio exige das entidades um compromisso constante com a ética e a transparência[80], na medida em que, estabelece que o tratamento dos dados deve seguir a sua finalidade, isto é, deve ser de acordo com o fim a que se destinam e não outro, de forma a respeitar os valores éticos da sua recolha. Isto traduz-se num voto de confiança por parte dos titulares dos dados que, tomam controlo e conhecimento do processo de tratamento dos seus dados.

Neste sentido, vem o Considerando (39) dizer que "O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados". E, por isso, as entidades responsáveis pelo

[80] O artigo 40.º n.º 2 al. a) diz que o tratamento de dados pessoais deve ser um "tratamento equitativo e transparente".

tratamento dos dados estão obrigadas a informar os titulares de todas as finalidades a que a recolha se destina[81], devendo para o efeito, zelar sempre pelos direitos dos titulares.[82]

Para tal, diz o artigo 13.º n.º 2 que as entidades responsáveis devem fornecer certas e determinadas informações para o pleno cumprimento deste princípio, como por exemplo, "a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo; b)A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados; c) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea a), ou no artigo 9.º, n.º 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado; d) O direito de apresentar reclamação a uma autoridade de controlo; e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados; f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.".

[81] Considerando (60) do RGPD pode ler-se "O responsável pelo tratamento deverá fornecer ao titular as informações adicionais necessárias para assegurar um tratamento equitativo e transparente tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados. O titular dos dados deverá também ser informado da definição de perfis e das consequências que daí advêm. Sempre que os dados pessoais forem recolhidos junto do titular dos dados, este deverá ser também informado da eventual obrigatoriedade de fornecer os dados pessoais e das consequências de não os facultar. Essas informações podem ser fornecidas em combinação com ícones normalizados a fim de dar, de modo facilmente visível, inteligível e claramente legível um útil perspetivo geral do tratamento previsto. Se forem apresentados por via eletrónica, os ícones deverão ser de leitura automática.".

[82] Considerando (47) do RGPD "(…) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento.".

### *3.3.1.3. Princípio da transparência*

O princípio da transparência encontra-se, desde logo, presente no primeiro contacto entre a entidade responsável pela recolha dos dados pessoais e o titular dos mesmos.

Este princípio assegura aos titulares dos dados, uma compreensão imediata e clara sobre como as suas informações serão recolhidas e usadas. Isto significa que as informações do tratamento de dados devem ser de fácil acesso e compreensão, elaboradas em linguagem simples e clara.

O Considerando (29) diz que o tratamento dos dados pessoais "deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados". Quer isto diz que, desde logo, deve haver uma preocupação por parte das entidades em transmitir, de forma transparente, sobre as finalidades a que se destinam os dados, bem como quais os mecanismos utilizados para o seu tratamento e o tempo de conservação[83]. Ou seja, o titular dos dados deve abraçar o dever de informação[84] a que está sujeito, de forma a estar plenamente consciente de todo o processo e os devidos riscos[85], para que, para os devidos efeitos, se encontre capaz de dar o seu consentimento.

Assim, este princípio defende que o titular dos dados deve ser capaz de determinar, antecipadamente, o âmbito e as consequências do tratamento dos dados, e não deve ser surpreendido posteriormente sobre as formas como os seus dados pessoais foram utilizados.[86] Como tal, as entidades estão obrigadas a fornecer certas e determinadas informações, que constam dos artigos 13.º, 14.º[87] do RGPD.

---

[83] Considerando (39) do RGPD "(…) Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados.".

[84] Estudaremos o dever de informação no Capítulo IV.

[85] Considerando (39) do RGPD ". As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento".

[86] GT 29, *Orientações relativas à transparência na aceção do Regulamento 2016/679 (WP260rev.1), 29 de novembro de 2017.*

[87] Ver artigos 34.º e 37.º do RGPD.

Mais se acrescenta que, o princípio da transparência não se esgota no exercício do direito à informação dos titulares dos dados pessoais, ou seja, há um claro apelo à participação ativa dos titulares no processo de tratamento dos dados, para que, se inteirem plenamente dos seus efeitos.[88]

#### *1.3.1.1 Princípio da limitação das finalidades*

O artigo 5.º n.º 1 al. b) dita que os dados pessoais devem ser "recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»)".[89]

Aquilo que aqui se pretende é assegurar que os dados recolhidos sejam tratados apenas para os fins originalmente especificados, sem que ocorra qualquer processamento posterior ou incompatível com tais finalidades. Isto reflete-se no dever de informar os titulares sobre as finalidades a que os dados pessoais se propõem, condenando a sua utilização indevida, isto é, para outro propósito que não aquele que foi previamente consentido[90].

Neste sentido, as finalidades pretendidas com a recolha dos dados pessoais, devem desde logo ser limitadas, antes do processo sequer se iniciar. Para o efeito, todas as questões inerentes ao tratamento dos dados e as finalidades a que se destinam, devem ser comunicadas ao titular dos dados, de forma transparente e claro e, portanto, ficar esclarecidas à priori.

Excetuam-se, obviamente, os casos em que as entidades processam os dados pessoais para fazer cumprir obrigações legais específicas[91], mesmo que esses propósitos não tenham sido inicialmente consentidos pelo titular. O que quer dizer que, é possível

---

[88] GT 29, *Orientações relativas à transparência na aceção do Regulamento 2016/679 (WP260rev.1), 29 de novembro de 2017.*

[89] No mesmo sentido, vem o artigo 8.º n.º 2 da Carta, quando utiliza a expressão "(…) para fins específicos (…)".

[90] Considerando (50) do RGPD, pode ler-se "o tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos.".

[91] Nomeadamente para fins de interesse público, investigação científica ou histórica, e fins estatísticos, que constam no Considerando (50).

que os dados pessoais sejam utilizados para finalidades diferentes daquelas para as quais foram inicialmente recolhidos, desde que as novas finalidades sejam compatíveis com as finalidades originais.[92]

#### *3.3.1.4. Princípio da minimização dos dados*

O princípio da minimização dos dados, previsto no artigo 5.º n.º 1 al. c), diz que os dados pessoais devem ser "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados".[93]

Por adequados, o legislador pretende transmitir a ideia de que os dados pessoais devem ser apropriados para a finalidade pretendida. Isto significa que devem ter uma relação direta e clara com o objetivo específico do tratamento.

Além disso, devem também ser pertinentes, o que significa que só devem ser objeto de recolha e posterior tratamento, os dados que se considerem necessários para alcançar a finalidade a que se destinam, em caso contrário, não devem ser recolhidos.

Por fim, devem ser limitados ao necessário, isto é, o tratamento dos dados deve se cingir ao mínimo necessário para fazer cumprir a finalidade a que se propõe. Ou seja, não devem ser recolhidos ou tratados dados irrelevantes, e por isso, não necessários para a finalidade específica.

Mais se acrescenta que este princípio estipula que os dados pessoais só devem ser recolhidos e processados, no caso de não existirem outros meios alternativos ou razoáveis para atingir o fim a que se destinam.[94] Para além disso, apenas devem ser objeto de recolha, os dados que se revelem imprescindíveis ao fim, e não quaisquer outros[95].

#### *3.3.1.5. Princípio da exatidão*

Dita o artigo 5.º n.º 1 al. d) do RGPD, que os dados pessoais são "exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para

---

[92] Nos termos do Considerando (50).

[93] No mesmo sentido, vinha a revogada Diretiva n.º 95/46/CE quando usou a expressão "não excessivos" no Considerando (29) – o tratamento de "dados pessoais deve ser efetuado de forma lícita e leal para com a pessoa em causa; que deve, em especial, incidir sobre dados adequados, pertinentes e não excessivos em relação às finalidades prosseguidas com o tratamento.

[94] Tomamos com exemplo a anonimização, prevista no artigo 32.º n.º 1 e a pseudonomização, artigo 25.º n.º 1 do RGPD.

[95] Considerando (39) e (50) do RGPD.

que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora".

Este princípio ressalva a garantia que as entidades devem ter no que toca aos recursos imediatamente disponíveis para atender às solicitações de correção ou atualização de informações feitas pelo titular dos dados.

Assim pressupõem-se do disposto no artigo 5.º n.º 1 al. c) parte final que, a proibição das entidades em recolher dados incorretos e, como tal, têm o dever de atualização dos dados recolhidos sempre que se mostre necessário, bem como, o dever de apagar[96] ou retificá-los[97] quando não correspondam com a realidade.

#### *3.3.1.6. Princípio da conservação*

O princípio da limitação da conservação diz-nos que os dados pessoais devem ser "conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados", nos termos do artigo 5.º n.º 1 al. e) do RGPD.

Quer isto dizer que, existem parâmetros em relação à recolha dos dados por período limitado ao seu fim, ou seja, devem ser tratados até ao termo do período necessário para atingir a sua finalidade, salvo disposição legal em contrário[98]. Isto significa que após o término das finalidades a que os dados se propõem, estes devem ser eliminados ou anonimizados, a menos que haja alguma obrigação legal que exija a sua retenção por um período mais longo.

---

[96] Artigo 17.º n.º 1 do RGPD, "O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada".

[97] Artigo 16.º do RGPD, "O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.".

[98] Considerando (39) e (50) do RGPD.

#### *3.3.1.7. Princípio da integridade e confidencialidade*

Segundo o artigo 5.º n.º 1 al. f) do RGPD, os dados pessoais devem ser: "tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas".

As entidades e organizações devem garantir a proteção dos dados pessoais solicitados contra os acessos não autorizados, isto é, possíveis invasões aos seus sistemas informáticos ou, em alguns casos, roubo dos formatos em papel[99]. Para o efeito, devem ser aplicadas medidas de controlo quer ao acesso físico quer digital destas informações, como por exemplo, as *firewalls*[100] e a criptografia[101] – métodos que visam garantir a confidencialidade das informações.

#### *3.3.1.8. Princípio da responsabilidade*

O princípio da responsabilidade, de acordo com o artigo 5.º n.º 2 do RGPD, dita que "o responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo.".

O responsável pelo tratamento tem de fazer cumprir com os princípios elencados ao longo do n.º 1 do artigo 5.º, ao mesmo tempo que, se revela capaz de demonstrar às autoridades de controlo e tribunais[102], o cumprimento desses mesmos princípios. Quer isto dizer que, o princípio da responsabilidade, assenta no efetivo cumprimento das disposições legais previstas no RGPD, no âmbito do tratamento dos dados pessoais.

---

[99] Considerando (39) e (49) do RGPD.

[100] MAC FREE, *O que é uma firewalls?* acedido e consultado a 20/08/2024, disponível em https://www.mcafee.com/pt-pt/antivirus/firewall.html, pode ler-se "As *firewalls* são programas de software ou dispositivos de hardware que filtram e examinam as informações provenientes da ligação à Internet. Representam a primeira linha de defesa porque podem impedir que um programa malicioso ou atacante tenha acesso à rede e informações antes que qualquer potencial dano seja causado".

[101] HOSTINGER, *O que é a criptografia?*, acedido e consultado a 20/08/2024, disponível em https://www.hostinger.pt/tutoriais/o-que-e-criptografia?ppc_campaign=google_search_generic_hosting_all&bidkw=defaultkeyword&lo=20879&gad_source=1&gclid=CjwKCAiAopuvBhBCEiwAm8jaMVLCtH1Kyo4YXzPLO5u4Q07o3L5aDamLmORqbFwCK2Gc8zCSZoQqgxoCSMwQAvD_BwE, pode ler-se "A criptografia é um método que converte textos em códigos abstratos conhecidos como *ciphertexts* ou textos cifrados. O propósito da criptografia é ocultar dados sensíveis, impedindo que usuários não autorizados acedam e roubem as informações".

[102] Artigo 55.º n.º 1 do RGPD, "As autoridades de controlo são competentes para prosseguir as atribuições e exercer os poderes que lhes são conferidos pelo presente regulamento no território do seu próprio Estado-Membro".

O facto da primeira parte do artigo 5.º n.º 2 referir, claramente, que "o responsável pelo tratamento é o responsável pelo cumprimento", leva-nos a crer que lhe é vedada a possibilidade de delegar as suas responsabilidades a outrem. Contudo, importa referir que, podem delegar tarefas específicas no âmbito do tratamento de dados pessoais aos subcontratantes.[103]

Embora o Regulamento não seja claro na forma como o responsável comprova o cumprimento dos princípios do RGPD, o artigo 24.º diz que o responsável pelo tratamento dos dados deve adotar a aplicação de medidas adequadas com interesse na salvaguarda dos princípios já estudados,[104] como a adoção de códigos de conduta nos termos do artigo 40.º e 42.º Para o efeito, deve o responsável ou o subcontratante, efetuar um registo de todas as atividades de tratamento sob a sua responsabilidade, dos elementos contantes no artigo 30.º n.º 1. Em caso de violação dos dados pessoais, deve o responsável, comunicar às entidades de controlo, no prazo de 72 horas após o conhecimento da mesma.[105]

### 3.3.2. O consentimento

Lemos no artigo 4.º n.º 11 do RGPD, que no ato do fornecimento dos dados pessoais deve existir um consentimento por parte do seu titular, isto é, "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".

---

[103] O artigo 4.º n.º 7 do RGPD define responsável pelo tratamento como "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro", já o n.º 8 do presente artigo, define subcontratante, "uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes".

[104] Artigo 24.º n.º 1 "Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades".

[105] Artigo 33.º n.º 1 "Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso".

O RGPD estabelece como um princípio relevante e fundamento da legitimidade da recolha e tratamento de dados pessoais, o consentimento, devendo este ser "mediante declaração ou ato positivo inequívoco", tendo este que dizer respeito ao titular desses mesmos dados".[106] Tanto é que, este princípio encontra-se previsto no artigo 8.º n.º 2 da Carta e na legislação nacional no artigo 35.º da CRP.[107] Assim sendo, a força jurídica do consentimento é inequívoca no RGPD, sendo este uma das causas de licitude por se considerar indispensável ao tratamento dos dados, tal como resulta da al. a) do n.º 1 do artigo 6.º.

O artigo 7.º do Regulamento, dedica-se exclusivamente às condições exigíveis e aplicáveis ao consentimento. Diz-nos o n.º 1 do presente artigo que, "o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais", isto é, sempre que exigível, o responsável pela recolha dos dados pessoais, deve conseguir mostrar e provar o consentimento do titular a que os dados respeitam. O n.º 2 acrescenta ainda que "o consentimento dado em declaração escrita relativo a outros assuntos, deve ser apresentada de modo inteligível, fácil acesso e numa linguagem clara e simples". Adianta o n.º 3 que "o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento", o que obriga as entidades a removerem o consentimento do titular da mesma forma que foi concedido, isto é, deve ser de modo fácil, através do mesmo meio anteriormente utilizado: por correio eletrónico, via internet, entre outros. Mais se acrescenta que a retirada do consentimento não pode, em momento algum, comprometer a licitude do tratamento efetuado. Para além do mais, "ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato".

[106] Podemos ler no Considerando (32) do RGPD, "O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral.".

[107] Artigo 8.º n.º 2 da Carta diz que os dados só devem ser objeto de tratamento com "o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei", já o artigo 35.º, exige o consentimento do titular no n.º 2 quando diz "a informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular (…)".

Aqui revela-se também importante aludir o artigo 8.º, que se dedica às condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação, sendo este consentimento lícito apenas em maiores de 16 anos, caso contrário é exigível o consentimento pelos titulares das responsabilidades parentais. Há a acrescentar que os Estados-membros têm a faculdade de alterar a idade mínima para o efeito, "desde que essa idade não seja inferior a 13 anos"[108].

Assim, por consentimento entende-se, nos termos do artigo 4.º nº 11, i) uma manifestação de vontade, ii) livre, iii) específica, iv) informada e, v) inequívoca, sendo estes os elementos-chave para a prática deste conceito, que estaremos a seguir com mais detalhe.

#### *3.3.2.1. Manifestação da vontade*

A manifestação de vontade corresponde a um dos requisitos que compõe a figura do consentimento e, comporta dois elementos distintos conquanto interligados, i) a vontade humana e ii) a declaração dessa vontade, ou seja, a sua exteriorização.[109] A vontade humana demonstra, desde logo, a intenção do titular dos dados em realizar determinado ato. Trata-se de um processo mental e subjetivo no qual uma pessoa determina o que quer ou não quer fazer e, portanto, livre. No contexto do consentimento no RGPD, a vontade humana implica que o titular dos dados esteja realmente intencionado, de forma consciente e ponderada, a autorizar o tratamento dos seus dados pessoais, o que significa, à partida, que está plenamente consciente da decisão que está a tomar. Quando assim é, esta vontade deve ser manifestada através de uma ação clara e inequívoca, isto é, a vontade é exteriorizada de forma objetiva mediante um determinado ato ou comportamento que, traduz, efetivamente, a vontade interna do indivíduo. Assim, em matéria de consentimento e predisposições do RGPD, estamos perante uma manifestação da vontade dos titulares quando estes, através de um ato positivo ou não, demonstram a vontade interna de prestar o seu consentimento, ou a falta dele, para o tratamento dos seus dados pessoais. [110]

---

[108] Artigo 8.º n.º 1 do RGPD.

[109] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 172-173.

[110] O Parecer 15/2011 sobre a *definição de consentimento* (WP 187), pág. 13, refere que o consentimento e a respetiva manifestação da vontade estava anteriormente previsto na Diretiva n.º 95/46/CE e, que esta não refere uma forma específica para o exercício da manifestação da vontade

#### *3.3.2.2. Livre*

A manifestação da vontade dos titulares está, intimamente ligada ao controlo e autonomia sobre os seus dados pessoais. Por isso mesmo, é imperativo que a manifestação da vontade seja livre.[111] Por assim ser, a manifestação da vontade não será válida "se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado",[112] o que quer dizer que, nos casos em que a vontade do titular tenha sido condicionada por qualquer fator, independentemente da sua natureza, esta não é considerada válida, uma vez que, representa um condicionamento, embora ás vezes indireto, ao livre arbítrio por parte do titular dos dados, que o RGPD defende.[113]

Neste sentido, o artigo 7.º n.º 4 revela um papel importante já que avalia se o consentimento é dado livremente, e para o efeito "há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato", a par com o disposto no artigo 6.º n.º 1 al. b).

Assim, existem algumas situações que, desde logo, se determina que a manifestação da vontade não é livre, como é o caso do disposto no Considerando (43) que determina que a manifestação de vontade dos titulares não é livre se o processo para obter o consentimento não permitir ao titular, prestar o seu consentimento separadamente

---

esclarecendo que "A forma da manifestação (i.e. a forma como é manifestada a vontade) não é definida na diretiva. Por razões de flexibilidade, o consentimento «escrito» foi excluído do texto final. Deve sublinhar-se que a diretiva admite «qualquer» manifestação de vontade. Isto possibilita um entendimento alargado do âmbito de tal manifestação. A expressão mínima de uma manifestação poderia ser qualquer sinal, suficientemente claro, suscetível de manifestar a vontade da pessoa em causa e de ser entendido pelo responsável pelo tratamento. As palavras «manifestação» e «pela qual... aceita» apontam efetivamente na direção de ser necessário um ato (por oposição a uma situação em que o consentimento pudesse ser inferido de uma omissão).".

[111] Parecer 08/2024 sobre *Consentimento Válido no Contexto de Modelos de Consentimento ou Remuneração Implementados por Grandes Plataformas Online*, pág. 19, ponto 68, pode ler-se "*Controllers must ensure that data subjects have a real freedom of choice when asked to consent to processing of their personal data, and they may not limit data subjects' autonomy by making it harder to refuse rather than to consent . This is also supported by one of the main purposes of the GDPR, which is to provide data subjects with control over their personal data. For consent to be freely given, the data subjects must be able to determine themselves if the processing can take place, without inappropriate influence from the controller or others, and be provided with appropriate information about the processing".*

[112] Parte final do Considerando (42) e (43).

[113] No mesmo sentido, vem o Parecer 08/2024 sobre *Consentimento Válido no Contexto de Modelos de Consentimento ou Remuneração Implementados por Grandes Plataformas Online*, pág. 19, ponto 69 e 70.

para diferentes operações. No mesmo sentido, vem o Considerando (32) dizer que "o consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins".

#### *3.3.2.3. Específica*

O artigo 5.º n.º 1 al. b) diz que os dados pessoais devem ser recolhidos para finalidades determinadas e, como tal, "o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas"[114], nos termos do artigo 6.º n.º al. a).

Para que a manifestação da vontade seja específica, o titular dos dados deve estar devidamente informado sobre as finalidades a que os seus dados se destinam, o que quer dizer que, as entidades responsáveis devem delimitar bens as finalidades e passar essa informação aos titulares,[115] com vista na sua autonomia.

O GT 29[116] entende que, para que a manifestação da vontade do titular seja específica, o responsável pelo tratamento atuar em função da i) especificação em função da finalidade como salvaguarda contra o desvirtuamento da função, ii) da granularidade nos pedidos de consentimento e iii) da separação clara entre as informações relacionadas com a obtenção de consentimento para atividades de tratamento de dados e as informações sobre outras questões. Menezes Cordeiro (2020) acrescenta uma outra, sendo ela a iv) especificação dos dados a tratar.[117]

A especificação em função da finalidade refere-se à obrigação dos responsáveis pelo tratamento dos dados limitar claramente os propósitos para os quais os dados pessoais são recolhidos e, portanto, desde o momento da recolha, o titular dos dados deve ser informado sobre o motivo exato pelo qual os seus dados estão a ser tratados.[118] Assim

---

[114] No mesmo sentido do princípio da limitação das finalidades que estudamos no Ponto 3.3.1.4.

[115] No mesmo sentido, vem o Parecer 08/2024 sobre *Consentimento Válido no Contexto de Modelos de Consentimento ou Remuneração Implementados por Grandes Plataformas Online*, pág. 35, ponto 161.

[116] GT 29, *Orientações relativas ao consentimento na aceção do Regulamento (UE)*, 2016/679, WP259 rev.01, 28 de novembro de 2017, pág.13.

[117] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 181.

[118] Parecer 3/2013 do GT29 *sobre a limitação da finalidade* (WP 203), pág.16, no âmbito das finalidades específicas: "Por estas razões, uma finalidade que seja vaga ou geral, como por exemplo "melhorar a experiência dos utilizadores", "para fins de comercialização", "para fins de segurança das TI"

sendo, as finalidades devem ser claras e precisas, sem qualquer ambiguidade, estando impedidas de ser alteradas posteriormente sem um novo consentimento do titular.[119]

A granularidade nos pedidos de consentimento refere-se, na prática, ao ato de solicitar o consentimento dos titulares de dados de forma específica e segmentada, permitindo-lhes dar ou recusar consentimento para cada finalidade de tratamento de dados de forma individual e separada. Desta forma, os responsáveis não devem apresentar ao titular dos dados um único pedido de consentimento para várias atividades de tratamento diferentes ao mesmo tempo, deve ser dada a possibilidade ao titular de escolher, individualmente, quais os propósitos específicos que deseja autorizar o uso dos seus dados.

A separação clara implica que, ao solicitar o consentimento para o tratamento de dados pessoais, as informações relevantes devem ser apresentadas de forma distinta e, não misturadas com outras informações que não estejam diretamente relacionadas com o consentimento. Isto significa que os dados relativos ao consentimento devem ser claramente diferenciados de qualquer outra informação fornecida aos titulares.

Por fim, a especificação de dados a tratar refere-se à necessidade de identificar de forma clara e precisa quais os dados pessoais que serão recolhidos e utilizados pelo responsável pelo tratamento para fazer cumprir com determinadas finalidades devendo, para o efeito, fazer referência ao âmbito e aos riscos do consentimento, evitando assim, generalidades de forma a não suscitar dúvidas no ato de prestar o seu consentimento.[120]

ou "para investigação futura" geralmente, sem mais pormenores, não cumpre os critérios de ser "específica".

[119] Neste sentido, o Ac. do TJUE, de 05/05/2011, n.º de processo c-543/09, https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A62009CJ0543, Ponto 65, considera que apenas é necessário renovar o consentimento quando as finalidades a que, inicialmente, os dados pessoais se predispuseram, alterem. Em caso contrário, o consentimento pode ser automaticamente renovado, isto se, "se existir a garantia de que os dados em causa não serão utilizados para fins diferentes daqueles para os quais foram recolhidos com vista à sua primeira publicação".

[120] Parecer 15/2011 sobre a *definição de consentimento* (WP 187), pág. 19, diz que "Para ser específico, o consentimento deve ser inteligível: deve fazer referência, de forma clara e precisa, ao âmbito e consequências do tratamento de dados. Não pode aplicar-se a um conjunto aberto de atividades de tratamento. Significa isto, por outras palavras, que o consentimento se aplica a um contexto limitado.".

#### *3.3.2.4. Informada*

O RGPD prevê no seu artigo 5.º, o princípio da transparência [121] que, está intimamente ligado com a licitude do tratamento dos dados prevista no artigo 6.º que, por sua vez, diz respeito ao dever de informação por parte do responsável pelo tratamento dos dados ao seu titular.

Este é um preceito imprescindível para que a manifestação da vontade do titular dos dados e, consequentemente o seu consentimento sejam válidos e, portanto, para que o consentimento seja válido, é fundamental que os titulares dos dados sejam devidamente informados antes de prestarem o seu consentimento. No caso de o responsável pelo tratamento não fornecer as informações que considerem imprescindíveis e que possam influenciar no ato de prestar o consentimento, o controlo do utilizador torna-se ilusório e o consentimento será um fundamento inválido para o tratamento.[122]

O direito à informação é extremamente necessário para que, os titulares possam tomar decisões conscientes e informadas, de forma a compreender plenamente o que estão a aceitar. Por isso mesmo, o responsável pelo tratamento está obrigado a fornecer todas as informações que considere imprescindíveis, sob pena de consentimento inválido.[123]

Para o efeito, o GT 29 entende como requisitos mínimos para o consentimento informado as seguintes informações específicas, i) identidade do responsável pelo tratamento[124], ii) a finalidade de cada uma das operações de tratamento em relação às quais se procura obter o consentimento iii) que (tipo de) dados serão recolhidos e utilizados, iv) existência do direito de retirar o consentimento[125], v) informações acerca da utilização dos dados para decisões automatizadas em conformidade com o artigo 22.º n.º 2 al. c), quando pertinente, e vi) sobre os possíveis riscos de transferências de dados

[121] O Considerando (39) esclarece este princípio dizendo que "O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados.".

[122] GT 29, *Orientações relativas ao consentimento na aceção do Regulamento (UE)*, pág. 14.

[123] Parecer 08/2024 sobre *Consentimento Válido no Contexto de Modelos de Consentimento ou Remuneração Implementados por Grandes Plataformas Online*, pág. 32, ponto 142-143.

[124] No mesmo sentido, o Considerando (42) diz que para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina.

[125] Artigo 7.º n.º 4 do RGPD.

devido à inexistência de uma decisão de adequação e de garantias adequadas, tal como previsto no artigo 46.º.[126]

Enquanto isso, Menezes Cordeiro (2020) afasta-se da posição do GT 29, considerando que as informações a prestar ao titular dos dados no momento de prestar o seu consentimento passam por, i) os dados pessoais a serem objeto de tratamento, ii) a identidade do responsável pelo tratamento, iii) as finalidades a que o tratamento se destina, iv) os direitos dos titulares dos dados e, v) os riscos associados ao tratamento.[127]

O RGPD não é claro na forma como este tipo de informações devem ser apresentadas ao titular, o que quer dizer que, é possível apresentar informações válidas de várias maneiras, tais como declarações escritas ou orais, mensagens áudio ou vídeo.[128] Há, no entanto, que ter em atenção as considerações previstas no artigo 7.º n.º 2[129] e no Considerando (32).[130]

No ato do consentimento, os responsáveis pelo tratamento de dados devem assegurar que para além das informações importantes estarem disponíveis ao titular, estas devem ser prestadas numa linguagem clara e acessível para todos. Isto significa que, a mensagem que se pretende passar, deve ser compreensível para uma pessoa comum, sem recorrer a longos avisos de privacidade ou declarações repletas de terminologias jurídicas, o que dificulta, claramente, a sua compreensão. Assim sendo, o consentimento deve ser claro, específico, percetível e de fácil acesso, o que significa que as informações importantes devem estar, de imediato, disponíveis para consulta, para que o ato de consentimento seja tomado com base nestas informações, sob pena de não ser válido.

Mais se acrescenta que, os responsáveis pelo tratamento devem envidar esforços no sentido de, decorrido um certo período de tempo, rever as escolhas das pessoas,

---

[126] Artigo 49.º n.º 1 al. a) do RGPD.

[127] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 183.

[128] GT 29, *Orientações relativas ao consentimento na aceção do Regulamento (UE)*, pág. 15.

[129] Artigo 7.º n.º 2 diz que "Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento".

[130] Considerando (32) do RGPD, admite várias possibilidades na forma como estas informações devem ser transmitidas ao titular dos dados, quando diz que "O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral.".

designadamente informando-as da sua escolha atual e oferecendo a possibilidade de confirmação ou revogação.[131]

#### *3.3.2.5. Inequívoca*

A manifestação de vontade inequívoca, refere-se a uma manifestação de intenção ou desejo que é clara, direta e sem qualquer dúvida. Quando o titular dos dados expressa a sua vontade de forma inequívoca, significa que a intenção deste é expressa de forma tão clara que não deixa margem para interpretações ambíguas ou para diferentes entendimentos.

O artigo 4.º n.º 11 diz que o consentimento provém de uma declaração ou ato positivo inequívoco, já que este reflete a vontade clara do titular em permitir que os seus dados sejam recolhidos e tratados pelo responsável. Nos termos do Considerando (32), a vontade inequívoca pode ser expressa mediante declaração escrita, oral (gravada) e até em formato eletrónico. E, por isso mesmo, há a considerar que o silêncio ou a inatividade do titular dos dados não pode ser interpretada como uma manifestação da sua vontade porque, de facto, não traduz a vontade expressa do titular em consentir o tratamento dos seus dados. [132] Assim sendo, consideramos que não se reconhece como consentimento o silêncio, opções pré-selecionadas ou omissão de comportamento. [133]

### 3.3.3. Condições de licitude do tratamento de dados sensíveis

Dada a natureza especial dos dados sensíveis o legislador europeu dedicou o artigo 9.º do Regulamento ao "Tratamento de categorias especiais de dados pessoais". Esta categorização especial deve-se à natureza particularmente delicada destes dados que, incluem categorias que podem revelar aspetos muito pessoais e da esfera privada de um

[131] O artigo 7.º n.º 3 determina que "O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.", no mesmo sentido, vem o Parecer 15/2011 sobre a *definição de consentimento* (WP 187), pág. 22-23.

[132] GT 29, *Orientações relativas ao consentimento na aceção do Regulamento (UE)*, pág. 18, dá o seguinte exemplo, "Aquando da instalação de um programa informático, a aplicação solicita aos titulares dos dados consentimento para utilizar relatórios de falha não anonimizados para melhorar o programa informático. Uma declaração de confidencialidade estruturada com as informações necessárias acompanha o pedido de consentimento. Ao assinalar ativamente a opção que indica «Concordo», o utilizador pode realizar validamente um «ato positivo inequívoco» dando consentimento para o tratamento.".

[133] O GT 29, *Orientações relativas ao consentimento na aceção do Regulamento (UE)*, pág. 18, entende também que "A utilização de opções pré-assinaladas de adesão é inválida nos termos do RGPD".

indivíduo, como a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos e até dados relativos à saúde, vida sexual ou orientação sexual de uma pessoa. [134],

O artigo 9.º estabelece que, em regra geral, é proibido o tratamento de dados sensíveis, exceto em situações específicas e previstas na lei, sob as quais o tratamento é lícito e admitido com base nos fundamentos legais previstos no n.º 2, que estudaremos ao detalhe a seguir.

Do confronto entre o regime comum do tratamento dos dados previsto no artigo 6.º, e o regime dos dados sensíveis, no artigo 9.º, verifica-se, no essencial, um agravamento dos requisitos legais para o tratamento de dados pessoais desta natureza. Assim, a positivação de um regime próprio e diferenciado justifica-se pela sua natureza, dado que a maioria dos dados sensíveis se relaciona com os direitos fundamentais, o que significa que os riscos associados ao seu tratamento são maiores.[135]

#### *3.3.3.1. Consentimento*

O regime geral do consentimento, previsto no artigo 7.º n.º 4 e estudado no Ponto 3.3.2., é igualmente aplicável no tratamento de dados sensíveis, aquilo que se espera aqui, é uma atenção redobrada no cumprimento das exigências previstas ao longo do Regulamento.

Isto significa que, a principal diferença entre o regime comum e o regime dos dados sensíveis assenta na exigência, que na prática, se traduz num nome requisito, a explicitude, isto é, um consentimento mais rigoroso do que aquele que é exigido no regime comum.[136]

E, portanto, representa uma exceção à proibição do tratamento de dados sensíveis "se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.º 1 não pode ser anulada pelo titular dos dados", artigo 9.º n.º 2 al. a).

---

[134] Ver Ponto 3.2. do presente Capítulo.

[135] CORDEIRO, A. Barreto Menezes, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019,* Almedina, Coimbra, 2021, pág. 136.

[136] CORDEIRO, A. Barreto Menezes, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019,* Almedina, Coimbra, 2021, pág. 136.

### *3.3.3.2. Obrigações laborais*

A alínea b) do n.º 2 do artigo 9.º prevê o tratamento de dados pessoais sensíveis, nos casos em que estes sejam necessários para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, com remissão para o artigo 6.º n.º 1 al. b).

Contudo, a aplicação prática do disposto acima, depende do preenchimento cumulativo dos seguintes elementos, i) existência de suporte legal bastante, ii) existência de uma relação direta entre o tratamento e o cumprimento das obrigações ou o exercício do direito[137], de forma a fazer cumprir com o princípio da minimização dos dados.[138]

Tomamos como exemplo, as justificações de falta por motivos de saúde, bem como atestados médicos e baixas médicas, estes documentos contêm informações de caráter extremamente privado e sensível, pelo que, só poderão ser disponibilizados ao abrigo do disposto na al. b) do n.º 2 do artigo 9.º.

### *3.3.3.3. Interesses vitais*

Nos termos da al. c) do n.º 2 do artigo 9.º, o tratamento de dados é lícito "se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento", o mesmo resulta do regime comum do tratamento de dados, previsto no artigo 6.º n.º 1 al. d).[139]

O conceito de "interesses vitais" refere-se a situações em que a vida ou a integridade física quer do titular dos dados ou de terceiros está em risco iminente. Nestas circunstâncias, como em emergências médicas, o responsável pelo tratamento dos dados,

---

[137] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 242.

[138] Ver ponto 3.3.1.5. do presente Capítulo, no mesmo sentido, CORDEIRO, A. Barreto Menezes, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, pág. 137, diz que "O tratamento também só pode ser descrito como necessário se não existir uma alternativa menos intrusiva do direito à autodeterminação informacional do titular dos dados".

[139] O regime comum do tratamento de dados pessoais, a propósito da licitude, considera igualmente os interesse vitais do titular ou de terceiros como fundamento legal para o seu tratamento, nos termos do artigo 6.º n.º 1 al. d), "O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular".

no caso uma instituição hospitalar (ou outra instituição do meio), pode agir sem obter o consentimento prévio do titular. O tratamento de dados nestes casos, é justificado pela necessidade de proteger a vida ou prevenir danos graves na saúde do titular, priorizando a sua segurança e bem-estar em detrimento da obtenção imediata do consentimento. Importa referir que, esta base legal tem um limite muito excecional, sendo apenas possível "no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento".[140]

Importa também ressalvar que na existência de eventuais representantes legais do titular, estes devem estar presentes para suprir a falta de consentimento.[141]

Neste contexto, a proteção dos interesses vitais atua como um mecanismo essencial para assegurar que os dados pessoais possam ser tratados de forma rápida e eficaz em situações críticas, garantindo que a resposta a uma emergência não seja atrasada por questões burocráticas. É uma salvaguarda importante que equilibra a necessidade de proteger a vida e a integridade física com a preservação dos direitos de privacidade do indivíduo.

#### *3.3.3.4. Fundações e associações*

Representa igualmente um fundamento legal para o tratamento de dados sensíveis, "se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares", nos termos do artigo 9.º n.º 2 al. d).

[140] Por exemplo, quando um indivíduo sofre um acidente e se vê incapacitado ou inconsciente, a necessitar urgentemente de cuidados médicos, os profissionais de saúde devem atuar de imediato para preservar a sua vida e saúde. Nestas situações, é crucial que os profissionais acedam aos seus dados pessoais, como dados de identificação ou histórico clínico, sem se preocuparem, em primeiro lugar, em obter o consentimento do paciente/titular dos dados. A prioridade aqui é garantir que o tratamento necessário é prestado sem demora, assegurando a melhor resposta possível à emergência e salvaguardando a vida do indivíduo.

[141] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 243.

Quer isto dizer que, o tratamento destes dados é lícito se forem recolhidos por fundações ou associações sem fins lucrativos,[142] se estas tiverem por objeto a política, a filosofia ou a religião, como são exemplo os sindicatos.[143]

Para o efeito, o tratamento dos dados deve ser realizado no âmbito das suas atividades legítimas, devendo dizer a membros, antigos membros ou pessoas em contacto regular com a organização em conexão com os seus objetivos e, por essa razão, não podem ser divulgados a terceiros sem o consentimento dos titulares.

#### *3.3.3.5. Dados tornados públicos pelo próprio titular*

Assim como resulta da al. e) artigo 9.º n.º 2, o tratamento de dados sensíveis é admissível "se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular".

Quando o titular dos dados decide tornar públicos os seus dados sensíveis, entende-se que há um consentimento implícito para o seu tratamento e que renuncia à proteção conferida pelo artigo 9.º n.º 1 do RGPD. Mesmo que os dados sejam públicos, a as entidades que os tratarem devem fazê-lo em conformidade com uma finalidade específica e legítima. O tratamento não pode exceder o que seria razoavelmente esperado pelo titular dos dados.

Embora estes dados sejam tornados públicos de forma livre e consciente pelo próprio titular, se estes forem objeto de tratamento, não se prescinde do dever de informação do titular, este deve ser igualmente informado sobre as finalidades e o propósito do seu tratamento. Por exemplo, se um indivíduo partilhar nas redes sociais informações sobre o seu estado de saúde, essas informações são consideradas como tendo sido tornadas públicas pelo próprio titular, no entanto, uma entidade que queira tratar esses dados para qualquer fim, como uma investigação ou campanha de saúde, deve garantir que o tratamento é justificado, proporcional e que respeita os direitos do titular.

[142] Sem fins lucrativos devemos entender, sem fins comerciais.

[143] A Liga Portuguesa Contra o Cancro (LPCC) é um exemplo de uma organização sem fins lucrativos, que tem como principal objetivo apoiar a luta contra o cancro em Portugal, promovendo a prevenção, o diagnóstico precoce, o tratamento e a reabilitação dos doentes oncológicos. Neste âmbito, a organização pode tratar os dados de saúde dos seus doentes para oferecer apoio ou desenvolver programas de investigação, garantindo sempre o cumprimento das normas de proteção de dados, tendo em vista a melhoria da qualidade de vida dos doentes com cancro e dos seus respetivos familiares.

#### *3.3.3.6. Processo judicial*

É igualmente lícito "se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional", artigo 9.º n.º 2 al. f).

O tratamento de dados sensíveis deve ser estritamente necessário para o propósito de exercer ou defender os direitos do titular no âmbito judicial. Este princípio aplica-se aos litígios de natureza civil, criminal, administrativa ou arbitral, independentemente do tribunal. Além disso, este preceito estende-se a processos extrajudiciais, de forma a assegurar que a proteção de dados seja sempre proporcional e justificada pelo propósito específico de salvaguardar os direitos em causa.[144]

Isto significa que a finalidade do tratamento deve estar claramente ligada ao processo judicial em questão, ou seja, os dados sensíveis devem ser tratados exclusivamente para fins diretamente relacionados com o processo a decorrer.

#### *3.3.3.7. Interesses públicos*

Diz-nos a alínea g) do artigo 9.º n.º 2 que "se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados", é admissível o tratamento deste tipo de dados.

Este preceito encontra o seu paralelo no regime comum previsto no artigo 6.º n.º 1 al. e), quando o legislador permite que os dados pessoais sejam tratados nestas circunstâncias, quando diz que se "o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento" é lícito. Tal implica que a sua finalidade deva ser fixada nesta base legal, ou seja, ser necessária para o desempenho de uma missão de interesse

[144] Tomamos o seguinte exemplo, num caso de litígio laboral em que um trabalhador alega discriminação com base na sua condição de saúde ou orientação sexual, os dados sensíveis sobre a saúde ou orientação sexual podem ser tratadas como parte do processo em tribunal a fim de estabelecer ou contestar as alegações. Estes dados serão tratados dentro dos limites do processo judicial e utilizados exclusivamente para a defesa ou reivindicação dos direitos envolvidos.

público ou para o exercício de funções na qualidade de autoridade pública por parte do responsável pelo tratamento dos dados.

#### *3.3.3.8. Cuidados de saúde*

"Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 32", o tratamento é lícito, nos termos do artigo 9.º n.º 2 al. h).

As categorias especiais de dados pessoais, como os dados de saúde, que requerem proteção rigorosa, só devem ser tratados para fins relacionados com a saúde quando sejam necessários para o bem das pessoas e da sociedade, como por exemplo para a gestão de serviços de saúde ou ação social, monitorização de sistemas de saúde, ou investigação científica e estatística.[145] Podemos retomar o exemplo dado no Ponto 3.3.3.4., da Liga Portuguesa Contra o Cancro.

Mais se acrescenta que este tipo de dados apenas pode ser alvo de tratamento no caso de o responsável por essa função, estar sujeito a sigilo profissional, garantindo que

[145] Considerando (52) do RGPD diz que "As categorias especiais de dados pessoais que merecem uma proteção mais elevada só deverão ser objeto de tratamento para fins relacionados com a saúde quando tal for necessário para atingir os objetivos no interesse das pessoas singulares e da sociedade no seu todo, nomeadamente no contexto da gestão dos serviços e sistemas de saúde ou de ação social, incluindo o tratamento por parte da administração e das autoridades sanitárias centrais nacionais desses dados para efeitos de controlo da qualidade, informação de gestão e supervisão geral a nível nacional e local do sistema de saúde ou de ação social, assegurando a continuidade dos cuidados de saúde ou de ação social e da prestação de cuidados de saúde transfronteiras, ou para fins de segurança, monitorização e alerta em matéria de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos baseados no direito da União ou dos Estados-Membros e que têm de cumprir um objetivo, assim como para os estudos realizados no interesse público no domínio da saúde pública. Por conseguinte, o presente regulamento deverá estabelecer condições harmonizadas para o tratamento de categorias especiais de dados pessoais relativos à saúde, tendo em conta necessidades específicas, designadamente quando o tratamento desses dados for efetuado para determinadas finalidades ligadas à saúde por pessoas sujeitas a uma obrigação legal de sigilo profissional. O direito da União ou dos Estados-Membros deverá prever medidas específicas e adequadas com vista à defesa dos direitos fundamentais e dos dados pessoais das pessoas singulares. Os Estados-Membros deverão ser autorizados a manter ou introduzir outras condições, incluindo limitações, no que diz respeito ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde. Tal não deverá, no entanto, impedir a livre circulação de dados pessoais na União, quando essas condições se aplicam ao tratamento transfronteiriço desses dados.".

as informações dos pacientes são protegidas contra acessos não autorizados e usadas apenas para os fins pretendidos.[146]

#### *3.3.3.9. Saúde pública*

O artigo 9.º n.º 2 al. i) admite a admissibilidade de tratamento "se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional".

O Regulamento (CE) n.º 1338/2008 [147], define saúde pública como "todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade"

Durante a pandemia COVID-19, surgiu uma necessidade urgente em tratar os dados pessoais relativos à saúde da população para fins muito específicos, como o rastreamento de contactos entre os infetados, a gestão dos cuidados de saúde, a monitorização da propagação do vírus e a implementação de medidas de saúde pública em resposta à crise no setor de saúde à escala mundial. Neste contexto, o tratamento de dados pessoais sensíveis, como informações sobre o estado de saúde, sintomas, resultados dos testes e vacinação, tornaram-se essenciais. Estes dados foram partilhados à escala global, sem o consentimento dos seus titulares,[148] com o objetivo de sensibilizar e alertar

[146] Artigo 9.º n.º 3, "Os dados pessoais referidos no n.º 1 podem ser tratados para os fins referidos no n.º 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes".

[147] REGULAMENTO (CE) n.º 1338/2008 DO PARLAMENTO EUROPEU E DO CONSELHO de 16 de dezembro de 2008, *relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho.*

[148] O Considerando (54) refere que, em sítios específicas, o consentimento não se revela imperativo quando estão em causa bens maiores, como a saúde pública: "O tratamento de categorias especiais de dados

a população aos riscos iminentes, priorizando o interesse público, nomeadamente a saúde pública, sobre a privacidade individual dos dados. Foi necessário encontrar um equilíbrio entre a proteção da privacidade e a urgência de combater uma ameaça à saúde pública.[149]

O princípio aqui subjacente é de que, em situações de grande risco para a sociedade, a privacidade dos dados pessoais não deve ser um obstáculo à proteção de interesses maiores, como a saúde pública. Assim, em circunstâncias excecionais, a salvaguarda do bem-estar comum pode justificar o tratamento de dados pessoais de cariz sensível sem o consentimento dos seus titulares, desde que sejam adotadas as devidas medidas de proteção e segurança.

Mais se acrescenta que nos termos do artigo 9.º n.º 4, "os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde", constituindo assim uma cláusula de abertura aos Estados-Membros para regulamentarem o tratamento destes dados. [150] No contexto do ordenamento jurídico português, destacamos o artigo 29.º da Lei n.º 58/2019, que prevê exatamente o tratamento de dados de saúde e dados genéticos.

### *3.3.3.10. Arquivo, investigação científica ou histórica e fins estatísticos*

Por fim, o Regulamento dispõe do seu artigo 9.º n.º 2 al. j) que o tratamento de dados sensíveis não é proibido "se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados".

pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados".

[149] Considerando (53), "As categorias especiais de dados pessoais que merecem uma proteção mais elevada só deverão ser objeto de tratamento para fins relacionados com a saúde quando tal for necessário para atingir os objetivos no interesse das pessoas singulares e da sociedade no seu todo (…)".

[150] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 252.

# CAPÍTULO IV – OS DIREITOS DO TITULAR DOS DADOS PESSOAIS

O Regulamento Geral da Proteção de Dados Pessoais (RGPD) fortaleceu os poderes de controlo, o que se converteu numa maior proteção jurídica aos direitos dos titulares dos dados pessoais. O RGPD não apresenta uma definição exata para titular dos dados, no entanto, relembremos o disposto no artigo 4.º n.º 1 que faz referência a esta figura quando esclarece o que são dados pessoais, sendo eles toda a "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)".

Nos termos do artigo 3.º, será titular dos dados, todo aquele que, independentemente da sua nacionalidade ou residência, cujos dados sejam objeto de tratamento efetuado no âmbito de atividades desenvolvidas pelo estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União Europeia, artigo 3.º n.º 1 e, todos os residentes no espaço da União cujos dados pessoais sejam objeto de tratamento, artigo 3.º n.º 2.[151]

Embora o consentimento[152] seja crucial e imprescindível ao tratamento de dados, como estudamos no Capítulo anterior, com a entrada em vigor do RGPD, foram adquiridas outras limitações e direitos com vista a consumar os objetivos do Regulamento. Assim, na esfera jurídica dos titulares passam a ser reconhecidos direitos como: o direito de acesso[153]; direito à retificação,[154] direito ao apagamento,[155] direito à limitação do tratamento,[156] direito de portabilidade[157] e o direito de oposição[158].

## 4.1. Direito de Acesso

Antes de demais, é indispensável apreciar o artigo 17.º da CRP, que pressupõe uma categorização dos direitos fundamentais, nomeadamente os direitos, liberdades e garantias e os direitos económicos, sociais e culturais, elencados no título II e título III da

[151] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 255.
[152] Ver Ponto 3.3.2. do presente Capítulo.
[153] Artigo 15.º do RGPD.
[154] Artigo 16.º do RGPD.
[155] Artigo 17.º do RGPD.
[156] Artigo 18.º do RGPD.
[157] Artigo 20.º do RGPD.
[158] Artigo 21.º do RGPD.

parte I da CRP, respetivamente. Para Gomes Canotilho e Vital Moreira (2010)[159], "o objeto deste preceito é a definição do âmbito de aplicação do regime próprio dos direitos, liberdades e garantias", cuja distinção não se afigura fácil.

Embora o direito de acesso aos documentos administrativos – artigo 268.º da CRP, não se encontre inserido no título II da parte I do diploma e, portanto, disperso no decorrer do mesmo, é abrangido pela categoria "direitos, liberdades e garantias". Por outras palavras, isto significa que este direito se encontra ao abrigo do disposto no artigo 17.º da CRP, ou seja, caracteriza-se como um direito fundamental de natureza análoga, o que, em termos práticos, se traduz na beneficiação do mesmo regime que os direitos, liberdades e garantias. Para Gomes Canotilho e Vital Moreira (2010), não é fácil "determinar o critério de identificação dos direitos fundamentais de natureza análoga à dos direitos, liberdades e garantias", na prática, o que importa é o "objeto do direito em causa", para que através da Constituição seja possível a sua materialização.

E, portanto, o direito de acesso aos documentos administrativos, artigo 268.º, é um direito fundamental de natureza análoga e, por essa razão, universal.

É também de realçar que, o direito de acesso constitui um princípio base do Estado de Direito Democrático em que vivemos, uma vez que, o acesso a documentos administrativos pressupõe uma participação democrática dos cidadãos, a chamada "democracia participativa", assim como se pode ler no artigo 2.º, artigo 9.º al. c) e artigo 267.º n.º 1 e 5 da CRP.

O artigo 268.º da CRP enumera dois direitos no seu n.º 1 e 2, que Jorge Miranda e Rui Medeiros (2010)[160], consideram como direitos de natureza análoga, sendo eles o "direito dos administrados à informação" (artigo 268.º nº1) e, ainda, o "direito de acesso aos arquivos e registos administrativos" (artigo 268.º n.º 2). Assim entendemos que neste artigo estão presentes dois direitos distintos, no n.º 1 o direito fundamental e universal de acesso a documentos administrativos e, no n.º 2 o direito procedimental, na medida em que o cidadão tem o direito de aceder a toda e qualquer informação decorrente de um determinado procedimento.

---

[159] CANOTILHO, Gomes José & MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, 4.ª Edição, Vol. I, Coimbra, Coimbra Editora 2010, pág. 371.

[160] MIRANDA, Jorge & MEDEIROS, Rui, *Constituição Portuguesa Anotada* - Tomo I, 2ª Edição, Coimbra Editora, Coimbra, 2010.

### 4.1.1. O princípio da administração aberta

O princípio da administração aberta encontra-se previsto ao longo de várias normas legislativas, nomeadamente na Constituição da República Portuguesa (CRP), no Código do Procedimento Administrativo (CPA) e na Lei n.º 26/2016, mais conhecida como LADA[161], o que faz de si um princípio composto.[162]

Assim, entendemos que o princípio da administração aberta é um dos princípios que deve pautar a atividade administrativa, funcionando como um mecanismo de controlo da Administração Pública, que se pretende aberta, clara, transparente e acessível.

Como já referido, o artigo 268.º da CRP salvaguarda o direito de acesso a documentos administrativos que faz referência ao princípio da administração aberta no seu n.º 2, embora não o mencione expressamente com essa designação.

Este artigo estabelece que os cidadãos têm o direito de aceder aos arquivos e registos administrativos, o que significa que podem consultar documentos que estão guardados ou circulam em qualquer centro ou local da Administração Pública, onde esses documentos estejam armazenados.[163] O direito de acesso aqui presente é amplo e independente de qualquer processo administrativo em andamento, ou seja, os cidadãos não precisam de estar envolvidos, quer direta ou indiretamente, num procedimento específico para solicitar o seu acesso. Tal facto distingue-se do direito à informação, previsto no artigo 82.º do CPA, que é mais restrito, já que se aplica apenas às pessoas que são diretamente interessadas num procedimento administrativo em curso, isto é, só nesta condição é que podem ter acesso a certos documentos.[164]. E, portanto, o artigo 268.º n.º 2, incorpora os princípios da transparência, acesso à informação, participação cívica e responsabilidade, que são componentes essenciais do princípio da administração aberta.[165]

---

[161] Lei de Acesso aos Documentos Administrativos.

[162] No sentido em que, por porvir de um conteúdo normativo de origens temporais distintas e de fontes legislativas diversas.

[163] MIRANDA, Jorge e MEDEIROS, Rui, *Constituição Portuguesa Anotada*, Tomo III 1ª edição, Coimbra Editora, 2007, pág. 602.

[164] Artigo 82.º n.º 1 do CPA, pode ler-se "Os interessados têm o direito de ser informados pelo responsável pela direção do procedimento, sempre que o requeiram, sobre o andamento dos procedimentos que lhes digam diretamente respeito, bem como o direito de conhecer as resoluções definitivas que sobre eles forem tomadas".

[165] Ac. do Supremo Tribunal Administrativo, de 17/01/2008, n.º de processo 0896/07, https://www.dgsi.pt/jsta.nsf/35fbbbf22e1bb1e680256f8e003ea931/7a11a8ad079aebc9802573de00374730?OpenDocument, a propósito do princípio da administração aberta subentendido no artigo 268.º da CRP, refere que "o nº 2 do art.º 268º da CRP impõe que a Administração paute a sua atividade pelos princípios

O artigo 17.º n.º 1 do CPA densifica o princípio da administração aberta, sendo mais claro na sua definição e, por isso, este princípio determina que "todas as pessoas têm o direito de acesso aos arquivos e registos administrativos, mesmo quando nenhum procedimento que lhes diga diretamente respeito esteja em curso, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal, ao sigilo fiscal e à privacidade das pessoas". O que quer dizer que, as entidades públicas só podem negar o acesso a documentos quando estejam em causa direitos absolutos, naturalmente legal ou constitucionalmente protegidos.[166]

Mais recentemente, a Lei n.º 26/2016, 22 de agosto, que aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos, também conhecida como "a nova LADA", doravante designado por LADA, [167] dedica o seu artigo 2.º a este princípio, num sentido distinto ao disposto no artigo 17.º do CPA. Enquanto o artigo 17.º reproduz de modo quase idêntico o teor do n.º 2 do artigo 268.º da Constituição, o artigo 2.º da Lei n.º 26/2016 segue um caminho distinto, preocupando-se em determinar condições da divulgação e do acesso à informação da Administração Pública.[168] Para o efeito, o legislador procurou relacionar o princípio da administração aberta com os demais princípios da atividade administrativa, como vemos no artigo 2.º n.º 1 quando diz que "o acesso e a reutilização da informação administrativa são assegurados de acordo com os demais princípios da atividade

---

da transparência e da publicidade de modo a que não só as suas decisões sejam públicas e acessíveis, mas também que o procedimento que as precede possa ser objeto de consulta e informação pois que só assim se promove a formação de uma opinião pública esclarecida e só assim se permite que os interessados conheçam as razões que determinaram os seus atos".

[166] No mesmo sentido, vem o Ac. n.º 2594/99 do Tribunal Constitucional, n.º de processo 456/97, relator Cons. Sousa e Brito, https://www.tribunalconstitucional.pt/tc/acordaos/19990254.html, quando diz que "O direito de acesso do interessado nunca pode ser menor do que o do cidadão em geral, até porque o interesse público na transparência da atividade administrativa ou numa "administração aberta", como forma de garantia do respeito pelos princípios constitucionais, norteadores dessa atividade, da igualdade, da proporcionalidade, da justiça, da imparcialidade e da boa-fé, só pode ser favorecido pela ação dos diretamente interessados e está na prática dependente dessa ação. (…)".

[167] A entrada em vigor da "nova LADA", resultou na revogação de duas leis, a Lei n.º 46/2007, 24 de agosto – a antiga LADA e, a Lei n.º 19/2006 – Lei de Acesso à informação ambiental, LAIA. Assim, a nova LADA teve como propósito de compilar o objeto dos diplomas revogados num só e, portanto, esta lei regula o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos. A nova LADA sustentou-se em três principais objetivos: agrupar toda a matéria de acesso à informação administrativa num só diploma; estimular a facilidade de acesso a este tipo de informação, disponibilizando-a online; erradicar qualquer dúvida ou conflito anteriormente gerados entre a LADA, a LPD e a Lei n.º 12/2005, 26 de janeiro, à cerca da sua competência e constitucionalidade, como anteriormente discutido.

[168] FREITAS, Tiago & ALVES, Pedro Delgado, *O Acesso à Informação Administrativa*, Almedina, Coimbra, 2021, pág. 8.

administrativa, designadamente os princípios da igualdade, da proporcionalidade, da justiça, da imparcialidade e da colaboração com os particulares", e não menos importante, o princípio da transparência que consta no n.º 2.

Neste sentido, Tiago Freitas e Pedro Alves (2010), identificam como os sentidos normativos atuais do princípio da administração aberta, i) o direito dos particulares a acederem de forma fácil e expedita à informação administrativa e o correspondente dever da Administração em facultá-la, e ii) o dever da Administração de publicitar os termos da sua organização, funcionamento e atividade junto do maior número de particulares, sempre que tais informações sejam necessárias para assegurar a transparência administrativa.

Para a concretização do primeiro sentido normativo, o legislador, pela primeira vez, deu uma definição exata ao conceito de documentos administrativos, sendo estes "qualquer conteúdo, ou parte desse conteúdo, que esteja na posse ou seja detida em nome dos órgãos e entidades referidas no artigo seguinte, seja o suporte de informação sob forma escrita, visual, sonora, eletrónica ou outra forma material, neles se incluindo, designadamente, aqueles relativos a: i) Procedimentos de emissão de atos e regulamentos administrativos; ii) Procedimentos de contratação pública, incluindo os contratos celebrados; iii) Gestão orçamental e financeira dos órgãos e entidades; iv) Gestão de recursos humanos, nomeadamente os dos procedimentos de recrutamento, avaliação, exercício do poder disciplinar e quaisquer modificações das respetivas relações jurídicas", artigo 3.º n.º 1 al. a). No sentido de assegurar o acesso a documentos administrativos e a proteção dos dados pessoais surgiu a criação da Comissão de Acesso aos Documentos Administrativos (CADA), uma entidade pública independente cujo objetivo passa, essencialmente, por assegurar o cumprimento das disposições legais no que toca ao acesso à informação administrativa.[169] E, em situações que o justificam, os tribunais desempenham, naturalmente, um papel igualmente importante na salvaguarda do direito de acesso aos documentos administrativos.

Para entendermos a consumação do segundo sentido normativo, importa-nos regressar ao princípio da transparência, presente no n.º 2 do artigo 2.º da LADA que determina que "a informação pública relevante para garantir a transparência da atividade administrativa, designadamente a relacionada com o funcionamento e controlo da

[169] Artigo 28.º e ss da LADA.

atividade pública, é divulgada ativamente, de forma periódica e atualizada, pelos respetivos órgãos e entidades". O legislador não é muito específico quando se refere a "informação pública relevante", podendo por isso, gerar algumas incertezas e ambiguidades na prática do princípio da administração aberta e na aplicabilidade do princípio da transparência, contudo, diz-nos o n.º 3 do mesmo artigo que "na divulgação de informação e na disponibilização de informação para reutilização através da Internet deve assegurar-se a sua compreensibilidade, o acesso livre e universal, bem como a acessibilidade, a interoperabilidade, a qualidade, a integridade e a autenticidade dos dados publicados e ainda a sua identificação e localização". Não obstante, o princípio da transparência é vital para a implementação efetiva da administração aberta, já que assegura que as atividades da Administração Pública sejam conduzidas de maneira aberta e acessível, promovendo uma gestão pública mais democrática, responsável e participativa.

### 4.1.2. Direito de acesso aos documentos administrativos

O direito de acesso, conforme definido no artigo 15.º do RGPD, confere aos indivíduos o poder de solicitar e receber informações sobre a forma como os seus dados pessoais estão a ser tratados, qual o tratamento aplicado e se este será o mais adequado e lícito.[170]

A essência do direito de acesso assenta na faculdade conferida aos titulares dos dados em saber se as suas informações pessoais estão a ser processadas, para que fins, quais as categorias de dados, quem são os destinatários desses dados e por quanto tempo estes serão armazenados. O direito de acesso assume um papel fundamental no exercício dos demais direitos dos titulares dos dados pessoais, até porque, se estes não conhecerem quais os dados que são objeto de tratamento, naturalmente que se vêm impedidos de fazer prevalecer os restantes direitos que estudaremos ao longo do presente Capítulo.[171]

[170] No mesmo sentido vem o artigo 8.º n.º 2 da Carta, salvaguardar o direito de acesso, "Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação".

[171] A este propósito, destacamos o Ac. do TJUE, de 07/05/2009, n.º de processo C-553/07, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62007CJ0553, "Esse direito de acesso é necessário para que uma pessoa em causa possa exercer os direitos consagrados nas alíneas b) e c) do artigo 12.º da diretiva, ou seja, quando o tratamento dos seus dados não respeite o disposto nessa diretiva, o de obter que o responsável pelo tratamento os retifique, apague ou bloqueio [alínea b)] ou que notifique a terceiros a quem os dados tenham sido comunicados essas retificações, apagamentos ou bloqueios, desde que essa notificação não seja impossível ou não implique um esforço desproporcionado [alínea c)]. Esse

O considerando (63) do RGPD dita que, sempre que solicitado, os titulares devem, sem dificuldade, ter a possibilidade de acesso aos seus dados. Este acesso deve ser de forma ponderada, espaçada no tempo, e com o objetivo de tomar conhecimento e apurar a validade do tratamento em causa.[172] Aqui inclui-se o direito de acesso aos "dados sobre a sua saúde, por exemplo os dados dos registos médicos com informações como diagnósticos, resultados de exames, avaliações dos médicos e quaisquer intervenções ou tratamentos realizados"[173]. A solicitação destas informações é feita através de um envio de um pedido de informação ao responsável pelo tratamento dos dados que, sempre que possível e sem demora[174], após verificar a identidade do titular, não deve recusar o seu acesso[175], apesar de que, nas situações em que o responsável detenha uma grande quantidade de dados objeto de tratamento respeitante ao titular, deve, antes de fornecer as informações solicitadas, pedir ao titular que especifique quais as informações que pretende ter conhecimento direto.[176]

A este propósito, entendemos que há aqui um outro direito subjacente, o direito à informação, implícito nos artigos 12.º, 13.º e 14.º do RGPD, que assentam essencialmente no princípio da transparência. Como já mencionado, o titular dos dados deve ter acesso às seguintes informações, i) finalidades a que os dados se propõem, artigo 13.º n.º 1 al. c) e 14.º n.º 1 al. c), ii) categorias dos dados pessoais em questão, artigo 13.º n.º 1 al. d) e 14.º n.º 1 al. d); iii) destinatários, artigo 13.º n.º 1 al. e), 14.º n.º 1 al. e) e 15.º n.º 1 al. c),

---

direito de acesso também é necessário para que uma pessoa em causa possa exercer o direito de oposição ao tratamento dos seus dados pessoais, a que se refere o artigo 14.º da diretiva, ou o direito de recurso quando sofra um prejuízo, previsto nos seus artigos 22.º e 23.º".

[172] Considerando (63) do RGPD pode ler-se "cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências" sem que isso prejudique "os direitos ou as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software".

[173] Fazemos referência aos dados de saúde, por se revelarem de grande importância ao estudo da presente dissertação, especialmente, ao estudo de caso do Capítulo V.

[174] No prazo de 10 dias, nos termos do artigo 15.º da LADA.

[175] Em caso de recusa e, consequentemente, ato de indeferimento, o responsável deve informar por escrito, o titular dos dados, sobre quais as razões de fundamento à recusa do direito de acesso, nos termos do artigo 15.º al. c) da LADA.

[176] Considerando (63) do RGPD, "Quando possível, o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais. (…) Todavia, essas considerações não deverão resultar na recusa de prestação de todas as informações ao titular dos dados. Quando o responsável proceder ao tratamento de grande quantidade de informação relativa ao titular dos dados, deverá poder solicitar que, antes de a informação ser fornecida, o titular especifique a que informações ou a que atividades de tratamento se refere o seu pedido".

iv) prazo e critérios de conservação, artigo 13.º n.º 2 al. a) e 14.º n.º 1 al. a), v) quais os direitos dos titulares, artigo 13.º n.º 2 al. c) e e) e 14.º n.º 2 al. c) e e), vi) origem dos dados, artigo 14..º e 15.º n.º 1 al. g). Importa ainda referir que o direito à informação se materializa por diversos meios de que são exemplos a consulta do processo, a reprodução ou declaração autenticada de documentos, a prestação de indicações sobre a sua existência e conteúdo e a emissão de certidões.

Menezes Cordeiro (2021)[177] considera alguns outros direitos aqui implícitos, sendo eles o direito à confirmação, isto é, o titular dos dados tem o direito de saber se os seus dados pessoais estão, ou não, a ser tratados pelo responsável, ainda que, o tratamento já se tenha findado e os seus dados tenham sido anonimizados e, ainda o direito de obter cópia dos dados, nos termos do artigo 15.º n.º 3 e 4.[178]

Aqui chegados, entramos na problemática do acesso à informação de saúde. O direito de acesso não compromete a confidencialidade e privacidade dos dados pessoais de saúde?[179]

De facto, pode parecer contraditório que o direito de acesso aos dados pessoais, incluindo os de saúde, não comprometa a confidencialidade e privacidade destes dados no seu exercício do princípio da administração aberta. No entanto, o RGPD, foi projetado para equilibrar os direitos dos indivíduos com a necessidade legítima das entidades processarem os seus dados pessoais, incluindo os dados de saúde, de forma a fornecer serviços de saúde mais adequados e personalizados, bem como para outros fins legítimos.[180]

Antes de mais, importa recordarmos o conceito de dados pessoais que se encontra previsto no artigo 4.º n.º 1 do RGPD, e nos artigos 35.º e 26.º da CRP. Para a consumação deste conceito, a LADA encontrou uma nova designação quando a eles se refere, falamos de "documento nominativo", previsto no artigo 3.º n.º 1 al. b) do presente diploma, sendo

---

[177] CORDEIRO, A. Barreto Menezes, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Almedina, Coimbra, 2021, pág. 175 - 178.

[178] Artigo 15.º n.º 3 e 4 do RGPD, "3. O responsável pelo tratamento fornece uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente. 4. O direito de obter uma cópia a que se refere o n.º 3 não prejudica os direitos e as liberdades de terceiros".

[179] Importa recordarmos o conceito de dados pessoais previsto no artigo 4.º n.º 1 do RGPD, bem como no artigo 35.º e 26.º da CRP, para o efeito, voltar ao Capítulo III.

[180] O Considerando (63) do RGPD refere exatamente isto, que os titulares têm direito de acesso aos dados de saúde.

este um "documento que contenha dados pessoais, na aceção do regime jurídico de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados".

Como estudado no ponto anterior, o artigo 2.º da LADA salvaguarda o princípio da administração aberta que se concretiza no artigo 5.º, cujo dita que "sem necessidade de enunciar qualquer interesse, o direito de acesso aos documentos administrativos, o qual compreende os direitos de consulta, de reprodução e de informação sobre a sua existência e conteúdo", o que demonstra, claramente, um conflito entre o direito de acesso e a proteção de dados, que aos olhos de Alexandre Pinheiro (2015) [181] é uma colisão natural entre o princípio da administração aberta e a proteção de dados pessoais.

O artigo 6.º da LADA apresenta as exceções ao exercício deste direito fundamental, o direito de acesso, dentro das quais, a proibição de acesso de terceiros a documentos nominativos, sem que este atue mediante um interesse direto, pessoal, legítimo e constitucionalmente protegido ou, então, sem que haja consentimento prévio do titular, nos termos do seu n.º 5. [182] Quer isto dizer que, sempre que um documento contenha informação relativa a uma pessoa singular identificada ou identificável, como vimos na análise do artigo 4.º n.º 1 do RGPD, o seu acesso é, em regra, proibido.

Foi esta a solução que o legislador da LADA encontrou para colmatar o conflito normativo entre o direito de acesso à informação administrativa e a proteção de dados pessoais, dentro dos quais, se incluem os dados de saúde, que se caracterizam como dados especiais ou sensíveis.

Assim, os dados pessoais de saúde só podem ser divulgados a terceiros em circunstâncias específicas e legalmente permitidas, como por exemplo, nos casos em que se verifique o consentimento explícito do titular dos dados ou quando exigido por lei.

[181] PINHEIRO, Alexandre Sousa, *Privacy e proteção de dados pessoais,* AAFDL Editora, 2015, páh.273.

[182] Importa aludir ao n.º 8 do artigo 6.º, cujo dita que "os documentos administrativos sujeitos a restrições de acesso são objeto de comunicação parcial sempre que seja possível expurgar a informação relativa à matéria reservada".

#### *4.1.2.1. Acesso ao processo clínico*

Até há pouco tempo, o processo clínico [183] era encarado como propriedade exclusiva das instituições de saúde ou dos próprios médicos, apoiando-se na sua natureza altamente técnica e científica, bem como no caráter pessoal das anotações dos médicos. No entanto, temos vindo a assistir a uma profunda reforma nesse sentido e à escala mundial.

Durante muitos anos, a maioria das ordens jurídicas previa o acesso ao processo clínico através do sistema de acesso indireto, isto é, mediante um médico com habilitação própria e escolhido para o efeito. O acesso indireto era previsto e regulado pela anterior Lei de Proteção dos Dados Pessoais[184], no artigo 11.º n.º 5[185] e, na Lei da Informação Genética Pessoal e Informação de Saúde, no artigo 3.º n.º 3. O que não deixa de ser um pouco contraditório, tendo em conta que esta última Lei, refere no n.º 1 do mesmo artigo, que as informações de saúde e os dados clínicos registados são propriedade da pessoa a que pertencem, servindo as instituições de saúde como meros depositários de informação, ao mesmo tempo que se conserva na ideologia de um acesso indireto, isto é, não feito através do próprio titular.

E foi neste sentido que, a partir de 2007 com a entrada em vigor da nova LADA, passou a ser legislado o acesso direto aos processos clínicos, que se traduz na dispensa da intermediação do profissional (o médico) para o efeito, podendo o próprio titular aceder às informações de saúde diretamente. Não há, no entanto, uma dispensa total do papel do médico no âmbito do acesso aos processos clínicos. A LADA dita que, pode ainda existir esta possibilidade quando o "requerente solicitar", artigo 7.º n.º 1.

Não obstante, o Código Deontológico da Ordem dos Médicos (CDOM), retém-se na ideologia do acesso indireto: "o doente tem direito a conhecer a informação registada no seu processo clínico, a qual lhe será transmitida, se requerida, pelo próprio médico assistente ou, no caso de instituição de saúde, por médico designado pelo doente para este

[183] Nos termos da Lei sobre Informação Genética Pessoal e Informação de Saúde, Lei n.º 12/2005, 26 de janeiro, "o processo clínico é constituído por qualquer registo informatizado ou não, que contenha informação de saúde sobre doentes ou seus familiares". O processo clínico consiste, então, num conjunto de documentos e informações registadas que refletem a história de saúde e os cuidados médicos prestados a um paciente e, portanto, revela-se crucial para a continuidade e qualidade da prestação dos cuidados de saúde ao doente.

[184] Lei n.º 67/98, 26 de outubro, revogada pela Lei n.º 58/2019, 8 de agosto, atualmente em vigor.

[185] Mais tarde revogada pelo RGPD, que no seu artigo 15.º dita os titulares têm acesso direto aos processos clínicos.

efeito", artigo 40.º n.º 3. De acordo com o Código Deontológico, os médicos têm a obrigação de assegurar que os pacientes tenham acesso à informação contida nos seus processos clínicos, mas esse acesso deve ser mediado e gerido pelo médico responsável pelo seu tratamento.

Ainda assim, o disposto na LADA é a regra geral no ordenamento jurídico português, isto é, os titulares têm acesso direto aos dados pessoais contidos nos processos clínicos a menos que este, solicite a intermediação de um médico.

Tal acontece porque, a legislação tem um peso normativo superior ao do código deontológico. A LADA é uma legislação nacional que estabelece os direitos de acesso aos documentos administrativos, incluindo documentos clínicos. Sendo uma lei, ela possui uma autoridade jurídica superior ao Código Deontológico, que é uma regulamentação interna da Ordem dos Médicos. E, portanto, o CDOM deve ser interpretado e aplicado em consonância com a legislação vigente. Embora o CDOM possa recomendar que o acesso efetuado por intermédio do médico, para garantir a correta interpretação das informações, não pode contrariar o direito legal de acesso estabelecido e protegido pela LADA.

A coexistência de duas leis que partilham do mesmo objeto,[186] principalmente no que toca ao acesso ao processo clínico por parte do utente, resulta, em muitas das vezes, em posições de contradição que suscitam algumas divergências entre duas entidades, sendo elas a CADA e a CNPD. Quer isto dizer que, as entidades que têm competência para se pronunciarem sobre o acesso ao processo clínico divergem entre si e, portanto, não existe um entendimento unanime na sua conduta.

Esta divergência acontece porque a CADA entende que este tipo de processos recai sobre a responsabilidade da LADA e, por essa razão, compete-lhe a si resolver qualquer questão ou conflito decorrentes da aplicação desta lei. Por outro lado, a CNPD partilha do entendimento que é sobre a Lei n.º 58/2019 que devem incidir as responsabilidades dos conflitos que dizem respeito ao acesso aos processos clínicos e, portanto, é a CNPD que deve solucionar estas questões.

Dada a incompatibilidade e a falta de entendimento por parte de ambas as entidades, os tribunais decidiram, de forma inequívoca e unanime, que quando está em

[186] Referimo-nos à LADA e ao RGPD. Para melhor entendermos esta divergência, devemos recuar ao Capítulo I, Ponto 1.3.

causa o acesso à informação de saúde no setor público, a sua regulação será feita pela LADA, o que significa que a responsabilidade de zelar pelo cumprimento da lei recai sobre a CADA. Quando está em causa um processo clínico depositado no setor privado, este vê-se ao abrigo da Lei n.º 58/2019 e, portanto, sobre a responsabilidade da CNPD.

## 4.2. Direito à retificação

Resulta do artigo 16.º do RGPD que o titular dos dados tem direito a exigir, sem demora injustificada, a retificação dos seus dados quando inexatos e, atendendo às finalidades do tratamento, exigir que os dados pessoais incompletos sejam completados, nomeadamente por meio de uma declaração adicional.[187]

O direito à retificação é a manifestação prática do princípio da exatidão[188], previsto no artigo 5.º n.º 1 al. c) do RGPD.[189] Enquanto o princípio da exatidão estabelece a necessidade de que os dados sejam precisos e atualizados, o direito à retificação garante que os titulares possam intervir para corrigir quaisquer erros ou desatualizações, assegurando a integridade e a transparência dos dados pessoais tratados por qualquer entidade.

Para exercer este direito, deve o titular contactar o responsável pelo tratamento dos seus dados pessoais e solicitar a correção das informações. A entidade responsável pelo tratamento dos dados deve responder ao pedido de retificação sem demora injustificada e, no caso do pedido de retificação não for atendido adequadamente, o titular dos dados deve apresentar reclamação à Comissão Nacional de Proteção de Dados (CNPD), que é a autoridade responsável pela aplicação e supervisão das leis de proteção de dados em Portugal.

Além do mais, o direito à retificação vem igualmente consumado no artigo 35.º n.º 1 da CRP, quando diz que "todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei", bem como no

[187] Artigo 16.º do RGPD, pode ler-se "O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional".

[188] Estudamos no Capítulo III, pág. 37-38.

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

artigo 8.º n.º 2 da Carta, "(…) Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação".

Este direito representa assim o dever das entidades em tratarem dados pessoais apenas quando estes correspondam à realidade e, por isso, transparentes. Para o efeito, resulta do artigo 19.º do RGPD a obrigação de notificação ao titular da retificação ou apagamento dos dados pessoais ou limitação do tratamento, isto é, "o responsável pelo tratamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido em conformidade com o artigo 16.º, o artigo 17.º, n.º 1, e o artigo 18.º, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. Se o titular dos dados o solicitar, o responsável pelo tratamento fornece-lhe informações sobre os referidos destinatários".

## 4.3. Direito ao apagamento (direito ao esquecimento)

O direito ao esquecimento é um conceito relativamente novo e emergente no âmbito do direito digital e da proteção de dados pessoais. Em Portugal, assim como em outros países da União Europeia, este direito ganhou destaque com a implementação do Regulamento Geral sobre a Proteção de Dados (RGPD) e, consiste no direito do titular em "obter do responsável pelo tratamento o apagamento dos seus dados pessoais", quando perante uma das situações previstas nas alíneas do artigo 17.º.[190]

O direito ao esquecimento[191] é uma concretização do princípio da minimização dos dados, previsto no artigo 5.º n.º 1 al. c) do RGPD que diz que os dados pessoais devem ser "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados".[192] O que quer dizer que, quando as finalidades a que os dados

[190] "A nossa Constituição acolhe, portanto, «uma dimensão transnacional dos direitos fundamentais. Significa isto que tanto os direitos infraconstitucionais (direitos fundamentais formalmente constitucionais fora do catálogo dos artigos 24.º a 79.º), como os direitos extraconstitucionais (consagrados na legislação ordinária, ou inclusivamente na legislação internacional ou comunitária), que possuam um caráter materialmente jusfundamental, serão, em regra, considerados direitos de natureza análoga aos direitos, liberdades e garantias, nos termos do artigo 17.º da Constituição. (…) o direito ao esquecimento poder-se-á configurar como um direito fundamental implícito ou um direito fundamental inferido", BOTELHO, Catarina Santos, *Novo ou velho direito? – O Direito ao esquecimento e o princípio da proporcionalidade no constitucionalismo global*, AB INSTANTIA, V (7), 2017, pág 15-16, https://papers.ssrn.com/sol3/results.cfm.

[191] Considerando 65 e 66 do RGPD.

[192] Ver Capítulo III, Ponto 3.3.1., pág. 36-37.

se propuseram se encontrem devidamente preenchidas, o titular tem o direito de os ver apagados, até porque, à partida, não serão mais úteis à entidade.

O Tribunal da Relação de Lisboa[193] entende o direito ao esquecimento como um direito que "pode ser definido como um direito fundamental de personalidade amparado no princípio da dignidade humana, segundo o qual o titular, pessoa individual ou coletiva, tem o direito à autodeterminação informativa, isto é, pode requerer o apagamento, retirada ou bloqueio da divulgação de dados, lícitos ou não, que lhe digam respeito, encontrados nos diversos meios de comunicação e que não tenham mais interesse público, judicial, histórico ou estatístico ou ainda que não sejam vedados por lei. Não se trata, portanto, de eliminar todas as referências a factos ocorridos no passado, mas apenas de evitar a exposição desnecessária e lesiva de acontecimentos desprovidos de interesse público atual. Exprime em suma um poder de autocontrolo dos próprios dados pessoais".

Quer isto dizer que, este direito deve ser exercido, sem demora injustificada, nas situações previstas no artigo 17.º n.º 1 al. a) a f) do RGPD, quando: os dados já não sejam necessários para atingir o fim para o qual foram recolhidos e não há nenhuma norma legal que imponha a sua conservação por mais tempo; tenha retirado o seu consentimento, no qual se baseava a legitimidade do tratamento; os dados estejam a ser tratados ilicitamente, o que carece de justificação por parte do titular; o titular se opõe ao tratamento; a recolha e o tratamento dos dados não respeita o disposto no RGPD ou no direito da União Europeia.

Há, no entanto, a salientar que, no artigo 17.º n.º 2, o legislador acaba por fazer uma distinção entre o direito de apagamento e o direito ao esquecimento dos dados pessoais. Ora, nos casos em que a entidade responsável pelo tratamento tenha tornado públicos os dados pessoais e se veja obrigada a apagá-los nos termos das alíneas do n.º 1, deve não só informar o titular de que apagou os dados, bem como, proceder ao apagamento das cópias ou reproduções dos mesmos, ou seja, não resultam quaisquer evidencias de que, alguma vez, estes dados foram tratados e, por isso, consideram-se esquecidos.[194]

---

[193] Ac. do Tribunal da Relação de Lisboa, de 02/05/2023, n.º de processo 12234/21.0T8LSB.L1-7,https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/6b57c49941d5779f802589aa0049be2a?OpenDocument.

[194] Artigo 17.º n.º 2 do RGPD, pode ler-se "Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua

Para melhor compreensão tomamos os seguintes exemplos: *A* deixou de ser cliente de uma empresa de telecomunicações há vários anos e percebe que a empresa ainda mantém os seus dados pessoais, pelo que *A* pode solicitar o apagamento dos deus dados do sistema de informatização da empresa, uma vez que, estes já não são necessários para a finalidade a que inicialmente se propuseram; *B* subscreveu uma *newsletter* de uma loja *on-line* e não pretende receber mais comunicações da mesma, pelo que, pode retirar o seu consentimento e solicitar que apague os seus dados pessoais para o envio da *newsletter*.

O Considerando (65) do RGPD considera ainda como um particular exemplo, o caso em que "o titular dos dados tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento, e mais tarde deseje suprimir esses dados pessoais"[195].

Existem, no entanto, exceções que estão previstas no artigo 17.º n.º 3, pelo que, excluem-se do direito ao apagamento ou esquecimento, as situações em que o tratamento se revele necessário: "a) Ao exercício da liberdade de expressão e de informação; b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.º, n.º 2, alíneas h) e i), bem como do artigo 9.º, n.º 3; d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1, na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou e)Para efeitos de declaração, exercício ou defesa de um direito num processo judicial".

Nestes casos, o responsável pelo tratamento deve notificar qualquer entidade (destinatários) com quem os dados pessoais foram compartilhados sobre qualquer retificação, apagamento ou limitação do tratamento dos dados, artigo 19.º RGPD.

Contudo, há que considerar que este direito não é absoluto e, em determinadas situações, cede perante outros direitos e obrigações como direitos de liberdade de

aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos".

[195] Artigo 16.º da Lei n.º 58/2019, 8 de agosto e artigo 6.º n.º 1 al. A) e 8.º do RGPD;

expressão e de informação, quando o tratamento dos dados decorre de uma obrigação de Direito da União ou de um Estado-Membro, por motivos de interesse público, quando o tratamento dos dados é relevante no âmbito de um processo judicial e ainda nos casos de proteção de saúde pública, artigo 17.º n.º 3 al. c) e artigo 9.º n.º 3 do RGPD.

## 4.4. Direito à limitação do tratamento

O artigo 4.º n.º 3 define limitação do tratamento, sendo este "a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro". O objetivo aqui é garantir que os dados pessoais não são utilizados ou tratados para qualquer outra finalidade que não aquela para as quais se destinam, inicialmente, com o consentimento do titular, ou seja, vez que os dados estejam "marcados" o seu tratamento futuro é restrito ou condicionado.

Nos termos do considerando (67), a entidade responsável pode socorrer-se de "métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio web dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados".

Enquanto isso, o artigo 18.º salvaguarda o direito à limitação do tratamento, elencando no n.º 1 as situações em que o titular dos dados pode solicitar ao responsável a limitação do tratamento dos seus dados pessoais, ou seja, na pendência de uma contestação à exatidão dos dados, se o tratamento dor lícito, se os dados deixarem de ser necessários para a finalidade que motivou o tratamento e, ainda na pendência de um pedido de oposição, intentado nos termos do artigo 21.º.[196]

Nos casos em que a entidade responsável entenda que já não se reúnam condições que justifiquem a limitação do tratamento dos dados, esta tem a obrigação de notificar o titular dos dados antes de tomar qualquer medida que anule ou suspenda a limitação que foi previamente concedida. Por outras palavras, se a entidade responsável pelo tratamento

[196] Nestes casos, diz o n.º 2 do mesmo artigo que "Quando o tratamento tiver sido limitado nos termos do n.º 1, os dados pessoais só podem, à exceção da conservação, ser objeto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro".

dos dados decidir que já não é necessária a limitação do tratamento, por exemplo, porque a questão que justificava a limitação foi resolvida, deve informar o titular antes de retomar o tratamento normal dos seus dados. A partir de então, os dados pessoais deixarão de estar sujeitos às restrições impostas e poderão voltar a ser tratados normalmente.[197]

## 4.5. Direito de Portabilidade

O direito à portabilidade encontra-se previsto no artigo 20.º do RGPD, pelo que o n.º 1 o decompõe em dois direitos distintos, o direito que o titular dos dados tem em receber os dados que lhe digam respeito, ao mesmo tempo que salvaguarda o direito que o titular tem em transmitir esses mesmos dados para outro responsável.

A especificidade da portabilidade é a de oferecer uma ferramenta prática para o titular gerir e reutilizar os dados que lhe digam respeito, de acordo com a sua vontade e interesses[198] e, por essa razão, estipula o n.º 1 que o titular deve receber os dados num formato estruturado, de uso corrente e de leitura automática. Deste modo, a portabilidade dos dados é um direito do titular dos dados a receber um subconjunto dos dados pessoais tratados por um responsável pelo tratamento e que lhe digam respeito, bem como a armazenar esses dados para uso pessoal posterior. Este armazenamento pode ser feito através de um dispositivo privado ou de uma nuvem privada, sem haver necessariamente lugar a uma transmissão dos dados para outro responsável pelo tratamento. Em segundo lugar, confere aos titulares dos dados o direito de transmitir os dados pessoais de um responsável pelo tratamento para outro responsável pelo tratamento sem impedimentos.[199]

Para o efeito, o direito à portabilidade depende da verificação de dois requisitos cumulativos que resultam das alíneas previstas no n.º 1, isto é, o tratamento dos dados deve ser baseado no consentimento do titular nos termos do artigo 6.º n.º 1 al. a) e 9.º n.º 2 al. a) e, o tratamento tem de ser realizado por meios automatizados.[200]

---

[197] Artigo 18.º n.º 3.

[198] COUTINHO, Francisco Ferreira e MONIZ, Graça Canto, *Direitos do titular dos dados pessoais: o direito à portabilidade*, Anuário da Proteção de dados, 2018, ISBN: 978-972-99399-5-2, disponível em SSRN: https://ssrn.com/abstract=3287763, pág. 27.

[199] GT 29, *Orientações sobre o direito à portabilidade dos dados (*WP 242rev.01), 13/12/2016, pág. 5 https://paulomeireles.pt/wp-content/uploads/2018/05/Orienta%C3%A7%C3%B5es_WP242_-sobre-o-direito-%C3%A0-portabilidade-dos-dados.pdf.

[200] Considerando (68) do RGPD, pode ler-se "Para reforçar o controlo sobre os seus próprios dados, sempre que o tratamento de dados pessoais for automatizado, o titular dos dados deverá ser autorizado a receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo

Assim, os dados a que o titular tem direito a receber devem não só dizer-lhes diretamente respeito, bem como, serem aqueles que este forneceu. Como tal, o GT 29 considera que, para potenciar ao máximo o valor deste novo direito, os dados fornecidos pelo titular devem igualmente incluir os dados pessoais que sejam observados a partir das atividades dos utilizadores, tais como os dados brutos tratados por um contador inteligente ou por outros tipos de objetos conectados, os registos das atividades e os históricos da utilização de um sítio *Web* ou das pesquisas realizadas. Esta última categoria de dados não inclui os dados criados pelo responsável pelo tratamento (com base nos dados observados ou diretamente inseridos), por exemplo um perfil de utilizador criado através de uma análise dos dados brutos de contagem inteligente recolhidos.

Posto isto, a entidade responsável, nos termos do n.º 3 do artigo 12.º, dispõe de um mês sem demora injustificada a contar da data de receção do pedido, para fornecer ao titular as informações sobre as medidas tomadas. Este prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos, perfazendo um total de três meses, devendo para o efeito, o titular estar devidamente informado.

## 4.6. Direito de Oposição

Nos termos do artigo 21.º, o titular tem o direito de se opor a qualquer momento ao tratamento lícito dos seus dados pessoais, quando, cumulativamente se verifiquem os pressupostos no n.º 1 do presente artigo.[201]

Este direito permite que os titulares se oponham ao tratamento dos seus dados pessoais em determinadas circunstâncias. Esta oposição tem lugar a qualquer momento e pode ser baseada em motivos de cariz pessoal, devendo por isso, a entidade responsável, suspender de imediato o tratamento destes dados. Contudo, diz-nos a parte final do artigo 21.º do RGPD, que o direito à oposição não tem efeito quando estejam em causa razões

tratamento num formato estruturado, de uso corrente, de leitura automática e interoperável, e a transmiti-los a outro responsável. Os responsáveis pelo tratamento de dados deverão ser encorajados a desenvolver formatos interoperáveis que permitam a portabilidade dos dados. Esse direito deverá aplicar-se também se o titular dos dados tiver fornecido os dados pessoais com base no seu consentimento ou se o tratamento for necessário para o cumprimento de um contrato. (…)".

[201] Artigo 21.º n.º 1, pode ler-se "O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.º, n.º 1, alínea e) ou f), ou no artigo 6.º, n.º 4, incluindo a definição de perfis com base nessas disposições".

legítimas para tal e que se sobreponham aos direitos e liberdades do titular dos dados, ou por motivos de declaração, exercício ou defesa de um direito num processo judicial.[202] O que não faz do direito à oposição um direito absoluto, com exceção dos tratamentos para efeitos de comercialização direta, artigo 21.º n.º 3.[203]

Nos restantes casos, o titular pode exercer o direito à oposição sempre que entender, até mesmo quando o tratamento tenha como finalidade uma investigação científica, fins históricos ou estatísticos – desde que estes não tenham como objetivo o interesse público.

[202] Parte final do artigo 21.º n.º 1, "(…) O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial".

[203] COUTINHO, Francisco Ferreira e MONIZ, Graça Canto, *Direitos do titular dos dados pessoais: o direito à portabilidade*, Anuário da Proteção de dados, 2018, ISBN: 978-972-99399-5-2, disponível em SSRN: https://ssrn.com/abstract=3287763, pág. 21, "O titular dos dados pessoais goza, nos termos do art. 21.º, do poder de se opor ao tratamento de dados, em qualquer momento, por razões preponderantes e legítimas relacionadas com a sua situação particular. Sendo um reconhecimento do direito à autodeterminação, por um lado, o seu exercício não é absoluto – com a exceção dos tratamentos para efeitos de comercialização direta – e, por outro, a sua aplicação não é geral".

# CAPÍTULO V – ESTUDO DE CASO

Como estudamos até aqui, a proteção de dados pessoais, em especial os dados de saúde, configura um direito fundamental que visa salvaguardar a privacidade e a confidencialidade das informações mais sensíveis de um indivíduo, conforme estipulado pelo Regulamento Geral sobre a Proteção de Dados (RGPD).[204] No entanto, a aplicação deste direito enfrenta desafios significativos, especialmente quando é necessário equilibrá-lo com o direito de acesso. O direito de acesso, tanto pelo próprio titular dos dados como por terceiros em situações muito específicas e previstas na lei, suscita questões delicadas, nomeadamente sobre até que ponto as informações de saúde de alguém podem ser partilhadas sem comprometer a sua confidencialidade e sem divergir com os pressupostos do RGPD e da Lei n.º 58/2019. Em contexto judicial, por exemplo, o acesso de terceiros a dados pessoais de saúde pode ser essencial para a resolução de disputas legais, o que cria uma crescente tensão entre a proteção da privacidade e a necessidade de transparência e justiça.[205]

A fim de consolidarmos a matéria da proteção de dados pessoais que estudamos na presente dissertação, analisemos ao detalhe um caso prático que traduz, eficazmente, o cariz especial dos dados pessoais de saúde, o direito de acesso a esses mesmos dados e as exceções que a lei aplica:

A autora *F*, na qualidade de herdeira, intentou uma ação de processo comum de declaração contra *A, B, C, D e E,*(também herdeiros) ao abrigo do artigo 598.º n.º 1 do CPC, na qual a autora solicitou a junção de cópia dos registos clínicos das consultas de *G* (pai da autora e dos réus e já falecido), relativos ao período 19/11/2006 a 18/09/2006 no Serviço de Neurologia do Hospital de *H*, bem como o plano de medicação e relatório de exames médicos, para prova de que, aquando da doação em vida que *G* fez em relação aos seus filhos, este encontrava-se acidentalmente incapacitado por força da doença que lhe fora diagnosticada, o Alzheimer. E, assim, *F* vem impugnar por via judicial a doação decorrida. Os réus contestaram, requerendo a inadmissibilidade e desentranhamento dos documentos juntos pela autora, alegando serem prova ilícita, ao abrigo do disposto no artigo 32.º da CRP, argumentando que, nos termos dos artigos 4.º e 9.º do RGPD, não é

[204] Rever Capítulo II e III.

[205] Rever Capítulo IV, Ponto 4.1., a propósito do princípio da administração aberta do direito de acesso.

permitido o tratamento de dados pessoais relativos à saúde das pessoas, os quais abrangem dados relacionados com a saúde física e mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde. Mais acrescentam os réus na contestação que, na falta de consentimento de *G*, tais documentos não constituem escusa de segredo médico, devendo e, por isso, permanecer na esfera privada do mesmo, como resulta do artigo 139.º do EOM[206]. Assim sendo, os réus requerem a nulidade das provas apresentadas pela autora, nos termos do artigo 32.º da CRP, pelo que, devem as mesmas ser desconsideradas pelo tribunal.[207]

Primeiramente, é importante ressalvarmos que estamos perante dados pessoais de saúde que se revelam de cariz especial cujo tratamento é, em regra, proibido salvo exceções previstas na lei, artigo 4.º n.º 1 e 9.º n.º 1 e 2. Mais sabemos que, como estudamos, a aplicação prática do RGPD, limita-se às informações relativas a pessoas vivas, até porque, a definição de dados pessoais, não inclui pessoas falecidas. [208]

Para o efeito, a parte final do Considerando (27) do RGPD, é acompanhada de uma cláusula aberta, que permite aos Estados-Membros estabelecer regras para este tratamento de dados em específico, pelo que, em Portugal, o tratamento de dados de pessoas falecidas encontra-se previsto no artigo 17.º da Lei n.º 58/2019, quando o n.º 1 diz que "os dados pessoais de pessoas falecidas são protegidos nos termos do RGPD e da presente lei quando se integrem nas categorias especiais de dados pessoais a que se refere o n.º 1 do artigo 9.º do RGPD, ou quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações, ressalvados os casos previstos no n.º 2 do mesmo artigo".

A salientar que o n.º 2 do artigo 17.º garante o exercício dos direitos previstos no RGPD relativamente ao titular dos dados pessoais, nomeadamente o direito de acesso, conveniente para o caso em apreço. Mais acrescenta, que estes direitos, tendo em conta que o titular faleceu, são exercidos "por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respetivos herdeiros", a menos que, o titular deixe

---

[206] Estatuto da Ordem dos Médicos;

[207] Ac. do Tribunal da Relação do Porto, de 24/01/2022, n.º de processo 3328/19.2T8STS-A.P1, https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/8fffb6004be424798025880100330de4?OpenDocument&Highlight=0,LEI,N.%C2%BA,58%2F2019,DE,08.08.

[208] O Considerando (27) do RGPD é muito expresso quando diz que "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".

"determinada a impossibilidade de exercício dos direitos referidos no número anterior após a sua morte", cfr. o n.º 3.

Face ao exposto, é nos igualmente conveniente, relembrar que os dados pessoais de saúde são propriedade das pessoas a que pertencem, sendo as unidades de saúde, meras depositárias dessas informações, conforme o artigo 3.º n.º 1 e 2 da Lei n.º 12/2005. Quer isto dizer que, no caso concreto, a tutela dos dados pessoais de saúde recai sobre *G*, podendo este reservá-los para si ou, mediante consentimento informado e voluntário, permitir que terceiros lhes acedam.[209] Tal acontece porque, estas informações estão, imperativamente, sujeitas a segredo médico, conforme o disposto no artigo 67.º e ss do CDOM e artigo 20.º da Lei n.º 58/2019, sendo esta uma condição essencial para prática médica, já que integram o estatuto profissional dos médicos quer do ponto de vista prático, como ético e deontológico.

No caso em apreço, os réus alegam que não houve autorização para a divulgação dos dados e que a autora não demonstrou que os registos clínicos requeridos e apresentados, tivessem sido alvo de dispensa do segredo médico e, por isso, estão sujeitos a sigilo profissional, nos termos do artigo 67.º do CDOM e 139.º do EOM, não tendo legitimidade para os requerer.

A ausência de consentimento explícito do falecido para o acesso aos seus dados de saúde é uma questão delicada e pode gerar alguma controvérsia. No entanto, como vimos no Capítulo IV, existem situações muito específicas em que a lei, permite este acesso, nomeadamente nos casos em que haja um consentimento explícito do titular do titular dos dados ou, em situações em que um terceiro atue mediante um interesse direto, pessoal, legítimo e constitucionalmente protegido, como resulta do artigo 6.º da LADA. Nos casos em contrário, sempre que um documento contenha informação relativa a uma pessoa singular identificada ou identificável, o seu acesso é, em regra proibido.

Assim sendo, há três questões importantes a analisar no caso em concreto, o consentimento do titular, o segredo médico e a condição em que o terceiro atua. Embora *G* não tenha prestado o seu consentimento para o acesso de terceiros aos seus dados de saúde, estes não estão abrangidos pelo segredo médico, já que "os dados pessoais de

[209] Vimos no Capítulo IV que o direito de acesso assenta na autodeterminação informacional e, conforme definido no artigo 15.º do RGPD e Considerando (63), confere aos indivíduos o poder de solicitar e receber informações sobre a forma como os seus dados pessoais estão a ser tratados, qual o tratamento aplicado e se este será o mais adequado e lícito.

pessoas falecidas são protegidos nos termos do RGPD e da presente lei quando se integrem nas categorias especiais de dados pessoais a que se refere o n.º 1 do artigo 9.º do RGPD, ou quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações", artigo 17.º da lei 58/2019, a menos que o titular deixe "determinada a impossibilidade de exercício dos direitos referidos no número anterior após a sua morte" (n.º 2 e 3 do presente artigo), o que não aconteceu.

Quer isto dizer que, nos termos do artigo mencionado, um familiar de um doente falecido só pode aceder à sua informação de saúde, se demonstrar, fundamentadamente, ser titular de um interesse direto, pessoal, legítimo e suficientemente relevante, que justifique tal acesso, nomeadamente, quando pretende apresentar uma reclamação ou recorrer à via judicial, para o exercício de um qualquer direito ou interesse. Mais acrescenta o Tribunal que estes dados estavam na posse e eram acessíveis às partes, sendo estes descendentes de *G* e, portanto, herdeiros nos termos do artigo 2133.º n.º 1 al. a) do Código Civil, o que significa que, *F* agiu com legitimidade para o efeito, já que, o artigo 17.º n.º 2 da Lei n.º 58/2019, "não exclui qualquer categoria de herdeiro: limita-se a remeter para o regime comum; e também não estabelece qualquer critério de ordenação, pelo que qualquer sujeito que pertença a uma destas sete classes de herdeiro poderá exercer os correspondentes direitos".[210]

Mais alegam os réus de que, não foram notificados nem autorizaram o acesso a estes dados, devendo, por isso, ter lhe sido negado o acesso ao processo clínico de *G*.

Ora, no caso concreto, estamos perante um acesso por quem sucedeu na titularidade dos dados de saúde, isto é, *F* agiu na qualidade de descendente e herdeira. Comprovada esta qualidade e a inexistência de impedimento legal, deve ser-lhe facultada a documentação sobre as informações de saúde que solicitou e que existam, sem obstáculo, conforme o artigo 5.º n.º 1 e artigo 15.º n.º 1 al. d) da LADA e artigo 17.º n.º da Lei n.º 58/2019.[211] O Tribunal refe ainda que, na qualidade de herdeira, a autora e qualquer outros dos descendentes, têm acesso aos dados de saúde de *G*, afim de proteger direitos que possam estar em posição de risco ou violação. Na prática, é o que acontece, uma vez que a autora pretende impugnar uma doação celebrada numa altura em que, alegadamente, o autor da doação (*G*) não se encontrava na plena capacidade das suas

[210] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019*, Almedina, Coimbra, 2020, pág. 119.

[211] Parecer da CADA n.º 250/2024, n.º de processo 317/2024.

faculdades mentais. Assim sendo, a autora está a zelar pelo benefício de *G*, uma vez que, verificada a veracidade dos factos, a doação em causa pode vir a refletir-se significativamente na herança aberta por morte deste. Posto isto, concluímos que, de facto, a autora ao intervir na qualidade de herdeira está a agir com um interesse direto, pessoal, legítimo.

Deste modo, face aos argumentos apresentados e à análise jurídica dos pressupostos, o Tribunal considera, efetivamente, a qualidade em que a herdeira intervém e mais solicita os dados clínicos do ascendente de todas as partes envolvidas, com o objetivo de demonstrar a veracidade dos factos e tomar uma decisão justa, decisão esta que se fundamentada no artigo 436.º do CPC. Os elementos clínicos solicitados não estão protegidos pelo segredo médico profissional e são essenciais para comprovar a alegada incapacidade mental do doador no período próximo à doação. Adianta também, o Tribunal, que de acordo com a lei, a autora, na qualidade de herdeira, tem direito não só a aceder, mas também a apagar ou a retificar as fichas clínicas do pai (*G)*, assim como tem direito aos dados relativos à imagem, intimidade da vida privada e comunicações, artigo 17.º n.º 2 da Lei n.º 58/2019.

A decisão do Tribunal da Relação do Porto serve como exemplo prático e jurisprudencial do acesso de terceiros às informações de saúde e processos clínicos de pacientes falecidos. No caso, a autora, herdeira do falecido, solicitou os registos clínicos do seu pai a fim de provar sua incapacidade mental, decorrente da doença Alzheimer, no período próximo à doação contestada.

Os réus argumentaram contra a admissibilidade dessas provas, citando a proteção de dados pessoais e o segredo médico, conforme a Constituição da República Portuguesa (CRP) e o Regulamento Geral sobre a Proteção de Dados (RGPD). No entanto, o Tribunal baseia a sua decisão no artigo 436.º do CPC, afirmando que os processos clínicos não estão protegidos pelo segredo médico profissional e constituem prova essencial, uma vez que tendem a provar a alegada incapacidade mental do doador.

O Tribunal destaca ainda que, de acordo com o artigo 17.º da Lei n.º 58/2019, os herdeiros têm o direito de aceder aos dados de saúde do falecido quando visem proteger direitos que possam, de alguma forma, estar em risco. A autora demonstrou um interesse direto, pessoal e legítimo, agindo na qualidade de herdeira para contestar a doação e proteger o património familiar. Assim, o Tribunal entende que, nesta qualidade, pode a herdeira, sem qualquer impedimento, aceder aos dados clínicos do seu pai, nos quais se

incluem informações sobre sua saúde mental, para demonstrar a veracidade dos factos e proteger os interesses da herança, conforme previsto no artigo 17.º, n.º 2 da Lei n.º 58/2019.Concluímos assim que, a decisão do Tribunal enfatiza a extrema importância de demonstrar um interesse direto, pessoal e legítimo para aceder os dados de saúde,

Concluímos assim que, o caso em análise demonstra as complexas interações entre a proteção de dados pessoais de saúde e o direito de acesso, especialmente em contexto judicial que envolvem herdeiros. Embora os dados de saúde sejam geralmente protegidos no âmbito da confidencialidade e do segredo médico, o ordenamento jurídico português prevê exceções muito específicas que permitem o acesso a dados pessoais sensíveis, incluindo os dados de saúde, nos casos em que exista um interesse direto, pessoal e legítimo. No caso em concreto, o Tribunal entendeu que, sendo a autora herdeira legítima, tem o direito de aceder aos dados pessoais de saúde do falecido, uma vez que tal acesso se revela imprescindível e necessário para proteger interesses patrimoniais do mesmo ao impugnar a doação em causa, ao mesmo tempo que visa equilibrar a necessidade de proteger a privacidade dos dados pessoais do falecido com a necessidade de salvaguardar os seus bens em matéria sucessória.

# CONCLUSÃO

A presente dissertação permitiu-nos tirar várias conclusões, desde logo o facto de que a proteção de dados pessoais, especialmente os de saúde, é essencial para garantir a privacidade e a dignidade dos indivíduos num mundo cada vez mais digitalizado.

O direito à privacidade e à proteção dos dados pessoais evoluiu significativamente ao longo do tempo, consolidando-se através de diversas normas legislativas internacionais e europeias, como Declaração Universal dos Direitos Humanos, a Convenção Europeia dos Direitos Humanos, e a Carta dos Direitos Fundamentais da União Europeia. Estes marcos legislativos estabeleceram as bases e os princípios fundamentais da privacidade e proteção de dados que influenciaram diretamente a legislação europeia subsequente. Através destas convenções internacionais, o direito à privacidade foi reconhecido como um direito fundamental, formando a base para a necessidade de proteger os dados pessoais de forma robusta e uniforme em toda a União Europeia que podemos testemunhar atualmente. Com o advento da Era digital, a proteção da privacidade ganhou uma nova dimensão, já que o volume de dados pessoais recolhidos, armazenados e tratados cresceu exponencialmente, muito impulsionado pela *internet*, pelas redes sociais e pela economia de dados. Este cenário trouxe à tona a necessidade de legislação e regulamentos mais rigorosos e, que se revelassem capazes de acompanhar o ritmo acelerado da inovação tecnológica e os novos riscos associados à recolha e ao tratamento massivo de informações pessoais.

A privacidade, neste contexto, deixou de ser apenas uma questão de proteção contra invasões físicas e passou a incluir a proteção e controlo digital contra o uso indevido de dados pessoais. O Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, que entrou em vigor em 2018, que representa um claro esforço dos Estados-Membros em abordar e fortalecer os direitos dos cidadãos europeus em relação à proteção dos seus dados pessoais, reforçando o direito à privacidade como uma componente central da proteção de dados e, por essa razão, estabelece normas restritas para o tratamento lícito e transparente dos dados pessoais, nomeadamente através do cumprimento dos princípios que orientam o tratamento dos dados pessoais, como a licitude, transparência, minimização, e o consentimento informado, são cruciais para assegurar que os dados sejam tratados de forma ética e conforme as expectativas dos titulares.

Tal acontece porque, até então, não existia nenhum regulamento que consolidasse a ideia da proteção de dados pessoais no contexto europeu, o que se traduziu numa fragmentação legislativa dos Estados-Membros e, portanto, o RGPD, veio substituir as legislações nacionais fragmentadas através de um conjunto de regras uniformes aplicáveis em toda a União Europeia. Esta harmonização foi essencial para garantir que todos os cidadãos europeus tivessem o mesmo nível de proteção de dados, independentemente de onde se encontrassem na UE, reforçando a proteção da privacidade e assentando a ideologia de um Mercado Único Digital. No contexto nacional, a transposição do RGPD para o ordenamento jurídico português foi essencial para garantir que o direito à privacidade e à proteção de dados fossem respeitados e aplicados de acordo com os princípios internacionais e europeus. A adoção da Lei n.º 58/2019, que transpõe para a legislação nacional as normas do RGPD, refletiu o compromisso de Portugal em assegurar uma proteção eficaz e contemporânea dos dados pessoais, especialmente à luz dos desafios trazidos pela digitalização e globalização.

Destacamos ainda a distinção entre dados pessoais e dados sensíveis que se revela fundamental para compreender as diferentes camadas de proteção impostas pelo RGPD, que reconhece que certo tipo de informações requerem uma proteção mais robusta devido ao potencial impacto que seu uso ou divulgação indevida pode ter sobre os direitos e liberdades dos seus titulares. Nestes dados, incluem-se os dados de saúde, que pela sua natureza íntima e potencialmente discriminatória, exigem uma proteção reforçada. O RGPD impõe obrigações rigorosas às entidades que tratam esses dados, especialmente no que se refere ao consentimento informado e livre do titular. O tratamento destes dados deve ser sempre realizado com base em princípios sólidos e base do Regulamento, de forma a assegurar que os dados recolhidos são estritamente necessários e adequados para as finalidades pretendidas.

Neste âmbito, o RGPD revelou-se inovador ao introduzir e ampliar os direitos dos titulares sobre os seus dados pessoais, como o direito ao acesso, à retificação, ao apagamento (direito ao esquecimento), à limitação do tratamento, à portabilidade dos dados e ainda à sua oposição. Estes direitos permitem que os titulares exerçam um maior controlo sobre as suas informações pessoais, fortalecendo a sua privacidade na órbita digital, aquilo a que chamamos de autonomia informacional.

Finalmente, o estudo de caso apresentado no último capítulo demonstrou as complexidades envolvidas na aplicação prática do RGPD, especialmente em situações

sensíveis como o tratamento de dados de saúde após a morte do titular. Este caso evidenciou a necessidade de uma interpretação cuidadosa e equilibrada das disposições do RGPD, de modo a proteger os direitos dos titulares enquanto se consideram também os direitos e interesses de terceiros. Consideramos importante a situação prática que apresentamos, na medida em que traduz, eficazmente, a complexidade e necessidade de equilíbrio dos direitos pessoais, especialmente os dados sensíveis, com outros direitos fundamentais. O estudo de caso mostra as dificuldades e nuances que surgem quando se tenta aplicar os princípios do RGPD a situações onde há múltiplos interesses em jogo. Por um lado, há a necessidade de proteger a privacidade e a confidencialidade dos dados de saúde do falecido, por outro lado, existem direitos e interesses de terceiros, como familiares ou entidades médicas, que podem justificar o acesso a esses dados. Uma das principais conclusões que retiramos desta análise é que, embora o RGPD forneça um quadro legal robusto, a sua aplicação em casos específicos requer uma interpretação cuidadosa e equilibrada. É necessário considerar o contexto particular de cada caso, garantindo que os direitos de todas as partes envolvidas sejam respeitados e que a proteção de dados não seja usada de forma a impedir o acesso legítimo a informações que podem ser cruciais para outros fins legais ou médicos.

Em suma, esta dissertação confirma que o RGPD é um marco legislativo essencial à proteção de dados pessoais na Era Digital, proporcionando um equilíbrio necessário entre a proteção dos direitos fundamentais e a promoção de um ambiente digital seguro e funcional. A aplicação prática deste regulamento, especialmente no contexto dos dados de saúde, exige uma abordagem flexível e contextualizada, garantindo que os direitos dos titulares sejam sempre salvaguardados sem comprometer outros direitos igualmente importantes.

## REFERÊNCIAS BIBLIOGRÁFICAS

BOTELHO, Catarina Santos, *Novo ou velho direito? – O Direito ao esquecimento e o princípio da proporcionalidade no constitucionalismo global*, AB INSTANTIA, V (7), 2017, https://papers.ssrn.com/sol3/results.cfm.

CANOTILHO, Gomes José & MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, 4.ª Edição, Vol. I, Coimbra, Coimbra Editora 2010.

CORDEIRO, A. Barreto Menezes, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019,* Almedina, Coimbra, 2021.

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

COUTINHO, Francisco Ferreira e MONIZ, Graça Canto, *Direitos do titular dos dados pessoais: o direito à portabilidade*, Anuário da Proteção de dados, 2018, ISBN: 978-972-99399-5-2, disponível em SSRN: https://ssrn.com/abstract=3287763.

CUNHA, Sílvia Maria Duarte, *Eliminação dos dados de Saúde: Um Direito do Paciente?* Dissertação de mestrado integrado em Medicina, Faculdade de Medicina, Universidade do Porto, Porto, 2018.

FRANCISCO, Daniel, & Francisco, Sandra, *Regulamento Geral de Proteção de Dados: 7 passos para uma metodologia de implementação do RGPD na Administração Pública*, Edições Sílabo, Lisboa, 2019.

FREITAS, Tiago & ALVES, Pedro Delgado, *O Acesso à Informação Administrativa*, Almedina, Coimbra, 2021.

GT 29, *Orientações relativas à transparência na aceção do Regulamento 2016/679 (WP260rev.1), 29 de novembro de 2017.*

GT 29, *Orientações relativas ao consentimento na aceção do Regulamento (UE),* 2016/679, WP259 rev.01, 28 de novembro de 2017.

GT 29, *Orientações sobre o direito à portabilidade dos dados (*WP 242rev.01), 13/12/2016,https://paulomeireles.pt/wpcontent/uploads/2018/05/Orienta%C3%A7%C3%B5es_WP242_-sobre-o-direito-%C3%A0-portabilidade-dos-dados.pdf.

GT 29, Parecer 4/2007, "*Images of individuals captured by a video surveillance system can be personal data to the extent that the individuals are recognizable*".

GT 29, Parecer n.º 4/2007 do, sobre o conceito de dados pessoais, de 20/06/2007.

GT29 Parecer n.º 3/2013 do *sobre a limitação da finalidade* (WP 203).

KPMG, *O Impacto do Regulamento Geral de Proteção de Dados em Portugal*, Estudo, março 2017, pág. 2, acedido e consultado em 13/08/2024, disponível em https://www.centromarca.pt/folder/conteudo/1722_7_pt-2017-rgpd.pdf.

MIRANDA, Jorge & MEDEIROS, Rui, *Constituição Portuguesa Anotada* - Tomo I, 2ª Edição, Coimbra Editora, Coimbra, 2010.

MIRANDA, Jorge e MEDEIROS, Rui, *Constituição Portuguesa Anotada*, Tomo III 1ª edição, Coimbra Editora, 2007.

MIRANDA, Jorge, *Direitos Fundamentais: Introdução Geral*, Diversos, Lisboa, 1999.

MOREIRA, Tiago Filipe Monteiro, *O Impacto do Regulamento Geral da Proteção de Dados Pessoais nas Organizações: Um Novo Paradigma*, Dissertação de mestrado em Solicitadoria, Instituto Superior de Contabilidade e Administração de Coimbra, Instituto Politécnico de Coimbra, 2018 NETO,

NETO, Eugênio Facchini & DEMOLINER, Karine Silva, Direito À Privacidade Na Era Digital – Uma Releitura Do ART. XII Da Declaração Universal Dos Direitos Humanos (DUDH) NA Sociedade Do Espetáculo, *Revista Internacional Consinter De Direito*, ANO V – NÚMERO IX, 2º Semestre, 2019.

OCDE, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*, 23 de setembro de 1980.

Parecer da CADA n.º 250/2024, n.º de processo 317/2024.

Parecer n.º 08/2024 sobre *Consentimento Válido no Contexto de Modelos de Consentimento ou Remuneração Implementados por Grandes Plataformas Online*.

Parecer n.º 15/2011 sobre a *definição de consentimento* (WP 187).

PARLAMENTO EUROPEU, *Trado de Lisboa*, acedido e consultado em 13/08/2024, disponível em https://www.parlamento.pt/europa/Paginas/TratadodeLisboa.aspx.

PINHEIRO, Alexandre Sousa, *Privacy e proteção de dados pessoais,* AAFDL Editora, 2015.

RIQUINHO, Ana Luísa, VENTURA, Catarina Sampaio, ANDRADE, J. C. Vieira de, CANOTILHO, J. J. Gomes, GORJÃO-HENRIQUES, Miguel, RAMOS, R. M. Moura, e, MOREIRA, Vital, *Carta de Direitos Fundamentais da União Europeia*, Coimbra Editora, 2001.

## LEGISLAÇÃO

Carta dos Direitos Fundamentais da União Europeia.

Código Civil.

Código Deontológico da Ordem dos Médicos.

Código do Processo Administrativo.

Código do Processo Civil.

Constituição da República Portuguesa.

Convenção Europeia dos Direitos Humanos.

Convenção n.º 108 para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal do Conselho da Europa, de 28 de janeiro de 1981.

Declaração Universal dos Direitos Humanos.

Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho de 24 de outubro de 1995.

Estatuto da Ordem dos Médicos.

Lei n.º 12/2005, 26 de janeiro.

Lei n.º 26/2016, 22 de agosto.

Lei n.º 58/2019, 8 de agosto

Lei n.º 67/98, 26 de outubro.

REGULAMENTO (CE) n.º 1338/2008 DO PARLAMENTO EUROPEU E DO CONSELHO de 16 de dezembro de 2008, *relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho*.

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

Tratado sobre o funcionamento da União Europeia.

## JURISPRUDÊNCIA

Ac. n.º 2594/99 do Tribunal Constitucional, n.º de processo 456/97, relator Cons. Sousa e Brito, https://www.tribunalconstitucional.pt/tc/acordaos/19990254.html

Ac. do TJUE de 07/02/1973, n.º de processo 39/72 (Comissão Itália), https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A1973%3A13

Ac. do TJUE, de 20/09/2001, n.º de processo C-453/99, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:61999CJ0453

Ac. do Supremo Tribunal Administrativo, de 17/01/2008, n.º de processo 0896/07, https://www.dgsi.pt/jsta.nsf/35fbbbf22e1bb1e680256f8e003ea931/7a11a8ad079aebc9802573de00374730?OpenDocument

Ac. do TJUE, de 07/05/2009, n.º de processo C-553/07, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62007CJ0553

Ac. do TJUE, de 05/05/2011, n.º de processo c-543/09, https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A62009CJ0543

Ac. do TJUE, de 19/10/2016, n.º de processo C-582/14, disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62014CJ0582

Ac. do Tribunal da Relação do Porto, de 24/01/2022, n.º de processo 3328/19.2T8STS-A.P1,https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/8fffb6004be424798025880100330de4?OpenDocument&Highlight=0,LEI,N.%C2%BA,58%2F2019,DE,08.08.

Ac. do Tribunal da Relação de Lisboa, de 02/05/2023, n.º de processo 12234/21.0T8LSB.L17,https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/6b57c49941d5779f802589aa0049be2a?OpenDocument.

## NETOGRAFIA

COMISSÃO EUROPEIA, *A União Europeia*, acedido e consultado em 14/08/2024, disponível em *https://portugal.representation.ec.europa.eu/quem-somos/uniao-europeia_pt*

COMISSÃO EUROPEIA, *Mercado Único Digital*, acedido e consultado em 14/08/2024, disponível em https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_pt#policy-areas

COMISSÃO NACIONAL DA PROPETÇÃO DE DADOS (CNPD), *O que somos e quem somos*, acedido e consultado em 14/08/2024, disponível em https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/

ONU em https://unric.org/pt/historia-da-onu/

MAC FREE, *O que é uma firewalls?* acedido e consultado a 20/08/2024, disponível em *https://www.mcafee.com/pt-pt/antivirus/firewall.html*

HOSTINGER, *O que é a criptografia?*, acedido e consultado a 20/08/2024, disponível em *https://www.hostinger.pt/tutoriais/o-que-e-criptografia?ppc_campaign=google_search_generic_hosting_all&bidkw=defaultkeyword&lo=20879&gad_source=1&gclid=CjwKCAiAopuvBhBCEiwAm8jaMVLCtH1Kyo4YXzPLO5u4Q07o3L5aDamLmORqbFwCK2Gc8zCSZoQqgxoCSMwQAvD_BwE*