DEPARTAMENTO DE DIREITO

MESTRADO EM DIREITO

ESPECIALIDADE EM CIÊNCIAS JURÍDICAS

UNIVERSIDADE AUTÓNOMA DE LISBOA

"LUÍS DE CAMÕES"

PROTEÇÃO DE DADOS: O DIREITO À PRIVACIDADE NA ERA DIGITAL

Dissertação para a obtenção do grau de Mestre em Direito

Autora: Adélcia Solange Pereira Gonçalves da Veiga

Orientadores: Professor Doutor Pedro Gonçalo Tavares Trovão do Rosário

Mestre Maria de Lurdes Videira Sequeira Dias Alves

Número da candidata: 30001505

Março de 2020

Lisboa

Dedicatória

À Ernestina Gonçalves, minha querida mãe.

Ao Adriano, meu amor.

Aos meus avós (…), meus irmãos e cunhadas.

Agradecimentos

Agradeço a Deus que sempre esteve ao meu lado durante toda a minha caminhada nesta estrada árdua e me tem ajudado a ultrapassar todos os desafios que me propus, com dedicação, amor e empenho.

A minha Mãe, Ernestina Gonçalves, companhia de todas as horas. Exemplo de integridade, dona de uma força sem igual e um coração invejável. A ti, devo tudo mãe!

Um agradecimento especial ao Adriano, meu amor, meu porto seguro, por ter acreditado sempre em mim e ter percebido os meus momentos de insegurança e nunca me deixar desistir. O teu amor tem feito de mim uma pessoa mais forte.

Aos meus orientadores, Doutor Pedro Trovão do Rosário e Mestre Lurdes Dias Alves, por todas as vossas ajudas, disponibilidade e por dividirem comigo um pouco da vossa sabedoria. A vossa orientação foi fundamental durante todo o trabalho.

Aos meus irmãos, Adilson Veiga, Belarmiro Veiga e Mireida Veiga, aos meus avós (…), à minha cunhada (…), aos familiares e amigos, em geral, que com suas particularidades contribuíram de forma inegável para a minha formação e o meu crescimento como pessoa, despertando uma versão melhor de mim.

Obrigada a todos pelo apoio, pela paciência e compreensão nas horas difíceis. Não existem palavras suficientes para agradecer o tempo que vos roubei.

Epígrafe

"O êxito da vida não se mede pelo caminho que conquistamos, mas sim pelas dificuldades que superamos ao longo do caminho."

Abraham Lincoln

Resumo

A atual sociedade digital, por alguns «*mundo de vidro*» e «*pessoas eletrónicas*», caracterizada por avanços tecnológicos sem precedentes, pelo acesso rápido às informações e tratamento automatizado dos dados, veio alterar significativamente a forma como nós nos relacionamos com os outros e vemos o mundo.

As redes sociais e as plataformas de compras e pagamentos eletrónicos constituem as faces mais visíveis desta sociedade digital. Nelas são depositadas diariamente, pelos seus utilizadores, grandes quantidades de dados pessoais, sem que os seus titulares tenham preocupação com a segurança dos mesmos, deixando, na maioria dos casos, os seus dados na dependência de plataformas digitais, acreditando que não farão uso ilícito dos mesmos, colocando em risco o seu direito à privacidade.

Face a esta nova realidade, a proteção dos dados pessoais e a garantia dos direitos pessoais, com particular atenção para o direito à privacidade, se afigura entre os maiores desafios das atuais sociedades políticas e seus poderes, uma vez que os ordenamentos jurídicos terão de encontrar fronteiras de equilíbrio e conciliar valores, na maioria dos casos, considerados antagónicos, como a liberdade, a segurança, a privacidade, entre outros.

Com a chegada da Internet, esses desafios tornaram-se ainda mais complexos e ingentes, porquanto o elemento geográfico do Estado, isto é, as fronteiras físicas diluíram-se, o que requer respostas inovadoras, quer em termos normativos quer em termos institucionais. Veja-se que os direitos pessoais, particularmente o direito à privacidade, constam da Declaração Universal dos Direitos Humanos, instituída a 10 de dezembro de 1948, pela Organização das Nações Unidas.

É neste sentido que a maioria das constituições nacionais, no caso particular a Constituição da República Portuguesa, introduziu tais direitos fundamentais nos seus textos constitucionais. Foi assim que em 1995, a União Europeia, através do seu Parlamento, aprovou a Diretiva 95/46/CE, de 24 de outubro, um instrumento importante, na medida em que impele os Estados-membros para a necessidade e importância de se proteger as informações e garantir os direitos pessoais, dentro e fora da União Europeia, evitando o tratamento e utilização

abusivos dos dados pessoais por terceiros, acautelando igualmente o direito à privacidade e à vida privada.

Outros instrumentos normativos e instituições igualmente importantes, quais sejam a Lei nº 67/98, de 26 de outubro, a Lei de Proteção de Dados Pessoais, o Regulamento Geral de Proteção dos Dados e a Comissão Nacional de Proteção de Dados, em Portugal, se apresentaram como importantes e determinantes em matéria de proteção de dados e, em consequência, na defesa desses direitos fundamentais.

Estes e outros instrumentos, anteriormente referidos, vieram colmatar algumas lacunas antes existentes, em razão até das características da atual sociedade digital e de novas realidades, em que os dados se transformaram numa nova matéria-prima, podendo ser comercializados em mercados transfronteiriços. Pois, as informações se «*converteram na nova matéria-prima*» importante para a criação e definição do perfil dos consumidores.

Palavras-chave: proteção de dados pessoais; privacidade; tratamento; mercado de dados.

Abstract

The current digital society, also known as «*glass world*» and «*electronic people*», characterized by unprecedented technological advances, quick access to information and automated data processing, which has significantly changed the way we relate to others and see the world.

Social networks, electronic purchasing, and payment platforms are the most visible faces of this digital society. Large amounts of personal data are stored daily by their users, without being concerned about the security of their data, leaving, in most cases, their data on digital platforms, believing that the digital platforms will not make illicit use of them, with prejudice to their right to privacy.

Given this new reality, data protection and the warranty of personal rights, with particular focus on the right to privacy, appears among the greatest challenges of current political societies and their competencies, since the legal systems will have to find boundaries of balance and reconcile values such as freedom, security, privacy, among other values, in most cases, considered incompatible.

With the arrival of the Internet, these challenges have become even more complex and immense, as the geographical elements of the State, the physical boundaries have been watered down, which requires innovative responses, either in normative or institutional terms.

It should be noted that personal rights, particularly the right to privacy, are outlined in the Universal Declaration of Human Rights, established on 10 December 1948 by the United Nations. It is in this sense that most national constitutions, in the case of Portugal and Cape Verde, have introduced such fundamental rights into their constitutional texts.

Thus, in 1995, the European Union, through its Parliament, approved the Directive 95/46/EC, of 24 October, an important instrument, as far as it impels the Member States to the need and importance of data protection and the warranty of personal rights, inside and outside the European Union, preventing the processing and/or abusive use of personal data by third parties and also safeguarding the right to privacy and private life. Other legal instruments also important institutions, such as Law No. 67/98 of 26 October 1998, the Law on Personal Data

Protection, the General Data Protection Regulation, and the National Data Protection Commission in Portugal, have presented themselves as important and determining factors in terms of data protection and, consequently, in the defence of these fundamental rights.

These and other instruments aforementioned have filled some of the gaps that previously existed, due even to the characteristics of the actual digital society and new realities, in which data have become a new raw material and can be marketed in cross-border markets. The information has, therefore «*become the new raw material*» important for creating and profiling consumers.

Keywords: personal data protection; privacy; processing; data market.

Índice

Dedicatória 2

Agradecimentos 3

Epígrafe 4

Resumo 5

Abstract 7

Lista de Siglas e Abreviaturas 11

Introdução 13

Capítulo I 18

Evolução Legislativa do Direito à Proteção de Dados e à Privacidade no Ordenamento Jurídico Português 18

1.1 Contextualização 18

1.2 Constituição da República Portuguesa 19

1.3 A Diretiva 95/46/CE, de 24 de outubro 24

1.4 A Lei nº 67/98, de 26 de outubro: Lei de Proteção de Dados Pessoais 27

1.5 Regulamento Geral de Proteção dos Dados 30

Capítulo II 34

O Direito à Privacidade 34

2.1. O Conceito de Privacidade e Intimidade 34

2.2. Direito à Privacidade enquanto Direito Fundamental 37

2.3. O Desrespeito pelo Direito à Privacidade na Era Digital 41

Capítulo III 44

Conflitos entre os Direitos Fundamentais e a Proteção de Dados Pessoais 44

3.1. Proteção de Dados e Direito à Privacidade 47

3.2. Direito à Privacidade e à Segurança dos Dados 48

3.3. Direito à Privacidade e à Informação 50

3.4. Direito à Privacidade e Consentimento 51
Capítulo IV 54
A Nova Geração de Direitos dos Titulares de Dados 54
4.1. O Direito à Informação e Acesso aos Dados 54
4.2. O Direito à Retificação dos Dados 56
4.3. O Direito à Portabilidade de Dados Pessoais 58
4.4. Direito de Oposição ao Tratamento de Dados 59
4.5. O Direito à Limitação do Tratamento de Dados 61
4.6. Os Princípios Fundamentais de Tratamento dos Dados 62
4.6.1. Princípio da Licitude, Lealdade e Transparência 63
4.6.2. Princípio do Propósito Limitado 65
4.6.3. Princípio da Segurança dos Dados 66
4.6.4. Princípio da Responsabilidade 67
Capítulo V 69
O Mercado de Dados Pessoais 69
5.1. Os Dados Pessoais como Nova Matéria-Prima 69
5.2. Transferência de Dados para Países Terceiros 80
5.3. Fiscalização e Sanções 89
Conclusão 95
Bibliografia 99
Bibliografia Consultada não Citada 101
Índice Remissivo 107

Lista de Siglas e Abreviaturas

Ac.	Acórdão
AIPD	Avaliação de Impacto sobre a Proteção de Dados
Al) /al)	Alínea, alínea
AR	Assembleia da República
Art.º art.º	Artigo, artigo
CADH	Convenção Americana dos Direitos Humanos
CC	Código Civil
CDFUE	Carta dos Direitos Fundamentais da União Europeia Comentada
CE	Conselho Europeu
CEDH	Convenção Europeia dos Direitos do Homem
CJ	Coletânea de Jurisprudência
CNPD	Comissão Nacional de Proteção de Dados
CRP	Constituição da República Portuguesa
DPO	*Data Protection Officer* (em português EPD - Encarregado de Proteção de Dados)
GT 29º	Grupo de Trabalho do Artigo 29º
LPDPPS	Lei da Proteção de Dados Pessoais e Pessoas Singulares
LPDP	Lei de Proteção de Dados Pessoais
ONU	Organização das Nações Unidas

RGPD	Regulamento Geral de Proteção de Dados
SS	Seguintes
UE	União Europeia

Introdução

As tecnologias de informação e comunicação vieram revolucionar as sociedades modernas e os seus integrantes. Na verdade, moldaram a forma como as pessoas se relacionam, quebraram as barreiras físicas e encurtaram as distâncias entre elas, tornando o mundo, de facto, plano em que pessoas entre continentes, países, cidades ou ruas diferentes podem fazer compras, encomendar comidas, fazer reservas de hotéis, comprar bilhetes de viagens ou concertos, realizar reuniões ou mesmo trabalhar sem saírem de casa, precisando apenas ter um equipamento ligado à Internet. Não será, pois, abusivo afirmar que a par da globalização económica passamos a assistir à globalização digital e a criação de um mundo virtual e das sociedades em redes.

Na verdade, as informações passaram a ser partilhadas a uma velocidade frenética de computador em computador, *Smartphones* em *Smartphones* de terceira e quarta gerações (estando já prevista a quinta geração) e de país em país, pondo em perigo o direito à privacidade.

Pois, deixou-se de falar e viver num pequeno mundo para se passar a viver num mundo virtual, sem fronteiras de qualquer espécie, em que tudo possa estar ao alcance de todos, para isso bastando um clique, e com ganhos em termos de comodidade e rapidez, em que certas tarefas do quotidiano, outrora complexas e morosas, passaram a ser realizadas de forma rápida e cómoda. Por isso, são evidentes os ganhos na saúde com a telemedicina, na educação, no comércio e nas transações internacionais, com os terminais eletrónicos de pagamentos e o *Internet Banking*, entre outros ganhos evidentes na área da inteligência artificial.

Porém, seria de uma ingenuidade primária não reconhecer as consequências nefastas que as tecnologias de informação e comunicação têm trazido para as pessoas, especialmente no que concerne à proteção dos seus dados e, em consequência, ao direito à privacidade e à intimidade. Daí um apelo permanente ao direito à privacidade e à necessidade de se controlar a difusão das informações que dizem respeito às pessoas, podendo viver sem serem observadas e, igualmente, o direito ao esquecimento.

Neste sentido, há que fazer uma adaptação do Direito a esta nova realidade e fazer face aos novos desafios, de forma a impedir que o mundo digital seja visto ou se transforme num lugar sem regras, em que a transgressão, não dá lugar a responsabilidade civil e/ou criminal.

Com o tema, "*Proteção de Dados: O Direito à Privacidade na Era Digital*" pretende-se, por um lado, saber em que medida as «*novas*» tecnologias de informação e comunicação tornaram os utilizadores mais expostos à utilização abusiva dos seus dados por terceiros (entidades, instituições, empresas e/ou particulares) e, por outro perceber se as medidas normativas e institucionais existentes garantem a proteção efetiva dos dados pessoais e permitem, em caso de sua utilização abusiva e indevida, responsabilizar civil e/ou criminalmente o infrator.

Justificação do tema

Atualmente, muitos dados pessoais são registados informaticamente e circulam pelos sistemas virtualmente sem limites temporais ou espaciais. O uso de meios eletrónicos (cartões de crédito, via verde, telemóveis, etc.…) fornece constantemente ao sistema, informações sobre a vida dos indivíduos. Ao se criar uma conta na Internet, realizar compras *online*, ou efetuar pesquisas nos motores de buscas, deixam-se registados dados de natureza pessoal (fotografias, moradas, nomes, números de telefones e de contas bancários, entre outros dados), que ficam à disposição do público em geral, podendo deles fazer uso indevido e ilícito, colocando em perigo a privacidade, violando, desta forma, o direito à privacidade e à intimidade.

Pois, qualquer indivíduo pode introduzir dados pessoais ou de um terceiro no mundo digital. As empresas recolhem os dados disponibilizados no mundo digital, armazenam os dados pessoais dos consumidores, o que lhes permite saber os gostos e as necessidades individuais, podendo, a partir destes dados, fazer o "*marketing one to one*", direcionando as suas ofertas e produtos a grupos sociais ou indivíduos bem determinados.

Assim, a escolha deste tema justifica-se essencialmente pela proteção da personalidade humana na atual sociedade de informação e era digital, em que a proteção dos dados pessoais e, em consequência, o direito à privacidade face o avanço tecnológico e suas consequências, em parte nefastas, será um desafio ingente, já que os alvos são essencialmente os direitos fundamentais. Pois, a natureza destes direitos, inerentes a própria existência da pessoa, obriga a que sejam tomadas medidas objetivas (normativas e outras) que permitam a conjugação da convivência social no atual mundo virtual com a necessidade da proteção de dados pessoais, do direito à vida privada ou à «*intimidade pessoal*», o que constituirá certamente um desafio para

os Estados modernos, considerando que são suas funções garantir a segurança, a justiça, o bem-estar e a paz social dos seus membros.

Para se fazer face a estas violações de direitos de personalidades, de modo a permitir que os indivíduos possam disfrutar das vantagens das tecnologias de informação e comunicação com segurança e garantia de proteção efetiva do seu direito à privacidade, pensa-se ser urgente, não só a criação de leis, mas também e sobretudo de mecanismos que permitam um controlo rigoroso de recolha, tratamento e partilha em segurança dos dados pessoais, capaz de dissuadir e punir qualquer desvio ou prática que possa configurar na violação de dados pessoais e consequentemente da privacidade e intimidade da pessoa.

Problemática

Neste trabalho propõe-se identificar e analisar a dificuldade demonstrada pelas instituições de proteção de dados pessoais em proteger de forma efetiva e segura os dados pessoais e garantir o direito à privacidade dos utilizadores dos dispositivos eletrónicos com ligação à Internet, por escassez ou imprecisão normativa. Para tanto, começa-se por observar e analisar as relações que se estabelecem entre a era digital, ou melhor, a utilização das tecnologias de informação e comunicação e a necessidade de proteção dos dados e a garantia do direito à privacidade. É neste sentido que são formuladas hipóteses que deveram apontar possíveis respostas às questões centrais do presente trabalho.

Assim, as perguntas de base levantadas são as seguintes:

I - As tecnologias de informação e de comunicação e, sobretudo, a Internet, diferencial da era digital, terão alterado a fronteira da vida privada, com prejuízos para o direito à privacidade?

II - Os mecanismos institucionais (DPO; CNPD) existentes, em especial os normativos (DUDH; CRP; Diretivas; Leis e RGPD) são suficientes face aos desafios da atual sociedade de informação (mundo digital) em matéria de proteção de dados pessoais e, em consequência, o direito à privacidade, considerando inclusive novos direitos como, o direito ao esquecimento, à oposição do tratamento e o direito à limitação de tratamento de dados pessoais?

Estrutura da Dissertação

Estas são algumas questões e hipóteses que se propõe responder e verificar ao longo dos capítulos que compõem a presente dissertação.

Assim, no capítulo I é feita a definição dos conceitos em estudo (Proteção, Dados, Privacidade e Era Digital). De seguida, será feita uma resenha histórico-jurídica da proteção de dados e do direito à privacidade. Os danos eventuais causados ao direito à privacidade e a sua eventual colisão com outros direitos fundamentais, bem como a importância do princípio da proporcionalidade.

No capítulo II, proceder-se-á a análise da comunicação de privacidade feita pelo próprio indivíduo e o seu autocontrole. Igualmente, a revelação voluntária da privacidade e o impacto das redes socias no direito da família, no âmbito laboral; o direito penal, com especial atenção para a questão do direito ao esquecimento e, por fim, a tutela jurídica na era digital.

O capítulo III será dedicado à compreensão da problemática dos dados no mundo digital. Relacionar-se-ão os dados e a inteligência artificial. Análise e tratamento dos dados na Internet. De seguida, será discutida a portabilidade dos dados, sua transferência para os países terceiros e o respeito e garantia do direito à privacidade.

No capítulo IV, vai se estudar os dados como uma nova matéria-prima, sua implicação na vida privada, com particular atenção para a necessidade de se encontrar o equilíbrio necessário entre os interesses económicos e a garantia dos direitos fundamentais dos titulares de dados.

O capítulo V, o último capítulo, será dedicado à fiscalização e sanções. Serão identificadas e analisadas as sanções e coimas a que ficarão sujeitos os responsáveis pelo tratamento de dados pessoais, em caso de não observarem o estatuído nas legislações de proteção de dados, assim como os meios de tutela dos direitos dos titulares de dados, em caso de violação dos seus direitos.

Finalmente, a conclusão mostrará em que medida a investigação conseguiu responder à problemática inicialmente formulada e que orientou toda a nossa investigação.

Metodologia

Para elaboração da presente dissertação optou-se por uma metodologia que contemple várias técnicas de recolha de informação, como "*a documentação indireta*"[1] com destaque para a pesquisa documental e bibliográfica sobre a problemática da proteção de dados e do direito à privacidade na atual era digital.

Na verdade, a escolha da metodologia a utilizar depende sempre da natureza da problemática em estudo. Assim, deve-se recorrer, com alguma frequência, a materiais já publicados sobre a temática em estudo, em revistas e materiais normativos, isto é, legislações publicadas, com destaque para Declaração Universal dos Direitos Humanos, a Constituição da República Portuguesa, as Diretivas, as Leis e o Regulamento Geral de Proteção de Dados, sem se esquecer de outros documentos igualmente importantes com publicações periódicas sobre o assunto, quais sejam Revistas, Anuários, entre outros documentos de igual relevância e rigor científico e documental.

A pesquisa documental e bibliográfica foi realizada em várias bibliotecas universitárias e não só, em Portugal e em Cabo Verde. Convirá, no entanto, acrescentar que boa parte da bibliografia utilizada na elaboração desta dissertação foi adquirida, considerando as circunstâncias da mestranda e condicionante de ter de escrever o trabalho em Cabo Verde, já que por razões familiares teve de regressar ao país de origem.

Por fim, importa referir que no respeitante às regras de citação e referências bibliográficas, se optou por seguir a norma da *American Psychological Association*, conforme estatui o Regulamento Geral de Apresentações dos Trabalhos de Mestrado e Doutoramento da Universidade Autónoma de Lisboa.

[1] Cf. Frada (1991, p. 72).

Capítulo I

Evolução Legislativa do Direito à Proteção de Dados e à Privacidade no Ordenamento Jurídico Português

1.1 Contextualização

A proteção dos dados pessoais e privacidade foram objeto de tratamento nos mais importantes instrumentos de direito do homem a nível internacional[2].

Assim, Declaração Universal dos Direitos do Homem, aprovada pela Assembleia-Geral das Nações Unidas, no dia 10 de dezembro de 1948, prevê no seu artigo 12º que "*ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação*."[3] Prevê ainda, que caso tais intromissões acontecerem, a pessoa tem direito a ser protegida pela lei. Tal preceito demonstra a importância do direito à privacidade, alertando desde já para a necessidade de sua garantia efetiva através da lei.

Igualmente, o Pacto Internacional relativo aos Direitos Civis e Políticos[4] estatui no seu texto semelhante preceito, regulando a defesa e garantia do direito à privacidade. No mesmo sentido dos documentos acima citados, a Convenção Europeia dos Direitos do Homem[5] veio reforçar, portanto, o direito à privacidade da pessoa, da família, seu domicílio e, igualmente, da sua correspondência, em consequência dos dados da pessoa.

Mais tarde, foi adotada a Convenção 108 do Conselho da Europa, um instrumento fundamental para a proteção das pessoas relativamente ao tratamento automatizado de dados de caracter pessoal[6], em que alguns dos princípios fundamentais de proteção de dados

[2] Marques, G. & Lourenço, M. (2006, p. 108).
[3] Cf. Declaração Universal dos Direitos do Homem, aprovada pela Assembleia-Geral das Nações Unidas, no dia 10 de dezembro de 1948, Artigo 12º.
[4] O Pacto Internacional foi aberto à assinatura a 19 de dezembro de 1966. Ratificado por Portugal através da Lei nº 29/78, de 12 de junho, que aprova para ratificação o Pacto Internacional sobre os Direitos Civis e Políticos, assinado em Nova Iorque a 7 de outubro de 1976, Artigo 17º.
[5] Cf. A Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais, assinada em Roma a 4 de novembro de 1950, e que entrou em vigor a 3 de setembro de 1953, Artigo 8º.
[6] Adotada em Estrasburgo, a 28 de janeiro de 1981.

consagrados na referida convenção vieram, posteriormente, integrar a Diretiva 95/46/CE, de 24 de Outubro, como são os casos dos princípios da finalidade, da adequação e da pertinência.[7]

Já a nível interno, particularmente no Ordenamento Jurídico português, o direito à privacidade e de proteção de dados, bem como os mecanismos de sua garantia, estão consagrados nos seguintes instrumentos:[8] a Constituição da República Portuguesa[9]; a Diretiva 95/46/CE, de 24 de Outubro; a Lei nº 67/98, de 26 de Outubro, Lei de Proteção de Dados Pessoais; e, por fim, o Regulamento Geral de Proteção dos Dados, a seguir analisados separadamente, no sentido de compreendermos o alcance e nível de segurança que estes instrumentos garantem em matéria de proteção de dados e do direito à privacidade.

1.2 Constituição da República Portuguesa

O direito à privacidade consta dos direitos pessoais fundamentais previstos na Constituição da República Portuguesa (CRP). No seu texto consagra vários direitos pessoais, como sejam o direito à identidade pessoal, garantindo inclusive "*a identidade genética do ser humano (…) na criação, desenvolvimento e utilização das tecnologias e na experimentação científica*", os direitos ao livre desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar, e o direito a proteção contra quaisquer formas de discriminação[10]. Estabelece ainda que "*são nulas as provas obtidas* [em razão da] *(…) abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações.*"[11]

Este facto é demonstrativo da natureza quase que sagrada desses direitos pessoais, como garantia da dignidade da pessoa, sendo por isso indispensável a sua proteção e observância.

---

[7]Castro, C. S e. (2005) *Direito da Informática, Privacidade e Dados Pessoais*. Coimbra: Edições Almedina, p. 40.
[8]Cf. A Constituição da República Portuguesa (2010 artigos 26º e 35º).
[9] Refira-se que o Código Penal nos seus artigos 190º "*a violação de domicílio*"; 191º "*a introdução em lugar vedado ao público"*; 192º *"a devassa da vida privada*"; 193º *"a devassa por meio de informática a violação de correspondência ou de telecomunicações*"; e nos artigos 194º, 195º e 196º *"a violação de segredo e o aproveitamento indevido de segredo*", prevê agravamento de quase todos esses crimes no caso de serem praticados através de meio de comunicação social, nos termos do art.º 197º, *al.* b). O Código Civil inclui também os direitos de personalidade, como seja o direito "*à reserva sobre a intimidade da vida privada"* previsto no seu artigo 80º.
[10] Cf. Constituição da República Portuguesa (2010, artigo 26º, nºs 1, 2 e 3).
[11] Cf. Constituição da República Portuguesa (2010, artigo 37º, nº 8).

Pois, a Constituição da República Portuguesa reconhece a inviolabilidade do domicílio, assim como a importância de se respeitar o sigilo da correspondência e outros meios de comunicação, considerando-os integrantes do direito a privacidade, um direito fundamental e indispensável à dignidade da pessoa e a vida em sociedade.

A C.R.P reconhece a todos os cidadãos o direito de acesso aos dados informatizados, reconhecendo-lhes ainda o direito de, em querendo, exigir a sua retificação, atualização ou mesmo o seu apagamento. Exige ainda que os titulares de dados sejam informados sobre a finalidade dos mesmos[12].

Com isto, fica evidente, portanto, a liberdade e a possibilidade objetiva que os titulares dos dados têm de, em querendo, poder controlar os seus dados e estar seguros dos fins a serem dados aos mesmos. Demostra também a importância que a CRP atribui à problemática da proteção de dados como condição e garante do direito à privacidade na era digital, tema central da presente dissertação e que será objeto de análise e discussão nos capítulos seguintes.

A Constituição da República Portuguesa (CRP) foi a primeira Constituição Europeia a consagrar a proteção de dados pessoais. Ora, a Constituição de 1976 já integrava no seu texto o direito especial de personalidade no sentido de proteger o cidadão dos perigos que pudessem resultar do uso da informática e na violação do direito a privacidade.[13]

De facto, a CRP, no artigo 35º, nº 1, determinava que "*Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização*."

A CRP não só reconhecia o direito de o cidadão tomar conhecimento dos seus dados registados e dos fins a serem dados aos mesmo, como proibia a utilização de informática "*para tratamento de dados referentes a convicções política, fé religiosa ou vida privada, salva quando se trate do processamento de dados não identificáveis para fins estatísticos*."[14]

[12] Cf. Constituição da República Portuguesa (2010, artigos 34º e 35º).
[13] https://www.cnpd.pt/bin/revistaforum/forum2016_2/files/assets/basic-html/page-53.html, consultada em 20 de novembro de 2019.
[14] Cf. Constituição da República Portuguesa (1976, artigo 35º, nº 3).

Por outro lado, não permitia que aos cidadãos fosse atribuído um número único de identificação, como forma de também preservar a identidade e garantir o direito à privacidade, enquanto direito pessoal e fundamental.

Importa observar que, apesar das sucessivas revisões feitas a CRP, sendo a 8ª e última em outubro de 2010, sempre se preservou o artigo 35º referente a "Utilização da informática", com significativa alteração textual, note-se mais amplo e completo, definindo dados pessoais e proibindo o acesso aos dados pessoais, somente em casos excecionais e em estrita observância da lei.

A CRP trouxe uma inovação oportuna em matéria de proteção de dados, ao prever sua utilização transfronteiriça, isto é, fora do país de residência do titular dos dados. Pois, face o direito de *"livre acesso às redes informáticas de uso público",* um direito constitucionalmente consagrado e os riscos associados a uma tal utilização de redes públicas de acesso, a CRP determinou que fosse definido por lei *"o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional*."[15]

Nota-se aqui uma clara preocupação com a proteção dos dados que os cidadãos disponibilizam em razão da necessidade de utilização das redes públicas da informática, podendo esses dados ficarem sujeitos a operações de tratamento para finalidades diversas, podendo resultar em prejuízos a vários níveis para os seus titulares e com riscos para a segurança e/ou interesse nacional. Assim, a CRP no artigo 35º, nº 7, estabelece que "*Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei*."

Fica, pois, evidente a preocupação do legislador em considerar novas realidades, nomeadamente a utilização das «*novas*» tecnologias de informação e comunicação, criando as condições para que a circulação, partilha e tratamento de dados se façam também fora do espaço geográfico nacional.

[15] Cf. Constituição da República Portuguesa (2010, artigo 35º, nº 6).

A CRP consagra um conjunto de direitos fundamentais com vista a impedir que a pessoa seja encarrada como um "*simples objeto de informação"*[16]. Com efeito, reconhecer o direito de acesso aos dados pessoais, de solicitar a sua retificação e atualização, poder eliminá-los, quando incorretos ou sujeitos a tratamento proibido, o direito de conhecer a finalidade a que se destinam os dados objeto de tratamento.

Ao reconhecer esse conjunto de direitos e os atribuir proteção constitucional, atesta a especial atenção atribuída ao *"direito a autodeterminação informacional"* e garantir a que *"cada um o direito de controlar a informação disponível a seu respeito*" (Canotilho & Moreira (2014, p. 551).

A CRP prevê o tratamento de dados pessoais, sua transmissão e utilização, colocando restrições ao tratamento de dados pessoais respeitantes às convicções filosóficas, políticas, filiação partidária ou sindical e fé religiosa, sobre a vida privada e origem étnica[17], como forma de proteger a privacidade, a intimidade e a vida privada dos titulares dos dados.

A CRP (1997)[18] vem esclarecer e aprofundar alguns princípios fundamentais já considerados na Constituição de 1976[19], admitindo que a lei possa autorizar o tratamento de dados pessoais relativos a convicções filosóficas, políticas, filiação partidária ou outras, desde que sejam apresentadas as garantias de não discriminação.

Importa referir que o tratamento desses dados só será permitido mediante consentimento expresso do seu titular e em observância da Lei. Com efeito, deve ser assegurando ao titular dos dados as garantias de não discriminação, ou então que o processamento de dados seja exclusivamente para fins estatísticos.

[16] Castro, C. S. e, (2004, p. 214).
[17] A Lei de Proteção de Dados, no seu artigo 7º, nº 1 veio reafirmar a limitação ao tratamento de dados sensíveis como a convicções filosóficas ou políticas, filiações partidárias ou sindical, fé religiosa, vida privada e origem étnica.
[18] Aprovada pela Lei Constitucional nº 1/97, de 20 de setembro, publicada no Diário da República nº 218/197, Série I-A de 1997-09-20.
[19] Canotilho & Moreira (2014, p. 185).

Como já se disse anteriormente, a Constituição de 1997, no artigo 35º, nº 4, proibia o aceso de terceiros[20] a dados pessoais. Proibição que, segundo Castro (2005, pp. 33-34), deve ser entendida num sentido amplo, porquanto a mesma pretende impedir que "*informações prestadas a um particular ou entidade possam ser por estes divulgadas a outras pessoas, concedendo a terceiros o acesso aos dados tratados e que possam ser usados para finalidades diversas daquela que esteve na origem do seu tratamento*."

Ainda sobre esta proteção constitucional de dados pessoais, defendem Canotilho & Moreira (2014, p. 185) "*nada mais é que a consequência lógica do alargamento do âmbito de proteção, regulando a proteção de todos e quaisquer dados pessoais, merecendo, por isso, os ficheiros manuais uma proteção idêntica à prevista no texto constitucional para os ficheiros automáticos*."

O alargamento do âmbito de proteção dos dados pessoais, no sentido de garantir o direito a privacidade e a vida privada, tem sido realizado através de introdução e reconhecimento de novos direitos, alargando assim o leque dos direitos fundamentais.

O reconhecimento de novos direitos, de que é exemplo o direito a autodeterminação informacional, com igual valor constitucional tem gerado algum conflito entre direitos fundamentais, desafiando os Estados e seus poderes a introduzirem nos dispositivos normativos, como é o caso da Diretiva 95/46/CE, de 24 de outubro, e a atualizarem os já existentes, introduzindo novos princípios, com especial destaque para o princípio da proporcionalidade e da razoabilidade, como forma de garantir direitos opostos, de que são exemplos, o direito a informação ou mesmo a liberdade de expressão com o direito a privacidade.

Na verdade, são preceitos constitucionais, relativos a direitos fundamentais, com aplicação direta e que vinculam todas as entidades públicas e privadas por força do artigo 18º da CRP, só podendo ser restringidos ou limitados nas situações previstas na lei, *"devendo limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos."* Pois, a CRP só permite que a lei possa restringir os direitos em situações especiais

[20] Segundo Canotilho & Moreira (2014), "a noção de terceiros deve abranger todas as pessoas, (…) o pessoal informático que a lei ou os códigos deontológicos considerem responsável pelo ficheiro deve estar sujeito a um dever de sigilo profissional, já previsto na Lei."

e previstas na Constituição, quando seja para garantir outros direitos. Mesmo assim, esta restrição deve "*limitar-se ao mínimo necessário*", deixando aqui em evidência a obrigatoriedade de se ter em devida conta o princípio da proporcionalidade, que será analisado no capítulo III.

1.3 A Diretiva 95/46/CE, de 24 de outubro

Neste subcapítulo vai-se analisar a Diretiva 95/46/CE, de 24 de outubro, o primeiro instrumento jurídico do Parlamento Europeu direcionado à proteção de dados pessoais singulares, seu tratamento e à livre circulação desses dados.

A diretiva proporcionou a cada Estado-membros a possibilidade de transcrever, com alguma liberdade, o seu conteúdo, o que acabou por se traduzir numa produção avulsa de legislação sobre a proteção de dados, originando uma aplicação não uniforme pelos países da União Europeia (EU), gerando assim, uma insegurança jurídica que, para alguns, não favoreceu o desenvolvimento da economia.

Entretanto, como forma de harmonizar um conjunto de leis dos Estados-membros, que já legislavam sobre essa matéria, foi aprovar uma diretiva, com a finalidade de tornar o nível de proteção dos direitos e liberdades das pessoas, no que diz respeita ao tratamento de dados, equivalente em todos os Estados-membros.

A Diretiva 95/46/CE, de 24 de outubro, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, veio procurar conciliar o direito à informação com o direito à circulação de informação. Na verdade, influenciou decisivamente o panorama do direito interno de todos os países da União Europeia, obrigando-os a adoção de normas jurídicas de proteção de dados pessoais, onde não as havia, e uniformizando o nível de proteção em todos os Estados- membros.

Estabelecido esse nível comum de proteção de dados pessoais, a circulação da informação e pessoa passou a ser livre entre Estados-membros, obedecendo, porém, especiais requisitos, quando exportados para países terceiros.[21]

A Diretiva 95/46/CE, de 24 de outubro, além de contribuir para a harmonização normativa nos Estados membros visava igualmente "*a proteção das liberdades e dos direitos fundamentais das pessoas singulares*", em especial "*o direito à vida privada, no que diz respeito ao tratamento de dados pessoais*", como também "*restringir ou proibir a livre circulação de dados pessoais entre Estados-membros por razoes relativas à proteção de dados*"[22] como forma de proteger alguns valores considerados fundamentais como seja a liberdade e a privacidade.

Contudo, deve-se realçar que os objetivos acima referidos mereceram posição e opiniões e leituras distintas, em alguns casos divergentes.

Para uns, a referida diretiva tem como objetivo proteger os direitos dos cidadãos, em particular a sua privacidade face à informática. Outros defendem que seu objetivo esgota na procura e obtenção de equilíbrio entre a exigência da circulação da informação e da proteção dos particulares em relação aos dados e atividades a eles ligadas.

Houve quem tivesse defendido que o objetivo da Diretiva 95/46/CE, de 24 de outubro, foi o de flexibilização da informação, enquanto instrumento do progresso económico, como é o caso de Marques & Lourenço (2000, p. 266) quando escrevem que *"o que se pretende com a referida diretiva não é de todo regular a proteção das pessoas em tal contexto, mas sim eliminar o travão que aquela proteção representa para a livre circulação dos dados*."

Todavia, entende-se que, contrariamente ao que estabelece a Convenção 108 do Concelho da Europa, o objetivo da Diretiva 95/46/CE, de 24 de outubro, consiste na proteção das pessoas face os riscos advenientes da utilização descontrolada e abusiva dos seus dados, como consta dos artigos 1º e 2º do referido normativo aprovado pelo Parlamento e Conselho Europeu.

[21] Castro, C. S. e (2006, pp. 9-15).
[22] Cf. Diretiva 95/46/CE, de 24 de outubro, artigo 2º.

O âmbito da aplicação da Diretiva 95/46/CE, de 24 de outubro, é outra questão que irá ser analisada, como se fará a seguir.

A Diretiva 95/46/CE, de 24 de outubro, aplica-se a todo tratamento automatizado de dados pessoais contidos ou não em ficheiros. Em relação ao tratamento de dados sensíveis, a referida diretiva estatuiu que "*os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosófica, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual*."[23] Uma proibição que, como já se referiu anteriormente, consta também da Constituição da República Portuguesa.

Ainda sobre o âmbito da aplicação deste normativo comunitário, foi possível identificar opiniões divergentes. Existem vozes que afirmam que a proibição do tratamento desses dados deve-se a uma especial vulnerabilidade existente, uma vez que a partir dos referidos dados é possível adotar decisões discriminatórias, suscetíveis de causar aos seus titulares graves prejuízos, embora admitam que o consentimento seja a primeira exceção à proibição ao tratamento de dados pessoais.

Na verdade, a diretiva, no que diz respeito ao consentimento, prevê e determina que se deve respeitar e proteger os direitos à integridade moral do titular dos dados, conforme o estabelecido no artigo 25º da CRP e artigo 70º do Código Civil português, respetivamente, normas de *"aplicação imediata"* nos termos do artigo 18º da CRP, "*Força jurídica*".

No que se refere ao requisito do "*consentimento informado",* a diretiva não definiu uma tramitação rígida para o efeito, nem para a prestação da informação, nem para a recolha do consentimento. Todavia, entende-se ser indispensável, em qualquer caso, que a informação seja suficiente para que o consentimento seja considerado esclarecido. Pois, a informação quer oral ou escrita tem de exprimir em linguagem corrente e conter elementos iguais àqueles que um cidadão de padrão médio, no caso concreto, julgaria necessário para tomar qualquer decisão, e prestado para cada ato de tratamento de dados. Assim, conseguiu-se, portanto, inferir que a informação suficiente é um dos requisitos bastante para a validade do consentimento. Pelo contrário, se a informação não for suficiente o processamento efetuado para o tratamento dos

[23] Cf. Diretiva 95/46/CE, de 24 de outubro, artigo 8º, nº 2.

dados passa a ser considerado como não autorizado, tendo as correspondentes consequências civis e penais.[24]

Importa, porém, referir que a temática do consentimento será objeto de análise mais à frente, em subcapítulo próprio.

1.4 A Lei nº 67/98, de 26 de outubro: Lei de Proteção de Dados Pessoais

A Lei da Proteção de Dados Pessoais (Lei nº 67/98, de 26 de outubro), outra legislação importante em matéria de proteção e tratamentos dos dados, na medida que vai permitir a transposição da Diretiva 95/46/CE, de 24 de outubro, para a ordem jurídica interna, contribuindo para o reforço dos normativos já existentes esta matéria.

A referida lei veio reforçar e estabelecer um conjunto de princípios, como sejam *"o tratamento de dados pessoais de forma lícita; da recolha para finalidades específicas; dados adequados e pertinentes; dados exatos e conservados de forma a identificar os seus titulares"*[25], enfim um leque alargado de princípios que, mais tarde serão objeto de análise e tratamento mais detalhado.

A nova lei sobre a proteção de dados pessoais vem reconhecer e alargar os direitos dos titulares de dados, com destaque para *"o direito a proteção dos dados pessoais; o direito a informação, ao acesso, a retificação, ao apagamento, a não ficar sujeito a decisões individuais automatizadas"*[26], mais tarde aperfeiçoados pelo Regulamento Geral de Proteção de Dados.

Por outro lado, introduziu importantes inovações "*no âmbito de aplicação e a concretização dos princípios, das condições de legitimidade a observar no tratamento dos dados pessoais, bem como a segurança da informação, as transferências de dados para os países da e fora da União Europeia, transferindo as atribuições e competências de controlo de*

[24] Marques, G. & Lourenço, M. (2000). *Direito da Informática*. Coimbra: Edições Almeida, pp. 268-271.
[25] *Ibidem.*
[26] Cf. Lei nº 67/98, de 26 de outubro, *Lei de Proteção de Dados*, artigos 10º e ss.

dados para as autoridades, ou seja, as Comissões Nacionais de Proteção Dados." Marques & Lourenço (2000, pp. 271-273).

Uma das inovações importantes da nova lei da proteção de dados pessoais foi transferir para as autoridades nacionais, através das Comissões Nacionais de Proteção de Dados, todas as competências em matéria de controlo das operações que tenham como objeto dados pessoais.

Diferente do Regulamento Geral de Proteção de Dados, cujas competências estão viradas para "*organizações de controlo europeias, deixando para as jurisdições nacionais a adequação do às autoridades locais*"[27], como se verá no subcapítulo seguinte dedicado a análise do Regulamento geral de tratamento de Dados, a Comissão Nacional de Proteção de Dados é uma entidade administrativa independente, com o fundamento jurídico-constitucional na Constituição, desde a revisão da constitucional de 1997.[28]

A Comissão Nacional de Proteção de Dados (CNPD), cuja natureza e a competência estão definidas na Lei 67/98, de 26 de outubro, exerce funções consultiva, de representação internacional e pedagógica, como garantia e proteção dos direitos dos cidadãos.

A CNPD tem ainda competência para emitir pareceres, quer no âmbito da legislação nacional ou internacional, quando estejam em causa disposições relativas ao tratamento de dados.[29] Exerce igualmente funções de decisões administrativas e dispõe de poderes para autorizar tratamento de dados que devam ser objeto de autorização formal[30], dados para finalidades não determinadas na recolha, e autorizar as transferências e investigação de dados para fora da União Europeia.[31]

A Lei da Proteção de Dados Pessoais estatui no seu *"princípio geral"* que "*o tratamento de dados pessoais deve processar de forma transparente e no restrito respeito pela reserva da vida privada bem como pelos direitos, liberdades e garantias fundamentais*" e define dados como "*qualquer informação de qualquer natureza e independentemente do respetivo suporte incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável*",

[27] Saldanha (2018, p. 11).
[28] Cf. Constituição da República Portuguesa (1997, artigo 35º, nº 2).
[29] Cf. Lei nº 67/98, de 26 de outubro, *Lei de Proteção de Dados*, artigo 23.º nº 1.
[30] *Idem*, artigo 28º.
[31] *Idem*, artigo 20º.

considerando "*identificável a pessoa que por referência a um número de identificação ou mais elementos específicos da sua identificação física, fisiológica psíquica, económica, cultural ou social*."[32] No entanto, estas definições são elaboradas a partir das definições dadas pela Diretiva 95/46/CE, de 24 de outubro, no seu artigo 2º.

O âmbito de aplicação da Lei 67/98, de 26 de outubro é mais amplo, aplicando-se ao tratamento de dados pessoais por meio automatizado de forma total ou parcialmente, bem como ao tratamento por meios não automatizados, quando contidos em ficheiros manuais ou a estes destinados.[33] Abrange também a videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas.[34]

A referida lei aplica-se também às situações em que o tratamento ou a recolha de dados se faça fora do território nacional, através da internet, mas o responsável pelo tratamento tem a sede no território português[35] ou no caso em que o tratamento é feito por um responsável não estabelecido em Portugal, mas que recorra aos meios automatizados ou não automatizados situados em Portugal.

Pelo contrário, afirma Castro (2004, p. 55), "*a lei portuguesa não será aplicável quando o meio que serve de recolha de dados é um PC pertencente ao titular dos dados, que, por sua iniciativa, consulta uma pagina internet e envia as sua informações pessoais para um país terceiro, a fim de serem utilizadas por uma entidade não estabelecida em território onde a lei portuguesa seja aplicável, mesmo que esse titular se encontre em território português*."

Por isso, pode-se depreender que a lei portuguesa no que se refere a proteção dos dados pessoais tem-se revelado importante, especialmente por se apresentar um âmbito de aplicação bastante amplo, uma vez que regula recolha e tratamento de dados transfronteiriço realizados fora do território nacional, um dos grandes desafios em matéria de proteção de dados, sobretudo na atual era digital em que existe um fluxo de dados cada vez maior e uma diluição de fronteiras físicas entre os Estados, em ração da Internet e enorme e em crescimento contínuo.

[32] Cf. Lei nº 67/98, de 26 de outubro, *Lei de Proteção de Dados*, artigos 2º e 3º.
[33] Marques, G. & Lourenço, M. (2000, pp. 275-277).
[34] Cf. Lei 67/98, de 26 de outubro, *Lei de Proteção de Dados*, artigo 4º, nº 2.
[35] Castro (2004, p. 55).

Contudo, a lei portuguesa ao não se aplicar aos dados recolhidos a partir de um computador pessoal pertencente ao titular dos dados, ainda que esteja a residir no território nacional, poderá ter deixado algum espaço para acesso abusivo a dados pessoais ou mesmo seu tratamento indevido, isto é, sem o consentimento dos titulares, primeira exceção à proibição de tratamento de dados pessoais. Desta forma, a lei poderá ter transferido para os titulares de dados a responsabilidade maior em matéria da proteção dos seus dados pessoais.

Não obstante, a Lei nº 67/98, de 26 de outubro, contribuiu para reforçar as competências das organizações nacionais, no caso a CNPD, ajudou a esclarecer os conceitos de dados pessoais e de terceiros, alargando os direitos pessoais, introduziu de forma positiva vários princípios importantes, a começar pelo "*tratamento de dados pessoais de forma lícita; da recolha para finalidades específicas; dados adequados e pertinentes; dados exatos e conservados de forma a identificar os seus titulares,"*[36] enfim, um leque alargado de princípios, que merecerão uma análise e tratamento mais detalhado no ponto seguinte.

1.5 Regulamento Geral de Proteção dos Dados

Neste subcapítulo procura-se compreender e analisar o Regulamento Geral de Proteção de Dados, um dispositivo normativo relevante em matéria de tratamento de dados pessoais e sua circulação, que terá a finalidade de proteger todos os cidadãos dos Estados-membros contra as violações do direito à privacidade na era digital, matéria objeto de tratamento no capítulo seguinte.

O Regulamento Geral de Proteção de Dados, aprovado pela Lei nº 58/2019, de 8 de agosto, publicada no Diário da República nº 151/2019, Série I, de 8 de Agosto. Trata-se de um documento que irá permitir a transposição para a ordem jurídica nacional o Regulamento (UE) n.º 2016/679 do Parlamento e do Conselho Europeu, de 27 de abril de 2016, "*relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*."[37] Com efeito, o Regulamento Geral de Proteção de Dados (2016), doravante

[36] Cf. Lei 67/98, de 26 de outubro, *Lei de Proteção de Dados*, artigo 28º e ss.
[37] Cf. Lei nº 58/2019, de 8 de agosto, artigo 1º.

designado RGPD, vem revogar a Diretiva 95/46/CE e criar um quadro legal mais claro e coerente para a nova realidade.

A Lei nº 58/2019, de 8 de agosto "*aplica-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou subcontratante, mesmo que o tratamento de dados pessoais seja efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse pública*"[38]. Já aqui, nota-se que o presente regulamento alarga o seu âmbito de aplicação para além do território nacional, não se aplicando apenas "*aos ficheiros de dados pessoais constituídos e mantidos sob a responsabilidade do Sistema de Informação da República Portuguesa*", sendo este regulado por disposições legais próprias, previstas na lei.

O RGPD não se aplica apenas aos dados pessoais constituídos e mantidos dentro do espaço europeu. O seu âmbito de aplicação alarga-se aos dados transfronteiriços, abarcando todas as operações realizadas por empresas da União Europeia, ainda que com sede fora da união. Fica, desde logo, claro que o presente regulamento apresenta um âmbito de aplicação ainda mais alargado. Pois, a Lei nº 67/98, de 26 de outubro, aplicava-se também às operações de tratamentos ou recolhas de dados feitos fora do território nacional, mas, contrariamente ao RGPD, as entidades responsáveis tinham de ter a sua sede no território nacional.

Contrariamente à Diretiva 95/46, de 24 de outubro, com aplicação direta na ordem jurídica interna dos Estados-membros, o RGPD tem com principais objetivos: a harmonização legislativa; a coerência no tratamento dos dados pessoais em todo o espaço europeu; e a segurança jurídica. Para tanto, vai harmonizar e assegurar a defesa dos direitos e liberdades fundamentais das pessoas singulares e garantir a livre circulação de dados pessoais entre os Estados-membros, contribuindo para a realização de um espaço de liberdade, segurança e justiça.

Pontanto, este novo dispositivo normativo europeu terá uma aplicação uniforme em todos Estados da União Europeia, tendo em visa a proteção de pessoas singulares e seus dados

[38] Cf. Regulamento Geral de Proteção de Dados (2016, artigo 2º).

pessoais, enquanto direitos fundamentais, não se importando a nacionalidade ou local de residência.

O RGPD vem clarificar o conceito de dados pessoais, tornando-o mais abrangente, e consagrar novos direitos para os titulares de dados, como "*o direito à portabilidade; o direito ao esquecimento; o direito de oposição; o direito de receber informações claras e compreensíveis sobre o mesmo; o direito a transferir os dados.*"[39], bem como prever aplicação de sanções ou medidas corretivas (coimas, advertências ou ordens) às empresas responsáveis pelo tratamento de dados pessoais e subcontratantes, em caso de violações.

Importa observar, que apesar de se aplicar em toda a União Europeia, o RGPD permitia que os Estados-membros, caso fosse necessário, legislassem sobre questões ligadas a aplicação prática do referido regulamento, como, por exemplo, a organização interna da Comissão Nacional de Proteção de Dados, autoridade nacional de controlo de tratamento, proteção e circulação dos dados.

Esta evolução legislativa exigiu, da parte da União Europeia, a "criação de um quadro legal de proteção de dados pessoais e de uma aplicação rigorosa dessas mesmas regras, de forma a gerar a confiança necessária quer aos cidadãos, para disponibilizarem os seus dado, já que poderão ter um controlo sobre os mesmos, quer às organizações, no que toca ao desenvolvimento da economia digital no mercado interno da União Europeia." (Saldanha, 2018, p. 15)

Pois, já se fazia sentir a necessidade de uma legislação inovadora em matéria de proteção de dados, perante um "aumento dos fluxos transfronteiriços, em consequência, uma cada vez maior integração económica [e] da criação do mercado único e (…) um intenso intercâmbio de dados entre setores público e privado, resultado da evolução tecnológica contínua e uma globalização já imparável, [permitindo] uma maior recolha e partilha de dados pessoais por parte das organizações e empresas, tanto públicas como privadas, em que os dados pessoais passaram a ter um valor económico muito real e mensurável" (Saldanha, 2018, p. 15). De facto, os dados pessoais transformaram-se em nova matéria-prima, como se verá no capítulo v.

[39] Cf. RGPD (2016, artigos 15º e ss).

O RGPD vem esclarecer e atualizar várias questões em matéria de proteção de dados e contribuir para acabar com a insegurança jurídica criada pela Diretiva 95/46, de 24 de outubro, que, como já se referiu anteriormente, permitia a que cada país transcrevesse, com relativa liberdade, para o seu conteúdo para o seu ordenamento jurídico interno, traduzindo numa produção avulsa de legislação e sua aplicação pouco uniforme pelos Estados-membros, com impacto negativo no desenvolvimento económico, uma vez que vai gerar uma concorrência perversa entre os Estados, deixa as autoridades nacionais sem capacidade de controlo.

Chegado a este ponto, pode-se concluir que o RGPD é o normativo que melhor responde aos desafios que os Estados-membros tinham pela frente em matéria de proteção dos direitos pessoais dos seus cidadãos, compatibilizando direitos de igual valor constitucional, mas por vezes contraditórios, como direito a privacidade, a intimidade, a segurança e a liberdade de expressão.

O RGPD a par da harmonização legislativa, objetivo inicialmente proposto, permitiu esclarecer e atualizar várias questões, ocupar o topo da hierarquia das leis da União Europeia, em matéria da proteção de dados. Contribuiu, para acabar com a insegurança jurídica criada pela Diretiva nº 95/46/CE, de 26 de outubro, que resultando em perda de controlo por parte das entidades nacionais com competências em matéria de proteção de dados pessoais.

Capítulo II

O Direito à Privacidade

A primeira referência à privacidade data de 1890, quando os americanos Samuel Warren e Louis Brandeis publicaram um artigo intitulado *"the right to privacy"*. Nessa altura, estes alertavam para a importância da proteção do direito de personalidade humana, como "*o direito a ser deixado só*."[40]

Porém, antes de se avançar para o estudo do direito à privacidade, torna-se pertinente definir a «*Privacidade*» até como forma de o distinguir de outro conceito que, frequente e erradamente, é usado como sinónimo – «*Intimidade*».

2.1. O Conceito de Privacidade e Intimidade

O termo «*privacidade*» tem sua origem etimológica no latim *"privatus",* significando privado, particular, próprio, pessoal e individual.[41] Percebe-se, desde logo, que o termo privacidade "*serve a uma significação bastante ampla (...) expressando as pretensões individuais de proteção legal derivada do direito a ser deixado só ou em paz e contra a disseminação de informações de caracter pessoal*."[42]

Não obstante o termo privacidade apresentar uma pluralidade de significados, autores como Samuel Warren e Louis Brandeis definem a privacidade como "*o direito à solidão, à intimidade da vida familiar e privada, ao anonimato e à distância em relação a estranhos*."[43]

Para Marques (2004, p. 24) a vida privada é "*aquele conjunto de atividades, situações, atitudes ou comportamentos individuais que, não tendo a relação com a vida pública, respeitam estritamente à vida pessoal e familiar de uma pessoa*."

[40] Cf. Correia (2000, p. 595).
[41] Cf. Sampaio, J.A.L, (1998). *"Direito à Intimidade e à vida privada".* Belo Horizonte: Del Rey, p. 268.
[42] Cf. Martins, L. M.*"O direito civil à privacidade e à intimidade."* In: Martins-Costa, Judith (Org.). *"A reconstrução do Direito Privado"*. São Paulo, Revista dos Tribunais, 2002. p. 344.
[43] Cf. Marques & Martins. (2000, p. 102-106).

No mesmo sentido, mas numa perspetiva de defesa da vida privada e do reconhecimento do direito à privacidade, Canotilho & Moreira (como citados em Guerra, 2001, p. 159), advogam que é "*o direito a impedir o acesso de estranhos a informação sobre a vida privada e familiar e o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem*."

Por sua vez, Paulo Mota Pinto afirma que "*a defesa da privacidade visa evitar ou controlar a tomada de conhecimento ou a revelação de informação pessoal, dos factos, comunicação ou opinião relacionados com o individuo que é razoável esperar que ele encare como íntimo ou pelo menos confidencial e que, por isso, queira excluir ou pelo menos restringir a sua circulação*" (Guerra, 2001, p. 158).

De facto, a privacidade se restringe àquilo que seja de esfera estritamente individual. Isto é, se refere às atividades, atitudes, comportamentos que, sendo individuais, situam-se fora da espera pública, ficando, por isso, o seu acesso interdito à terceiros.

Na atual era digital, em que, segundo Gonçalves (2003, p. 83), "a vida privada vai para além daquilo que cada indivíduo faz em casa, já que inclui também o direito à tranquilidade, à solidão, o direto de comunicar com os outros em segurança e confidencialidade", a sua proteção torna-se cada vez mais necessária para prevenir a má reputação e a discriminação do indivíduo.

É neste sentido que a privacidade se encontra consagrado nos textos constitucionais como um direito fundamental, cuja proteção constitui responsabilidade do Estado e do próprio cidadão, com vista à salvaguarda da dignidade da pessoa.

O termo «*intimidade*», por sua vez, deriva de *"intimus", significando* aquilo que é íntimo, interior, em relação a qual não cabe qualquer publicidade, pois, *"ela é alheia a qualquer relação com terceiro."*[44]

Contrariamente à privacidade, entendida, por alguns autores, como "*o direito à solidão, à intimidade da vida familiar e privada, ao anonimato e à distância em relação a estranhos*"[45]

[44] Cf. Marques & Martins. (2000, p. 102-106).
[45] Cf. Marques & Martins (2000, p. 102).

ou "*o direito a impedir o acesso de estranhos a informação sobre a vida privada e familiar*"[46], a intimidade é entendida como *"o mais exclusivo dos direitos da privacidade",* ou seja*, "o âmbito mais restrito da vida privada, essencial à vida do individuo".*[47]

Importa, portanto, dizer que, apesar de utilizados frequente e erradamente como sinónimos, privacidade e intimidade, são conceitos com significados diferentes, reportando para realidades distintas.

Pois, a intimidade exclui qualquer forma de comunicação com outras pessoas, ao passo que a privacidade se caracteriza pela comunicação com terceiros. A intimidade recusa qualquer publicidade, já que se trata de algo pessoal que não possa ser comunicado.

No entanto, a privacidade, enquanto direito fundamental[48], tem a particularidade de se desdobrar, por um lado, no direito de impedir o acesso de estranhos a informação sobre a vida privada e familiar, por outro lado no direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem. São duas dimensões da privacidade que, advoga Correia (citado em Canotilho, 1997, p. 644), "*devem merecer o mesmo nível de proteção e força de dignidade*."

A Constituição da República Portuguesa, estabelece que "*o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis*" e proíbe também *"(...) toda a ingerência das autoridades públicas nas correspondência, nas telecomunicação e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de procedimento criminal*"[49], deixando antever que a defesa e a proteção da privacidade goza, de facto, de força de dignidade.

Todavia, advoga Canotilho (1997, p. 644) "*o sigilo que a Constituição consagra sobre os direitos que compõem a esfera privada do indivíduo é posto em risco*", uma vez que, acrescenta o professor, "*determinados direitos fundamentais colidem com outros direitos*

[46] Cf. Canotilho & Moreira (como citados em Guerra, 2001, p. 159).
[47] Martins, L. M. (2017). *A tutela jurídica da privacidade e do sigilo na era digital: Doutrina, Legislação e Jurisprudência*. In Revista de Investigações constitucionais. (Vol. IV), Curitiba, Nº3, pp. 167-200. setembro/dezembro, acedido em https://revistas.ufpr.br/rinc, consultado a19 de novembro 2019.
[48] Direito à Privacidade está consagrado na Declaração Universal dos Direitos Humanos de 1948; na Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais de 1950; na Carta de Direitos Fundamentais da União Europeia e em várias Constituições da República.
[49] Cf. Constituição da República Portuguesa de 2010, artigo 34º, nº 1 e 4.

constitucionalmente protegidos que encontram limites constituídos pelo direito de outras pessoas e limites da própria ordem social, estando [portanto] *a todo momento em conflito*".

Este conflito permanente entre os direitos fundamentais, como o direito a privacidade, a informação e de ser informado, a liberdade de expressão, tem-se mostrado complexo, uma vez que se trata de direitos fundamentais, por vezes conflituantes, mas revestidos da força jurídica, cuja restrição é proibida por lei. A sua resolução tem implicado, não poucas vezes, como que a restrição, ainda que proibida por lei, de um direito de forma a garantir outro direito e vice-versa, pautando pelo princípio de proporcionalidade, como se irá verificar no capítulo iv, dedicado ao estudo do Conflito entre os Direitos Fundamentais.

Retomando o tema deste subcapítulo, a privacidade pode ser entendida ainda como "*o direito à solidão, à intimidade da vida familiar e privada, ao anonimato e à distância em relação a estranhos*"[50] ou "*o direito a impedir o acesso de estranhos a informação sobre a vida privada e familiar.*"[51] A privacidade se refere, portanto ao *"âmbito mais restrito da vida privada, essencial à vida do individuo."*[52]

A privacidade é um dos valores intrínsecos à natureza da pessoa humana, sendo, por isso, um direito de personalidade, cuja proteção constitui uma das grandes responsabilidades dos Estados modernos e seus poderes. Um direito fortemente ameaçado na atual era digital, caracterizada por uma maior circulação e partilha de dados pessoais, podendo tais dados serem alvo de acesso não autorizado e utilização indevida por terceiros, violando assim o direito à privacidade, objeto de análise no subcapítulo seguinte.

2.2. Direito à Privacidade enquanto Direito Fundamental

O presente subcapítulo serve para abordar a problemática do direito a privacidade enquanto direito fundamental.

Como advoga Marques (2004, p. 24), a vida privada é "*aquele conjunto de atividades, situações, atitudes ou comportamentos individuais que, não tendo a relação com a vida*

[50] Cf. Marques & Martins (2000, p. 102).
[51] Cf. Canotilho & Moreira (como citados em Guerra, 2001, p. 159).
[52] Martins, L. M. (2017). *A tutela jurídica da privacidade e do sigilo na era digital: Doutrina, Legislação e Jurisprudência*. In Revista de Investigações constitucionais. (Vol. IV), Curitiba, Nº3, pp. 167-200. setembro/dezembro, acedido em https://revistas.ufpr.br/rinc, consultado a19 de novembro 2019.

pública, respeitam estritamente à vida pessoal e familiar de uma pessoa", constituindo por isso num direito da pessoa de não ver tais atividades ou comportamentos divulgados, ou seja do seu direito à privacidade.

O direito a privacidade "*enquadra-se no âmbito dos direitos de personalidades.* [Os chamados] *direitos absolutos que impõe uma obrigação passiva universal e o dever de respeito*"[53] estando, por isso, consagrados na CRP e no Código Civil, quando reconhecem a todos os indivíduos o direito de personalidade jurídica[54] e que "*todos devem guardar reserva quanto a intimidade da vida privada de outrem*"[55], podendo o titular desse direito limitar voluntariamente o exercício de direitos de personalidade desde que não sejam contrários aos princípios da ordem pública.[56]

Segundo Vasconcelos (1999, p. 250), os direitos de personalidades são aqueles sem os quais as pessoas não são tratadas como pessoas, já que se trata de direitos que são exigidos pela sua dignidade enquanto pessoas. Constituem, por isso, *"os fundamentos ontológicos da personalidade e da dignidade humana*." Acrescenta este autor, que "*os direitos de personalidades são direitos supralegais e, por isso, hierarquicamente superiores aos outros direitos, inclusive aos direitos fundamentais que não sejam direitos de personalidades*."

O direito a privacidade, quando analisado em termos doutrinais, apresenta, segundo Vasconcelos (1999, p. 250) *"três esferas na defesa da privacidade",* a saber: a esfera pública; a esfera privada; e a esfera íntima.[57]

A esfera pública, defende o autor, refere-se aos *dados públicos*. Aqueles dados "*manifestamente tornados públicos pelo seu titular*."[58] A segunda esfera é a privada, onde estão os dados não sensíveis, definidos como "*qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável*."[59] A terceira e última, a esfera íntima que contém os *dados sensíveis* "*referentes a convicção filosófica ou política, filiação partidária ou sindical,*

[53] Cf. Correia (2003, p. 83).
[54] Cf. Constituição da República Portuguesa (2010, artigo 26º).
[55] Cf. Código Civil (1966, artigos 80º e 81º).
[56] Cf. Pinto (2002, pp. 1-2).
[57] Cf. Vasconcelos (1999, p. 250).
[58] Cf. Regulamento Geral de Proteção de Dados (2016, artigo 7º, nº 3, alínea c)).
[59] *Idem*, artigo 4º.

fé religiosa, vida privada e origem racial ou étnica, bem como relativos à saúde e à vida sexual, incluindo os dados genéticos."[60]

Logo, advoga Vasconcelos (1999, p. 250) que "*a reserva da vida privada deve ser considerada*, [portanto], *uma regra e não exceção*." Para autor, *"*[é]*esse sentido que se retira, por um lado, da natureza do direito à privacidade como o direito de personalidade, e por outro, da sua consagração constitucional como um direito fundamental*".

Assim, "*o direito à privacidade só pode ser licitamente agredido, quando e só quando um interesse público superior assim o exija, (...) que o contrário possa ser causa de danos gravíssimos para a comunidade*." Porém, a sua agressão pode ser considerada lícita, escreve este autor, se o bem público em presença for superior, em intensidade e conteúdo, em "*que o exercício do direito à privacidade se torne abusivo." Uma situação em que o exercício de um tal direito pudesse "*[exceder] *manifestamente os limites impostos pela boa-fé, pelos bons costumes ou pelo fim social ou económico desse direito*" (Vasconcelos,1999, p. 251).

Neste caso, a persistência na defesa do direito a privacidade poderia significar o não cumprimento de "*um dever de cidadania e de solidariedade que sobreleva em concreto e que leva a qualificar coo egoísta e eticamente insustentável*." Pois, estar-se-ia em presença de uma situação de abuso do direito à privacidade, na modalidade do exercício desproporcionado.

Quando assim for, a agressão necessária deverá ser a mais limitada possível, de modo a reduzir ao mínimo a lesão do direito à privacidade. Caso contrário, o Código Civil, no artigo 483º, determina o dever de indemnizar a violação de direitos de outrem, nomeadamente os direitos de personalidade.

Portanto, é considerada como ilícita e inadmissível qualquer agressão a privacidade quando o interesse que a impulsiona seja eticamente pouco relevante, como o simples interesse de lucro, de comercialização, de segurança de crédito, de jornalismo, ou mesmo eticamente negativo, como o sensacionalismo, a inveja, o ódio, a chantagem, a difamação ou injúria.

Apesar de a lei de proteção de dados pessoais não derrogar nem comprime os direitos de personalidade, designadamente o direito à privacidade dos titulares dos dados, direitos com

[60] Cf. Regulamento Geral de Proteção de Dados (2016, artigo 9º).

dignidade jurídica superior e tutela constitucional, ela deve ser interpretada, integrada e concretizada com respeito pelos direitos de personalidades.

Para tanto, quando estejam em causa direitos de personalidade, "*será necessário encontrar para tal prática um fundamento de ordem pública, uma necessidade insuperável de interesse coletivo, que não permita uma solução alternativa e que justifique em termos éticos uma tal agressão*."

Fica, pois, evidente que a violação deste direito fora desse quadro de ponderação dos valores e do princípio de proporcionalidade (direito à privacidade e o interesse coletivo, em que este seja superior) implicam a responsabilidade civil, mas também "*requerer as providências judicias adequadas às circunstâncias do caso, com a finalidade de evitar a consumação da ameaça ou atenuar os efeitos da ofensa já cometidas*."[61]

O direito à privacidade, enquanto direito fundamental, como anteriormente referido, divide-se em duas vertentes normativas. A primeira refere-se ao direito de impedir o acesso de estranhos a informações sobre a vida privada e familiar, que se junta também ao direito a que ninguém divulgue as informações que tenha acesso sobre a vida privada e familiar de outrem. A segunda é a proibição de divulgação de dados pessoais reservados, também denominado de "*princípio da liberdade informática."* Ou melhor, o direito de controlar, conhecer, corrigir, retirar e agregar os dados pessoais inscritos num programa eletrónico[62].

Para Belleil (2001, p. 8), "*a privacidade abrange não duas vertentes, mas sim, quatro direitos: o direito a ser deixado em paz; o direito de controlar a difusão das informações que lhe dizem respeito; o direito de viver sem ser observado; e o direito ao anonimato*."

Em síntese, o direito à privacidade, enquanto direito fundamental, não se esgota no "*direito de impedir o acesso de estranhos a informações sobre a vida privada e familiar*" ou de "*impedir que alguém divulgue as informações sobre a vida privada e familiar de outrem*." Pois, "*enquadra-se no âmbito dos direitos de personalidades*." Aqueles direitos considerados

[61] Cf. Código Civil de Portugal (1966, artigo 70º, nº 2). De referir que a Constituição da República Portuguesa de 2010 consagra o direito à privacidade como direito fundamental incluído na categoria civilista dos direitos da personalidade, nos termos do artigo 80º do Código Civil (Portugal, 1966).
[62] Cf. Correia (2003, p. 332-340).

absolutos, exigidos pela dignidade da pessoa, estando consagrados na CRP (2010) e em outros textos normativos relevantes, como a Declaração Universal dos Direitos Humanos.

2.3. O Desrespeito pelo Direito à Privacidade na Era Digital

A era digital, caracterizada pela Internet e tecnologias de informação e comunicação, tornou o mundo mais pequeno, à dimensão de um clique, permitindo uma maior migração de pessoas e dados pessoais. Uma realidade que interpela a todos para a necessidade de proteger os seus dados pessoais, evitando que sejam utilizados de forma indevida por terceiros, desrespeitando um direito fundamental, que é o direito à privacidade.

O direito a privacidade e os dados pessoais encontra-se, cada vez mais, sujeitos a maiores riscos de violação pela quantidade de informação e dados pessoais acumulados no ciberespaço.

Pois, poucos serviços na Internet dispensam a recolha, armazenamento, tratamento e difusão de dados pessoais. Ademais, toda utilização deixa traços diversos sobre a vida do utilizador, como sua opinião, seus gostos, os hábitos de consumo, o nível socioprofissional, entre outros[63].

Atualmente, a ameaça a privacidade advém do tratamento automatizado dos dados pessoais, que permite que as pessoas sejam "*perseguidas"* durante todos o dia e transformados em pessoas "*eletrónicas*"[64].

O desrespeito pelo direito a privacidade significa a violação desse direito. Na atual era digital, a violação do direito a privacidade assume várias formas, desde violação de *e-mails* particulares, de dados pessoais sobre a conta bancária, de dados pessoais sobre as convicções política e religiosa, de ficheiros guardados nos arquivos eletrónicos, o controlo das compras efetuadas através do cartão de multibanco, a facilidade de obter dados pessoais através da navegação na internet, entre outras formas de violação do direito à privacidade.

[63] Cf. Gonçalves (2003, p.173).
[64] Cf. Castro (2005, p. 21).

Os motores de buscas na internet, particularmente os "*cookies, que permitem ao servidor identificar, de forma única, o utilizador, conhecendo as páginas por ele visitadas ou anúncios visionados*."[65] Tem-se, igualmente, os casos de envio maciços de *spams* para a caixa de correio eletrónico, constituindo uma pressão sobre a privacidade dos destinatários, sem possibilidade de reagirem aos seus emissores.

Existem outros exemplos claros de registos de dados pessoais, como a via verde e os chipes antirroubo, que registam as viagens, os cartões de crédito e de fidelização que cadastram compras, os servidores de correio eletrónicos, as redes sociais, as páginas visitadas, as preferências e os contactos, e os *smartphones,* que dão a localização exata em tempo real.

Nas praças, nas ruas, nos transportes públicos, nos espaços comerciais, nos espaços dos condomínios e até nos espaços de culto religioso vive-se, atualmente, sob constante observação, muitas vezes, com o pretexto da salvaguarda da segurança.

As tecnologias de informação e comunicação têm permitido que todos os seus utilizadores se transformem em produtores de informações sobre si próprio e sobre os outros, com as pegadas digitais, sítios, fotografias, entre outros ficheiros e dados.

Pois, o mundo digital é um dos locais mais procurados para as intromissões na privacidade. Advoga Correia (2016, p. 87) "*existe uma espécie de show do eu, em que são as próprias pessoas que se exporem com facilidades as suas vidas privadas através das redes sociais (Facebook, Youtube, Twitter…), exibindo elas mesmas o trabalho, a casa, a sua intimidade amorosa, o ginásio que frequenta (...)*."

Existem casos em que os próprios pais revelam dados pessoais dos filhos menores nas redes sociais, como a fotografia, o nome da escola, a morada da família ou outras informações que permitam identificar os filhos, com relativa facilidade.[66]

Sobre esta problemática, foi possível perceber que são os próprios titulares de dados que se expõem, muitas vezes de forma inconsciente, disponibilizando seus dados pessoais e de seus

[65] Cf. Castro (2006, p. 25).
[66] Tribunal da Relação de Évora: Processo nº 789/13.7TMSTB-B.E1 (25/06/15), disponível em www.dgci.pt consultado a 19/11/2019.

familiares a terceiros, sem se aperceberem de que estarão a contribuir para que sua privacidade seja agredida, com prejuízo para o seu direito a privacidade e de sua família.

A utilização generalizada das redes sociais tem constituído um risco para os direitos fundamentais e proteção de dados pessoais, bem como da reserva da intimidade da vida privado.

A divulgação dos dados pessoais acarreta diversos riscos, com especial incidência no contexto da criminalidade sexual, em que as vítimas são, na maioria dos casos, menores. Um perigo real, em que a Internet e, sobretudo, as redes sociais poderão favorecer a atividade criminosa e sustentar outro tipo de atuação que, não sendo criminosa, seja violadora de direitos.

Pois, a Internet, pela facilidade de divulgação, reprodução, acesso e adulteração da informação, propicia a sua utilização ou reutilização para finalidades não desejadas ou sequer imagináveis.[67]

No que se refere à recolha e tratamento de dados pessoais, sabe-se que as tecnologias de informação e comunicação têm permitido que empresas, através dos sistemas automatizados, procedam a recolha e tratamento de dados pessoais, sem que o cidadão tenha conhecimento que seus dados estão a ser compilados. Esses dados são posteriormente trocados entre órgãos públicos ou por empresas, aumentando o volume de dados pessoais disponíveis, podendo ser tratados, como se referiu anteriormente, sem consentimento dos seus titulares, em claro desrespeito dos direitos fundamentais do cidadão, em especial o direito a privacidade, consagrados nos diversos dispositivos normativos, desde a Constituição, as Leis de Proteção de Dados, o RGPD.

Na verdade, as tecnologias de informação e comunicação, aliadas a Internet, são hoje indispensáveis à vida, mas a sua utilização comporta riscos e constituem uma ameaça permanente e real para os direitos fundamentais, sobretudo o direito a privacidade que, como escreve Correia (2016 p. 87) "*é alvo de desrespeito (...) através das mais diversas formas*."

[67] Disponível em https://www.cnpd.pt/bin/revistaforum/forum2016_3/files/assets/basic-html/page-84.html, consultado a 20/11/2019.

Capítulo III

Conflitos entre os Direitos Fundamentais e a Proteção de Dados Pessoais

Neste capítulo vai-se proceder o estudo de potenciais conflitos de direitos fundamentais, sobretudo por meio de comunicação *online,* os métodos de resolução e o entendimento do tribunal face as novas demandas sociais.

Numa era em que os direitos a privacidade e liberdade de comunicação entram facilmente em colisão, porque os indíviduos acedem à Internet e utilizam os meios de comunicaçao *online*, disponibilizando um conjunto de dados pessoais relativos a sua vida privada, como informações sobre o seu computador, tipo de ligaçao a internet, seus hábitos de navegação que podem ser recolhidas por meio de terceiros, com prejuízos para os seus direitos fundamentais.

Assim, torna-se imperativo a actualização os mecanismos legislativos no sentido de garantir a proteção dos direitos fundamentais, que, segundo Alexy (2008, p. 95), são direitos "*inerentes à própria condição humana previstos pelo ordenamento jurídico*". Acrescenta ainda este autor, os "*direitos fundamentais correspondem a direitos subjetivos, universalmente garantidos a todos os seres humanos*."

A Constituição da República Portuguesa[68] consagra os direitos, liberdades e garantias de carácter fundamental, defendendo a liberdade de expressão, o direito a informação, a segurança e a inviolabilidade da vida privada.

Os direitos fundamentais entram facilmente em conflito com outros direitos constitucionalmente protegidos. Pois, advoga Bobbio (2004, p. 14) "*são bem poucos os direitos considerados fundamentais que não entram em concorrência com outros direitos também considerados fundamentais.*"

Para Canotilho (1999, p. 1191), há colisão de direitos "*quando o exercício de um direito fundamental por parte de seu titular colide com o exercício do direito fundamental por parte*

[68] A 2ª Revisão Constitucional, aprovada pela Lei Constitucional nº 1/89, de 08 de julho, reforçou o princípio da proporcionalidade, com designação expressa no texto constitucional, artigos 19º, nº 4, e 266º, nº 2.

de outro titular". Nestas situações, acrescenta este constitucionalista, "*não estamos perante um cruzamento ou acumulação de direitos (como na concorrência de direitos), mas perante um 'choque', um autêntico conflito de direitos*."

Este conflito e não concorrência de direitos fundamentais, como afirma Canotilho (1999), é inevitável e são, segundo o politólogo italiano Bobbio (2004), frequentes, uma vez que poucos são os direitos fundamentais que não colidem com outros direitos igualmente fundamentais.

Esta situação de concorrência ou conflito permanente entre direitos fundamentais demanda soluções legislativas que passariam pela aplicação do critério de valoração.

Para Alexy (2008, p. 95) a solução passaria por "*definir qual desses interesses, que abstratamente estão no mesmo nível, tem maior peso no caso concreto*". Acrescenta ainda este autor que *"esta relação de tensão não pode ser selecionada com base em uma precedência absoluta", mas sim "por meio de um sopesamento entre interesses conflituantes."*

Ainda sobre esta tensão ou relação de conflito entre direitos fundamentais, Alexy (2001, p. 295), influenciado por Dworkin, elaborou uma tese, na qual defende que *"o conflito entre regras de direito, o choque entre princípios, assumidos como direitos fundamentais, deve ser resolvido por critério de valoração, enquanto o conflito de regras deve ser solucionado mediante a declaração de invalidade de uma das regras conflituantes ou a aplicação da cláusula de exceção."*

Dessa maneira, fica determinado o critério de ponderação, já que existem interesses ser resguardados por princípios conflituantes. Com efeito, esse critério busca avaliar qual dos interesses, *"abstratamente do mesmo nível"*, possui *"maior peso diante das circunstâncias do caso concreto"*.

Portanto, a tensão entre princípios equivalentes não pode ser resolvida com a atribuição de prioridade absoluta de um sobre o outro. Pois, perante princípios equivalentes abstratamente, prevalecerá, no caso concreto, o que tiver maior peso diante das circunstâncias.

Existe, no entretanto, autores, como Farinho (2006) que defendem a resolução do conflito entre direitos fundamentais com recurso à ponderação ou princípio de proporcionalidade. Pois, advoga o autor "*a resolução de problemas de colisão de direitos só pode ser encontrada em recurso à ponderação*", acrescentando ainda que nestes casos deve aplicar a *metódica de ponderação acordada no princípio da proporcionalidade*" (Farinho, 2006, p. 64).

No mesmo sentido, mas numa perspectiva mais abrangente encontra-se o Acórdão n.º 634/93, segundo o qual, o prncípio de proporcionalidade *"desdobra-se em três subprincípios: princípio da adequação",* para a qual *"as medidas restritivas de direitos, liberdades e garantias devem revelar-se como um meio para a prossecução dos fins visados, com salvaguarda de outros direitos ou bens constitucionalmente protegidos."* De seguida, *o princípio da exigibilidade",* em que *"essas medidas restritivas têm de ser exigidas para alcançar os fins em vista, por o legislador não dispor de outros meios menos restritivos para alcançar o mesmo desiderato,* e por fim o *"princípio da justa medida, ou proporcionalidade em sentido estrito (não poderão adotar-se medidas excessivas, desproporcionadas para alcançar os fins pretendidos)."*

Por outro lado, a Jurisprudência constitucional desdobra o princípio da proporcionalidade em princípio da proporcionalidade, em sentido lato, pode, além disso, desdobrar-se analiticamente em três exigências da relação entre as medidas e os fins prosseguidos: a adequação das medidas aos fins; a necessidade ou exigibilidade das medidas e a proporcionalidade em sentido estrito, ou 'justa medida'.[69]

Pode-se, portanto, afirmar que a verificação da adequação se configura como o primeiro critério de resolução, uma vez que só em caso da medida não for adequada, violadorá do princípio da proporcionalidade.

Sobre esta tensão frequente entre direitos fundamentais e sua resolução com recurso a diversos critérios (valoração, adequação e princípio da proporcionalidade), importa ainda notar que no ordenamento jurídico português ela se tem revelado, de certa forma, pacífica, uma vez

[69] Cf. Acórdão do Tribunal Constitucional n.º 403/2015 Processo n.º 773/15 Acordam, em Plenário, no Tribunal Constitucional, disponível em https://dre.pt/pesquisa/-/search/70300353/details/maximized, consultado em 2 de fevereiro de 2020.

que "*não existe nenhum direito absoluto ou ilimitado*." Pois, estes direitos encontram-se limitados por outros direitos e/ou valores igualmente consagrados na constituição.

3.1. Proteção de Dados e Direito à Privacidade

A proteção de dados pessoais, enquanto dados relativos a pessoa singular identificada ou suscetível de identificação, se integra no âmbito do objetivo de proteção do direito a vida privada. Deste modo, em regra, lá onde estejam em causa dados pessoais, existirá uma ingerência no direito à vida privada.

O direito a privacidade e proteção dos dados pessoais são valores reconhecidos em todo o mundo civilizado e objeto de múltiplas recomendações e instrumentos jurídicos internacionais e comunitários. Importa observar que Portugal foi o primeiro país a consagrar na sua Constituição os diretos à privacidade, à vida privada e à proteção dos dados pessoais.[70]

A necessidade de proteção da privacidade e dos dados pessoais tem sido uma prioridade em todas as épocas. Todavia, com o desenvolvimento acelerado das tecnologias de informação e comunicação, aliada ao advento da Internet, nos finais do Séc. XX e início do Séc. XXI, essa necessidade tornou-se crucial e premente, já que se "*torna imperiosa proteger a informação para que a sua utilização abusiva não venha a servir interesses ilegítimos e atentatórios dos direitos, liberdades e garantias dos cidadãos*."[71]

Pois, a capacidade de controlar quem pode ter acesso as informações sobre a vida privada e atividades de outrem, tornou-se numa tarefa árdua e complexa, pelo que só uma garantia efetiva da privacidade permitirá ao seu titular escolher com quem deseja partilhar seus pensamentos e sentimentos. A privacidade protege as informações que o titular não pretende tornar públicas[72].

Nem sempre esses dois valores convivem harmoniosamente, pois, há casos que por interesse público os dados privados são tornados públicos. Configurando nestes caso conflitos

[70] Cf. Constituição da República Portuguesa (2010, artigos 26º e 35º).
[71] Cf. Vaz (2007, p. 35).
[72] Disponível em https://www.editorafi.org/193reginaruaro, consultado a 12 de dezembro de 2019.

de direitos ou valores constitucionalmente consagrados, resolvidos com recurso aos critérios anteriormente referidos, particularmente através do princípio da proporcionalidade.

3.2. Direito à Privacidade e à Segurança dos Dados

A privacidade e a segurança na era digital são assim valores que merecem a maior preocupação, por estarem associados à utilização dos sistemas de informação e de comunicação. Neles baseiam as atividades dos Estados, das instituições, das empresas e dos cidadãos.

Diversas instituições, nomeadamente a União Europeia, o Conselho da Europa, a Organização para a Cooperação e Desenvolvimento Económico e as Nações Unidas, iniciaram e têm desenvolvido estudos, apostando na divulgação de instrumentos que reforcem a segurança dos dados e garantam a proteção da privacidade, como forma de prevenir e combater a utilização ilegítima dos sistemas de informação[73].

Para tanto, o responsável pelo tratamento dos dados deve adotar mecanismos preventivos de atuações de modo a garantir a segurança dos dados pessoais. Ademais, fica obrigado a proteger os dados contra a sua destruição, acidental ou ilícita, e ainda contra a perda da segurança.

O direito à liberdade é um direito fundamental consagrado na Constituição da República Portuguesa. Pois, a CRP, lei fundamental, determina que "*que todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, pela imagem ou por qualquer outro meio, bem como o direito de informar, de se informar e de ser informados, sem impedimentos nem discriminações" e que "o exercício destes direitos não pode ser impedido ou limitado por qualquer tipo ou forma de censura*."[74]

Logo, a garantia da Confidencialidade, Integridade, e Disponibilidade das informações é indispensável, podendo o cidadão exprimir-se, sem censuras ou intromissões indevidas, e

[73] Cf. Saldanha (2019, p. 131).
[74] Cf. Constituição da República Portuguesa (2010, artigo 37º, nº 1 e 2).

certificar de que estejam também assegurados os instrumentos necessários à segurança da informação.

De outra forma, a informação é posta em causa por ações criminosas[75], que vão desde o acesso indevido à informação, quebrando a característica da confidencialidade, até à alteração do seu conteúdo, podendo mexer com a integridade do seu titular. Tudo, como afirma Ana Vaz, "*para causar prejuízo ou obter benefícios económicos ou de outra natureza, designadamente na interceção de segredos militares pondo em causa a segurança nacional*."[76]

A garantia de segurança dos dados abrange tanto a segurança física nas instalações como a segurança logica. Por seu turno, os dados pessoais envolvem as situações da recolha, do consentimento, do tratamento, da transferência, dos arquivos físico e digital, bem como a destruição dos dados.[77]

Sendo importante a proteção dos direitos fundamentais, nomeadamente os direitos à privacidade e à segurança, seja coletiva ou singular, e face novas técnicas de recolha, tratamento, transferência e partilha de dados pessoais, as finalidades, os custos e riscos associados à utilização indevida e abusiva desses dados, que podem mexer com a própria integridade dos mesmos, o legislador, ciente dessa nova realidade, previu no RGPD "*algumas medidas técnicas e organizativas, capazes de assegurar a confidencialidade, integridade, dos dados perante os sistemas e serviços técnicos; reestabelecer a disponibilidade e o acesso atempado dos dados, em caso de incidente físico ou técnico, introduzir também mecanismos para testar, apreciar e avaliar, de forma regular e eficaz, tais medidas de maneira a garantir a segurança dos dados*"[78].

Note-se, portanto, que o desrespeito dessas medidas de segurança faz o responsável pelo tratamento dos dados ou subcontratante incorrer na contraordenação prevista no RGPD e CRP [79].

[75] Como o roubo de identidades, a burla e a falsidade informáticas, a espionagem industrial e a própria sabotagem.
[76] Cf. Vaz A. (2007). *Segurança da informação, proteção da privacidade e dados pessoais*. In Nação e Defesa, Nº 117, 3ª Série, pp. 35-63.
[77] Cf. Castro (2004, pp. 267-268).
[78] Cf. Regulamento Geral de Proteção de Dados (2016, artigo 32º, nº 1).
[79] Cf. Constituição da República Portuguesa 2010, artigo 37º, nº 2. Regulamento Geral de Proteção de Dados, artigo 32º, nº 2.

3.3. Direito à Privacidade e à Informação

O dever de reserva da intimidade da vida privada é, em primeiro lugar, do individuo. Então, a divulgação de sua privacidade ou de informações de foro pessoal, em maior ou menor grau e extensão, é sempre da sua responsabilidade, porquanto o "*indivíduo tem a possibilidade de negar informação pessoal ou opor-se à sua recolha, a difusão e a tendo a liberdade de dispor e de controlar as informações que lhe respeitem*."[80]

Na era digital, dados sobre pessoas são registados pelos sistemas de comunicação como cartões de crédito; telemóveis, entre outros dispositivos móveis, circulando constantemente nos sistemas de informações. Estes dispositivos eletrónicos possibilitaram maior recolha, tratamento e circulação das informações virtualmente sem limites de tempo ou de espaço.

Contudo, o problema estará no facto do computador facilitar a acumulação e a interconexão de informação sobre pessoas, criando condições para violação do direito à privacidade.

Com isto, a defesa dos interesses individuais, particularmente a proteção da privacidade, como direito fundamental, é assegurada pelas Leis nacionais e pelos textos internacionais relativos aos Direitos do Homem. A sua proteção, além de necessária, se justifica precisamente porque as informações relativas às pessoas são utilizadas com apoio da informática para fins diversos, com risco de serem usadas abusivamente, com intuito discriminatório ou para fins diferentes dos que estiveram na base da sua recolha.

Em linha da frente, encontram-se os direitos fundamentais, como a liberdade de expressão e o direito à informação, indispensáveis para o exercício de cidadania, que é o direito de participação na vida pública, "*direitos individuais com garantia constitucional* [fazendo] *parte da procura de transparência na vida pública, fundamental no Estado moderno*" (Dias, 2001, p. 4).

Na verdade, a preocupação de se encontrar um ponto de equilíbrio no exercício e defesa dos direitos fundamentais e de personalidades, neste caso entre o direito à privacidade e o direito à informação, ficou patente nos diversos instrumentos normativos, particularmente na Diretiva

[80] Cf. RGPD (2016, artigo 21º).

95/46/CE, de 24 de outubro. Como escreve Marques (2004, p. 41), "*a elaboração da diretiva teve por base a procura de um equilíbrio entre a proteção de direitos de personalidade e o direito à informação, estabelecendo no seu art.º 9 exceções para quem faça esse tratamento para fins exclusivamente jornalísticos, de expressão artística ou literário*."

Por outro lado, a modernização administrativa trouxe uma administração aberta aos cidadãos, em que estes têm acesso à informação administrativa, enquanto direito, defende Dias (2001, p. 2) "*poderá colidir por vezes com o direito à reserva de intimidade e vida privada dos mesmos"* porquanto será necessário informar os cidadãos, facultando-lhes o acesso à informação e, ao mesmo tempo, garantir-lhes outro direito fundamental que é a reserva da sua vida privada e à intimidade, ou seja, conciliar o direito à informação e o direito à privacidade, consubstanciando-se em conflitos de direitos ou princípios fundamentais.

Atualmente, muitos dados são tratados informaticamente e circulam pelos sistemas de comunicação, e essas informações referentes a vida privada acedidas ilicitamente põem em risco a privacidade. Esses direitos dotados de garantias constitucionais confrontam-se, por um lado, com o interesse do indivíduo na proteção dos dados a seu respeito e, por outro com o interesse de entidades públicas[81].

3.4. Direito à Privacidade e Consentimento

O Regulamento Geral de Proteção de Dados trouxe um importante ganho em matéria de proteção e tratamento dos dados pessoais, na medida em que introduz a autorização do titular dos dados pessoais, ou seja, de consentimento do titular para que se possa proceder ao tratamento dos dados. Com o RGPD, qualquer tratamento de dados pessoais sem o consentimento prévio dos seus titulares passa a configurar-se violação, sujeitando o responsável o direito de indemnizar o titular dos dados.

Logo, as empresas e organizações ficam obrigadas a procederem à legalização das suas bases de dados, tornando-as conformes o regulamento, em que "*a recolha deste tipo de*

[81] Cf. Gonçalves (2003, p. 82).

informação ainda merece a atenção e a conformidade por parte dos responsáveis pelo tratamento." (Saldanha, 2019, p. 47).

O consentimento do titular dos dados é "*uma manifestação de vontade, livre, especifica, informada e explicita, 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*"[82], sendo, por isso, o primeiro requisito a se ter em conta na recolha dos mesmos.

De facto, o consentimento poderá ser considerado uma das grandes inovações em matéria de tratamento e proteção de dados. Introdução deste direito permitiu ao titular de dados ter o total controlo das suas informações e decidir quais deverão ser tratados, impondo, desta forma, um limite e garantindo o seu direito à privacidade no âmbito do direito à autodeterminação informativa.

Como escreve Pinto (2002, pp. 4-6), "*o titular da privacidade tem a faculdade de conformar as fronteiras e os limites do exercício do seu direito à privacidade*." Posição partilhada por Canotilho & Machado (como citados em Correia, 2016, p. 225), ao defenderem "*que o conceito de privacidade envolve a ideia de autonomia e de autodeterminação/autocontrole, que consiste na possibilidade da pessoa controlar tanto quanto possível a massa de informação sobre si mesma a que os outros podem ter acesso*". Alem disso, "*a privacidade não é um direito absoluto, o seu titular pode dispor dele, bastando o seu consentimento*" (Pinto, 2002, p. 7).

Por outro lado, o direito à privacidade não é um direito absoluto e o consentimento em se trata de mera manifestação de vontade, este pode ser retirado uma vez que não é definitivo.[83]

Logo, advoga Castro (2014, p. 207), "*o consentimento deve ser livre, sem qualquer pressão e retirada sem restrições ou oposição, e sem que o titular sofra qualquer consequência*."

Note-se, portanto, que os incapazes, como menores e deficientes físicos ou psíquicos, gozam igualmente do direito à autodeterminação informativa, "*bastando para tal depreender*

[82] Cf. RGPD (2016, artigos 4º, nº11 e 7.º, nº1).
[83] Cf. Marques, G. & Lourenço, M. (2006, p. 339).

que no momento em que dispõe do seu direito tinha capacidade para aferir as suas consequências, no caso de ser privada a imaturidade do titular é o tutor que terá uma palavra a dizer." (Pinto, 2002, p.12).

Pode-se inferir que o direito ao consentimento, manifestação de vontade do titular de dados, apesar de não ser definitivo, quando respeitado escrupulosamente reforçará a garantia do direito a privacidade, sendo certo que o tratamento de dados comporta sempre riscos para a privacidade. Segundo Magalhães & Pereira (2018, p. 10), "*dando o consentimento torna se necessário garantir a privacidade durante todo o processo, pois desde a conceção deve se considerar o risco que tal representa para a privacidade*."

O conflito entre a privacidade e o consentimento pode ocorrer na medida em que, por um lado tem-se interesse do indivíduo em não dar ou retirar o consentimento, para que não haja tratamento dos seus dados pessoais ou não revelar informações sobre a sua vida privada e, por outro lado a necessidade do consentimento para proceder o tratamento lícito dos dados pessoais. Conflito, como já se referiu anteriormente, permanente e frequente, carecendo sempre de resolução, sendo "*a melhor metodologia é num primeiro momento, por interpretação, proceder-se à descoberta do objeto de cada direito*" (Farinho 2006, p. 58), que para Novais (2004, p. 455) *"(...) depende de qual o direito que se tomar como referências*", uma vez que segundo Farinho (2004, p. 60) "*não existe, porém, um padrão ou critérios de soluções de conflitos de direitos válidos em termos gerais e obstractos*." Logo, deve-se recorrer ao princípio da proporcionalidade de forma a coordenar e combinar os bens jurídicos em conflito, evitando o sacrifício total de uns em relação aos outros.

Capítulo IV

A Nova Geração de Direitos dos Titulares de Dados

Este capítulo será dedicado aos novos direitos dos titulares de dados, instituídos pela Lei nº 58/2019, de 8 de agosto, designada igualmente de Regulamento Geral de Proteção de Dados.

Com efeito, o Regulamento Geral de Proteção de Dados (RGPD) consagra uma nova geração de direitos, como *o direito à informação e acesso aos dados; à retificação dos dados; ao esquecimento; à portabilidade dos dados; o direito de oposição ao tratamento dos dados; e o direito à limitação do tratamento dos dados*.[84] Um conjunto de direitos que, como se verá no capítulo seguinte, referente aos princípios fundamentais de tratamentos de dados pessoais, deverá permitir reforçar a garantia do direito à autodeterminação informativa que assiste os titulares de dados, atribuindo-lhes "*uma maior liberdade, um poder de dispor das suas informações pessoais, e de controlo da utilização das informações a seu respeito (…) e que concretizam o direito à autodeterminação informativa*" (Castro, 2005, p. 16).

4.1. O Direito à Informação e Acesso aos Dados

O direito à informação é um dos muitos direitos fundamentais consagrados em quase todas as constituições modernas, não sendo a Constituição da República Portuguesa uma exceção. Esta determinar que todos têm direito à serem informados e se informarem, sendo proibida a limitação do exercício desse direito por qualquer tipo ou forma de censura.

Na segunda metade do XX, em consequência da liberdade de expressão, surgiu o direito à informação, numa altura em que entidades públicas e privadas, nacionais e não só, começavam a recolher, armazenar informações pessoais e a constituírem bases de dados, em vários suportes, sobre seus colaboradores, parceiros ou clientes visando diversas finalidades.

[84] Cf. RGPD (2016, artigo 12º e ss).

Assim, o direito à informação se estendeu ao direito de acesso aos dados pessoais, podendo os seus titulares, em querendo e a todo tempo, ter acesso ao seus dados, ficando os responsáveis pela recolha e tratamento dos dados proibidos de realizarem qualquer operação sobre os dados pessoais sem o consentimento dos titulares de dados e obrigados a informar os titulares qual ou quais as finalidades do tratamento dos dados que sobre si são recolhidos de forma direta ou indireta.

Estas inovações visavam, fundamentalmente, minimizar e prevenir os riscos e prejuízos que uma operação de recolha, tratamento e manutenção de dados pessoais poderá trazer para os seus titulares.

Neste sentido, o responsável pelo tratamento dos dados tem o dever de fornecer aos titulares dos dados um conjunto de informações necessárias para garantir um outro direito, igualmente importante, que é o direito a autodeterminação informática e do controlo dos seus dados pessoais. Com efeito, os titulares devem estar informados sobre "*a identidade e os contactos do responsável pelo tratamento ou do seu representante se for o caso, das finalidades do tratamento a que os dados pessoais se destinam, do prazo de conservação, entre outras informações, como a transferência de dados para países terceiros, caso o responsável pelo tratamento dos dados tenha a intenção de o vir a fazer*."[85]

Os titulares de dados devem ainda ter acesso aos dados que lhe digam respeito, podendo os retificar, apagar e inclusive limitar o tratamento dos seus dados. Com efeito, assiste aos titulares de dados "*o direito de se opor ao tratamento e à portabilidade dos seus dados, de reclamar para a autoridade de controlo, caso perceba que existe da parte do responsável pelo tratamento dos dados intenção de proceder ao tratamento de dados para fim contrário ao que tenha sido recolhido*."[86]

Para tanto, essas informações devem ser concisas, transparentes, clara e precisa e, como veremos adiante, em linguagem simples e acessível, podendo ser por escrito ou não.

Todavia, importa dizer que esses direitos não são absolutos, pelo que podem ser limitados, caso não seja possível garantir aos titulares de dados tais direitos, nos casos em que

[85] Cf. RGPD (2016, artigos 46º, 47º e 49º).
[86] *Ibidem*.

a sua garantia se obrigue a esforços desproporcionais, ou o acesso aos dados estão condicionados pela confidencialidade dos mesmos ou o seu responsável seja obrigado ao dever de sigilo profissional.

O direito de acesso traduz-se, portanto, na possibilidade que os titulares dos dados têm de saber se os seus dados estão ou não a ser tratados, se foram ou não transferidos para outra entidade, podendo aceder e ter, de forma gratuita, todas as informações no que respeita ao tratamento dos mesmos, desde que um tal acesso a estas informações não prejudique o segredo comercial ou de propriedade intelectual.[87]

4.2. O Direito à Retificação dos Dados

O direito à retificação dos dados é outra faculdade importante em matéria da garantia do direito de autodeterminação. Permite, pois, ao titular dos dados exigir do responsável pelo tratamento a correção ou atualização dos seus dados sempre que verificar que o princípio da exatidão e atualização dos dados não está a ser observado. Isto é, em caso de os seus dados não estejam corretos ou careçam de atualização, solicitar junto do responsável pelo tratamento dos dados a retificação ou atualização dos mesmos.

Note-se que o direito à retificação dos dados decorre da exigência da qualidade dos dados, já que determina que "*os dados pessoais sejam exatos e, se necessário, atualizá-los, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou retificados os dados inexatos ou incompletos*"[88]

Além disso, o direito à retificação obriga o responsável pelo tratamento a proceder a retificação dos dados, num prazo razoável e sem custos excessivos para o titular. Caso contrário, estando obrigado a retificar os dados e os manter sempre atualizados, não o fazendo incorre a uma contraordenação, para mais quando o responsável pelo tratamento for uma entidade administrativa pública, em que tem o dever de os manter atualizados.

[87] Cf. Magalhães & Pereira (2018, p. 24).
[88] Cf. RGPD (2016, artigo 16º).

Por outro lado, o titular de dados, além de solicitar sua correção e atualização, poderá, em querendo, solicitar o apagamento dos dados, já que tem a faculdade de pedir que seja "*esquecido*", exercendo o seu direito ao apagamento, uma das muitas inovações introduzidas pelo RGPD[89], em matéria de tratamento de dados.

O direito ao apagamento atribui ao titular o poder de solicitar ao responsável pelo tratamento o apagamento dos seus dados. Logo, o responsável pelo tratamento fica obrigado a apagar os dados pessoais, sem demora injustificada, em situações em que dados se revelem desnecessários para a finalidade que foram recolhidos ou tratados. Poderá ainda *"o titular opor-se ao tratamento de dados pessoais utilizados para fins automatizados, os dados pessoais que tenham sido tratados de forma ilícita, se o titular retirar o seu consentimento, ou então não exista outro fundamento legal par o tratamento de dados*."[90]

Portanto, o direito ao apagamento de dados, como não poderia deixar de ser, tem limitações legais. Desde logo, limitações de ordem territorial, em consequência das competências dos organismos da União Europeia, e de natureza dos dados, uma vez que existem dados que por razões de interesse público, segurança nacional, de faturação, comercialização, fiscais e outros, a sua conservação se justifica.[91]

Pelo contrário, o direito ao apagamento não se aplica quando se trata do exercício de autoridade pública por parte do responsável pelo tratamento de dados, visando "*o interesse público no domínio da saúde pública, para questão de arquivo de interesse público, para fins de investigação cientifica ou histórica ou para fins estatísticos, para declaração exercício ou defesa de um direito num processo judicial*."[92]

No entanto, caso o responsável pelo tratamento venha transferir os dados, cujo apagamento o titular solicitou, para outras entidades, fica aquele obrigado a comunicar esta vontade do titular dos dados às entidades recetoras. Para tanto, o responsável pelo tratamento dos dados obriga-se adotar as medidas que se mostrarem necessárias e razoáveis para a execução deste dever.

[89] Cf. RGPD (2016, artigo 17º, nº 1).
[90] Cf. Anuário da Proteção de Dados (2019, pp. 57-63).
[91] Cf. Magalhães & Lourenço (2006, p. 25).
[92] Cf. RGPD (2016, artigo 17º, nº 3, a)).

4.3. O Direito à Portabilidade de Dados Pessoais

Hoje, mais do que nunca, numa era de grandes migrações de pessoas e, particularmente de dados pessoais, da proliferação de dispositivos móveis de partilha, transferência, transmissão e armazenamento de dados pessoais, a portabilidade representa, mais do que uma necessidade, uma nova geração de direitos, tendo em conta o imperativo de proteger os dados pessoais, conciliando os direitos à circulação e à privacidade. Ou seja, permitindo que as pessoas possam circular livremente e sem prejuízo para o seu direito à segurança (pessoal e dos seus dados pessoais) e à privacidade.

Assim, o direito à portabilidade de dados pessoais visa dar mais poderes aos titulares dos dados em relação aos seus próprios dados pessoais, podendo transferir, copiar ou transmitir de um ambiente informático par outro. Por isso, o RGPD determina que "*o titular dos dados tem o direito de receber os dados que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir*."[93]

Além disso, estatui o mesmo regulamento, que o direito à portabilidade só é aplicável em situações de existência de pelo menos um dos fundamentos jurídico para o tratamento dos dados. Logo, o titular só poderá exercer o direito de transferir, copiar ou transmitir de um ambiente informático para outro, os seus dados, com fundamento no princípio de consentimento ou num contrato no qual seja parte.[94]

Outrossim, o direito à portabilidade só se aplica aos dados pessoais que digam respeito ao titular e terem sido por este disponibilizados ao responsável pelo tratamento, sem prejuízo também para os direitos e a liberdades de terceiros.[95]

Significa, pois, dizer que as balizas para o exercício do direito à portabilidade são, de certa forma, apertadas, na medida em que só se aplica em casos excecionais. Logo, só é possível quando o tratamento for lícito, isto é, realizado mediante o consentimento e por meios

[93] Cf. RGPD (2016, artigo 20º).
[94] Cf. RGPD (2016, artigo 20º, nº1 alínea a) e artigos 6º, nº 1, alíneas a) e b) ou artigo 9º, nº 2, alínea a).
[95] Cf. RGPD (2016, artigo 20º, nº1).

automáticos, e se tratarem de dados sobre o titular, mas que não prejudicam direitos e liberdades de terceiros, já que implica apagamento de dados pessoais.

De referir que o RGPD fixa um prazo de um mês, podendo ser alargado, nos casos complexos, até três meses no máximo[96], para o responsável pelo tratamento responder um pedido de portabilidade.

Porém, quando se encontram reunidas as condições para o exercício do direito à portabilidade, a lei obriga que os dados pessoais devem ser fornecidos em formatos que apresentem um nível de abstração relativamente a qualquer formato interno ou específico, porque a portabilidade dos dados visa retirar dados pessoais do sistema de informação do responsável pelo tratamento dos dados, podendo a sua transmissão constituir um risco para esses dados.

Neste caso, como forma de proteção dos dados, o responsável pelo seu tratamento deve adotar todas a medidas de segurança necessárias para garantir que os dados pessoais sejam transmitidos em segurança até ao destino e ainda continua a proteger os dados que permanecem no seu sistema.[97]

4.4. Direito de Oposição ao Tratamento de Dados

Como outros direitos anteriormente referidos e analisados, o direito de oposição ao tratamento de dados vem igualmente reforçar o direito do titular de poder dispor dos seus dados pessoais e deles ter total controlo, podendo os copiar, partilhar, transferir, durante toda a fase de tratamento, inclusive de os apagar ou solicitar o apagamento dos mesmos. Com efeito, o titular dos dados pessoais pode, em qualquer altura, se opor a qualquer tipo de tratamento dos seus dados, "*por razões relacionadas com a sua situação particular*" (Castro, 2005, p. 254).

[96] O responsável pelo tratamento de dados deve, em caso de prorrogação do prazo, informar o titular dos dados os motivos de tal decisão.
[97] Disponível em https://www.cnpd.pt/bin/rgpd/docs/wp242rev01_pt.pdf, consultado a 10 de outubro de 2019.

Neste sentido o RGPD confere ao titular dos dados "*o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento de dados pessoais que lhe digam respeito*."[98]

Por isso, o direito de oposição ao tratamento, quando exercido pelo titular dos dados pessoais, impõe ao responsável pelo tratamento dos dados o dever de interromper o tratamento dos dados, devendo inclusive os apagar, ao menos que "*que apresente razões imperiosas e legitimas para o tratamento que prevaleçam sobre os interesses, direitos e liberdade do titular de dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial*."[99]

A existência de exceções demonstra que o direito de oposição, à semelhança do direito à portabilidade anteriormente analisado, não é absoluto. Com efeito, o responsável pelo tratamento dos dados poderá não se obrigar a suspender o processo de tratamento, caso entenda existir razões *imperiosas* e *legitimas* que justifiquem a sua continuidade, relegando para um plano infra legal os direitos e liberdades do titular dos dados.

Para isso, o responsável pelo tratamento de dados teria de "*considerar a importância das informações e o seu objetivo específico, os impactos sobre os interesses, os direitos e as liberdades do titular dos dados e realizar um exercício de ponderação*."[100]

Pode se tomar como exemplo, uma situação em que a "*a definição de perfis*" tem por objetivo prevenir a propagação de uma doença altamente contagiosa, como o é o Covid-19 do Coronavírus, em que há uma ameaça real para a sociedade em geral. Aqui, trata-se de prevenir a sociedade no seu todo e não apenas para interesses particulares do responsável pelo tratamento.

Fica, pois, evidente que o direito de oposição ao tratamento dos dados contribui sim para que o titular possa dispor do poder de controlar os seus dados pessoais, mas não é um direito absoluto pelo que exige requisitos legais para o seu exercício.

[98] Cf. RGPD (2016, artigo 6º, nº 1, alíneas e) e f).
[99] Cf. RGPD (2016, artigo 21º, nº 1).
[100] Cf. RGPD (2016, artigo 21º).

4.5. O Direito à Limitação do Tratamento de Dados

O tratamento de dados deve sempre ser limitado, uma vez que existem dados que, como referido anteriormente, pela sua natureza sensível e versarem a intimidade da pessoa, o seu tratamento deve ser por si já limitado. Além disso, o tratamento ilimitado desses dados pessoais violaria alguns direitos fundamentais e de personalidade consagrados no texto constitucional e o direito à limitação do tratamento de dados previsto no Regulamento Geral de Proteção de Dados (RGPD) ao determinar que "*o tratamento dos seus dados pessoais, sejam limitados aos seus interesses*."[101]

O direito à limitação do tratamento dos dados, à semelhança dos demais direitos dos titulares de dados, alguns já referidos e tratados, poderá minimizar os riscos inerentes ao tratamento de dados pessoais, bastando, para isso, o titular dos dados invocar erros ou desatualização dos dados, o tratamento for ilícito ou em caso de o titular declarar a sua vontade em apagar os dados. Se os dados se mostrarem desnecessários à finalidade da sua recolha, pode também o titular exercer o seu direito de limitação de tratamento dos mesmos, a não ser que, à semelhança do direito à oposição, "*se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados*."

Nestes casos, como ocorre nos casos em que o titular se opõe ao tratamento ou o direito ao esquecimento, o responsável pelo tratamento de dados deve também comunicar o titular dos dados da decisão de continuar o processo. Se os dados foram transmitidos a uma outra entidade para proceder ao tratamento, esta deve igualmente ser comunicada da vontade dos titulares dos dados, "*só não o fazendo se essa comunicação se revelar impossível ou implicar um esforço desproporcionado*."[102]

Pelo acima exposto neste capítulo, pode-se concluir que os novos direitos dos titulares de dados pessoais, introduzidos pelo Regulamento Geral de Proteção de Dados (RGPD), aprovado pela Lei nº 58/2018, de 08 de agosto, além de garantir o direito de autodeterminação dos titulares de dados pessoais, contribuem para prevenir e minimizar os riscos sempre presentes no processo de tratamento de dados e limitar a liberdade dos responsáveis pelo tratamento dos dados pessoais, já que os atribui responsabilidade criminal e cível em caso de o

[101] Cf. RGPD (2016, artigo 18º, nº 1).
[102] Cf. Castro (2006 p. 18).

tratamento não obedecer os princípios fundamentais e os direitos dos titulares durante todo o processo de tratamento. Pois, advoga Saldanha (2019, p. 54) "*o que se procura com este direito é dar poderes ao titular dos dados, conferindo lhes um maior controlo sobre os seus dados, atribuindo-lhes uma maior liberdade de escolha e, dessa forma, reequilibrando a relação entre titulares e responsáveis*."

4.6. Os Princípios Fundamentais de Tratamento dos Dados

O Regulamento Geral de Proteção de Dados reconhece um conjunto de novos direitos aos titulares de dados, com destaque para o direito ao consentimento, uma manifestação de vontade, através da qual deverá ser o titular de dados a decidir quais dados devem ser tratados, tendo o controlo sobre os mesmos. Logo, o mesmo dispositivo normativo vem introduzir também um conjunto de princípios fundamentais que devem ser observados no tratamento dos dados pessoais, com "*o princípio da licitude e transparência; princípio da livre circulação; princípio do propósito limitado; princípio da minimização dos dados; princípio da precisão e exatidão; princípio da limitação à retenção dos dados; princípio da segurança dos dados; e o princípio da responsabilidade*."[103]

Deste conjunto de princípios norteadores do tratamento de dados pessoais, optou-se por analisar apenas os princípios da licitude, lealdade e transparência; de propósito limitado, de limites à retenção dos dados, da segurança dos dados e da responsabilidade, por considerar serem aqueles que melhor contribuem para reduzir os riscos associados ao tratamento de dados pessoais e garantir o direito à privacidade e à reserva a vida privada, sem com isto querer, no entanto, minimizar a importância dos outros princípios.

[103] Esses princípios estão enumerados no artigo 5º do Regulamento Geral de Proteção de Dados.

4.6.1. Princípio da Licitude, Lealdade e Transparência

O princípio da licitude, lealdade e transparência, presente no RGPD, deve ser a base de todo o sistema consagrado no regulamento. Logo, os dados pessoais, na sua relação com o titular têm de ser objeto de um tratamento lícito, leal e transparente.

A transparência e a licitude implicam que a recolha dos dados pessoais seja feita de forma transparente e nos termos da lei. A legalidade passará primeiramente por obedecer o consentimento prévio do titular dos dados, bem como respeitar a finalidade específica a que se propôs, aquando do consentimento. Caso não seja observado o princípio da licitude e o dever de lealdade e transparência, qualquer ato de recolha e tratamento seria ilegal, já que se configura numa violação grave de direitos fundamentais e de personalidade.

A transparência a que fica obrigado quem recolhe e trata os dados, consiste na necessidade de as pessoas singulares, a quem os dados dizem respeito, serem avisados dos riscos, regras, garantias e direitos associados ao tratamento dos seus dados pessoais e devem ser também alertados para os meios de que dispõem para exercer esses direitos.

Já a licitude significa que titular deu o seu consentimento para que os seus dados pessoais fossem objeto de tratamento para uma ou mais finalidades específicas. São situações em que o tratamento é necessário para a execução de um contrato, no qual o titular dos dados seja parte, ou para diligências pré-contratuais, a pedido do titular dos dados, ou então se o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito.

Considera-se caso semelhante quando entidades patronais procedem a tratamento de dados dos seus funcionários. Portanto, se o tratamento for necessário para a defesa de interesses vitais dos titulares dos dados ou de outras pessoas singular, para o exercício de funções de interesse público ou exercício da autoridade pública de que está investido o responsável pelo tratamento, bem como para defender os interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, considera-se lícito o seu tratamento, uma vez que se pode verificar que o titular dos dados pode não ser a única pessoa com interesse legítimo. Pelo contrário, se prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoas, em especial se o titular for uma criança, o tratamento não será permitido, pelo que seria considerado ilícito.

O tratamento leal implica que tenha havido a concordância do titular, isto é, que o tratamento seja feito com o prévio consentimento do titular e o responsável pelo tratamento seja capaz de poder fazer prova desse consentimento, já que será sempre dele a responsabilidade de provar que tenha sido com o consentimento daquele.

Importa, no entanto, afirmar que o consentimento, para que possa ser válido deve respeitar determinados pressupostos. Logo, a pessoa em causa não pode estar sujeita a qualquer pressão no momento da tomada da decisão, como também deve estar informada sobre o objeto e as consequências do seu consentimento e o âmbito do mesmo ser razoavelmente concreto.

Além disso, o consentimento só é livre se o titular dos dados puder exercer uma verdadeira escolha e não existir risco de fraude, intimidação, coação ou consequências negativas importantes se o consentimento for recusado.

A declaração de consentimento, se previamente fornecida pelo responsável pelo tratamento, deve ser escrita numa linguagem clara e simples, sem cláusulas abusivas. Por outro lado, se declaração for efetuada num contexto de uma declaração escrita referente a outras matérias, tem de existir garantias suficientes de que o titular dos dados está plenamente consciente do consentimento dado.

Para tanto, o titular dos dados deve ter informações suficientes antes de tomar a decisão de aceitar ou não partilhar os seus dados. A informação deve incluir uma descrição rigorosa e facilmente compreensível do objeto do consentimento e também das consequências da aceitação ou da recusa do consentimento. Mas mais, a informação prestada tem de ser rigorosa.

Refira-se que todo o consentimento é suscetível de ser retirado a qualquer momento. E essa retirada não compromete a licitude do tratamento efetuado até esse momento por parte do responsável pelo tratamento.

Em síntese, todas informações ou comunicações acerca dos direitos do titular dos dados, relativamente ao tratamento de dados pessoais, devem ser de fácil acesso e compreensão, devendo ser formuladas numa linguagem simples e clara.

Para isso devem incluir as informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento desses dados, os fins a que o tratamento se destina, as informações que asseguram que o tratamento é efetuado com equidade, a salvaguarda do seu direito de obter a confirmação e a comunicação de que os seus dados pessoais estão a ser tratados, "*podendo ser apresentadas por via eletrónicas, principalmente se essa foi a forma escolhida para fazer a recolha do consentimento*" (Saldanha:2018, p. 43).

4.6.2. Princípio do Propósito Limitado

O princípio do propósito limitado prevê que todos os dados recolhidos e sujeitos ao consentimento explícito por parte dos titulares dos direitos devem ser tratados obedecendo a uma finalidade determinada. Para tanto, a finalidade deve ser comunicada ao titular dos dados no momento da solicitação do consentimento.

Por isso, no ato da solicitação do consentimento o titular deve ser informado, com igual clareza, das finalidades da recolha dos dados, os fins a que destinam. Em caso de tratamento deferente do inicialmente ou de qualquer outra alteração, fica o responsável pelo tratamento obrigado a solicitar novo consentimento, visto que a finalidade não pode ser, em caso algum, diferente do inicialmente determinado no momento da solicitação do consentimento.

Desta forma, fica claro que, não obstante o consentimento para o tratamento dos dados, torna-se imperativo que o responsável pelo tratamento diga com clareza qual a finalidade do tratamento do, sendo certo que fica vedado, constituindo mesmo uma ilicitude, o tratamento de dados para fins indeterminado ou ilimitado.

Logo, todas as situações de tratamento posteriores, sejam para fins de arquivo de interesse público, de investigação científica ou histórica ou até para fins estatísticos, não devem ser consideradas incompatíveis com as finalidades iniciais, uma vez que esse tipo de tratamento está sujeito a um conjunto de regras que garantem os direitos e liberdades do titular dos dados, nomeadamente a adoção de medidas técnicas e organizativas, que assegurem o princípio da minimização da informação e também de segurança, como a encriptação dos dados, técnica adotada por quase todas as plataformas digitais.

Por outro lado, os dados recolhidos e arquivados, embora sejam de interesse público, investigação científica ou outra finalidade, devem ser retidos ou guardados durante o tempo necessário à realização desses propósitos, isto em observância ao princípio de limitação à retenção dos dados.

Assim, o tempo de retenção dos dados deve ser limitado ao mínimo, pelo que o responsável pelo tratamento deverá mesmo fixar os prazos para o apagamento ou revisão periódica, sem prejuízo de, em algumas situações, poderem ser alargados para períodos mais longos.[104]

4.6.3. Princípio da Segurança dos Dados

A segurança dos dados é a preocupação central em matéria de tratamento dos dados pessoais. Pois, o receio de informações de reserva absolutamente pessoal poderem ser partilhadas ou esteja ao alcance de terceiros acompanha todo o cidadão no ato da sua disponibilização ou mesmo quando é o próprio titular a tratá-los.

Por isso, falar de segurança dos dados é falar de integridade e confidencialidade da informação retida pelo responsável pelo tratamento. Assim, o princípio de segurança prevê que os dados devam ser tratados pelos responsáveis de forma a garantir a segurança, incluindo a proteção contra o tratamento de dados não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.

É assim que o responsável pelo tratamento de dados, além de garantir a segurança dos dados, garantindo o direito à privacidade dos titulares, podendo incorrer em responsabilidade criminal, poderá também ter que assumir responsabilidade civil por situações de tratamento indevido ou ilícito, assim como sua perda, destruição ou danificação acidental, caso se venha a provar que se tenha resultado de sua ação, omissão ou negligência.

O tratamento dos dados, hoje em dia, faz-se essencialmente através de sistemas informáticos, devendo, por isso, ser salvaguardado por meios que asseguram a segurança das

[104] Ver os artigos 89º e *ss* do Regulamento Geral de Proteção de Dados.

redes, ou melhor, que garantam que quer as redes quer os sistemas informáticos possam resistir, com certo nível de confiança, a eventos acidentais ou ações maliciosas ou ilícitas que comprometam a disponibilidade, autenticidade, integridade e confidencialidade dos dados pessoais mantidos ou transferidos para terceiros.

O próprio regulamento de proteção de dados, relativa à segurança e proteção de dados pessoais aconselha que, sempre que possível o tratamento de dados seja através de pseudonimização/encriptação. Logo, o RGPD determina que o "*tratamento de dados pessoais deve ser feito de forma que deixem de poder ser atribuídos a um titular de dados específicos sem recorrer a informações suplementares, desde que essas informações suplementares sejam metidas 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*."[105]

4.6.4. Princípio da Responsabilidade

Se o regulamento obriga a que os dados pessoais sejam tratados em segurança, não poderia deixar de exigir responsabilidades às empresas, organizações, instituições ou outras entidades responsáveis pelo tratamento dos dados. Caso contrário estar-se-ia perante uma situação em que a obrigação de garantir a segurança no tratamento dos dados ficasse a depender da vontade dos responsáveis em quererem ou não comprimir, podendo, sendo-lhes favorável, descuidar da segurança, na certeza de que não teriam qualquer consequência negativa de uma utilização insegura ainda que com dolo.

O princípio de responsabilidade, presente no RGPD, determina que "*caberá ao responsável pelo tratamento dos dados responder por toda a implementação do regulamento e pela colocação da organização (...) em conformidade com o regulamento*."[106]

O responsável pelo tratamento tem não só de tomar todas as medidas regulatórias, mas também terá de se responsabilizar pela sua efetividade. Está-se perante a inversão do ónus da prova, ou seja, esta responsabilidade exige, por parte dos responsáveis pelo tratamento, a

[105] Cf. RGPD (2016, artigo 4º, nº 5).
[106] Cf. RGPD (2016, artigo 25º).

implementação ativa de medidas de promoção e salvaguarda da proteção de dados nas suas atividades, sendo certo de que terão provas de sua existência.

Portanto, o responsável fica obrigado a assegurar a conformidade das operações de tratamento e proteção de dados, devendo estar em condições de demostrar, a todo o tempo, essa conformidade com as legislações sobre a proteção de dados.

Como forma de reforçar o princípio da responsabilidade, o RGPD aponta alguns instrumentos, como "*a promoção do controlo prévio das operações planeadas através da avaliação de impacto sobre a proteção de dados; a solicitação de consulta prévia às autoridades de controlo; a criação do cargo de encarregado de proteção de dados; a criação de códigos de conduta, para que sejam explicitadas regras especifica de segurança de dados aplicáveis num determinado segmento da sociedade*."[107] Um conjunto de princípios que "*poderão, se implementado contribuir para o cumprimento do princípio da responsabilidade*"[108] a que fica obrigado as entidades de recolha e tratamento de dados pessoais.

[107] Cf. RGPD (2016, artigos 35º, 36º e 40º).
[108] Cf. RGPD (2016, artigo 35º).

Capítulo V

O Mercado de Dados Pessoais

5.1. Os Dados Pessoais como Nova Matéria-Prima

Os dados se converteram na nova matéria-prima do mundo económico. Como afirma Clive Humby [109] os dados são o novo petróleo com a particularidade de que o petróleo um dia poderá acabar, enquanto os dados se multiplicam a cada segundo. Afirma ainda o matemático inglês, que assim como o petróleo precisa ser refinado, os dados, quando analisados, são uma ferramenta poderosíssima, permitindo tomadas de decisões eficientes.

O aparecimento da Internet impulsionou o desenvolvimento das tecnologias de informação e comunicação, com acesso a uma grande quantidade de informações o que permitiu a criação de novas oportunidades de negócio em diversas atividades, em especial económicas, intelectuais e criativas. Logo, aumenta a capacidade das empresas na recolha de informações o que lhes vão permitir conhecer melhor os seus gostos, as suas necessidades dos consumidores e com isso fazer o *marketing one to one*, propondo ao cliente a oferta correspondente às suas necessidades.

De facto, o advento da Internet e o desenvolvimento das tecnologias permitiram maior difusão e circulação de informações sobre pessoas, entidades e instituições públicas e privadas, nacionais e internacionais, em diferentes partes do mundo e, desta forma, aumentar os riscos de estas pessoas, entidades e empresas verem seus dados na posse de terceiros, que deles poderão, de forma ilícita ou abusiva, tirar vantagens económicas e ou outras.

Com efeito, afirma Belleil (2001, p. 18) "*A Internet traz a doença: a concorrência. A Internet proporciona o remedio: a personalização. Porém, o efeito secundário é mais nefasto que a própria doença, a destruição da vida privada, fruto da coleta desenfreada de dados*."

Aliás, como escreve Guerra (1999, p. 109), *"a Internet veio impulsionar o desenvolvimento da sociedade de informação, permitindo às empresas a aquisição,*

[109] Clive Humby é matemático e empresário na área de dados e estratégias. Autor de vários livros, *Scoring Points: How Tesco Continues to Win Costumer Loyalty*, publicado em 2008, pela Kogan Page Editora; *Conseguir Pontos*, publicado em 2000, pela Paperback Editora, acedido em https://medium.com/project-2030/data-is-new-oil-a-ludicrous-proposition-1d91bba4f294, consultado a 12 de dezembro de 2019.

armazenamento, processamento, valorização, transmissão e distribuição de informações que, por um lado, possibilitaram a criação de conhecimento e, por outro lado a satisfação das necessidades dos indivíduos, com impacto na melhoria da qualidade de vida e consequentemente da atividade económica." Com efeito, as empresas vão apoiar-se nas tecnologias de informação e comunicação, particularmente a informática para tratar os dados pessoais e armazenar informação sobre o indivíduo, visto que começaram a consciencializar sobre o valor económico e os dados pessoais relativos à identidade, gostos, hábitos, constituem uma verdadeira matéria-prima, fonte de riqueza para as empresas.

Como afirma Belleil, (2001, p. 22) "*Diz-me quem és, lucrarei o suficiente para te poder oferecer gratuitamente este serviço*."

Como forma de evitar que as empresas procedam ao tratamento dos dados pessoais de forma indevida, com foco apenas em interesses comerciais, são introduzidos mecanismos legislativos capazes de, por um lado, manter o equilíbrio necessário entre os interesses relativos ao processo económico e o desenvolvimento do comércio, que não prejudicasse a defesa e respeito pelos direitos fundamentais das pessoas singulares[110]e, por outro lado reforçar e garantir o respeito pelos dados pessoais e a salvaguarda da reserva da vida privada e das famílias dos titulares dos dados.[111]

Na verdade, os dados pessoais são o maior ativo e a matéria-prima mais valiosa, sendo por isso muito apetecida pelas empresas de diferentes áreas. Por isso, o seu tratamento deve respeitar, como anteriormente referidos, os direitos dos titulares e os princípios do seu tratamento, como o consentimento, a limitação do fim para que foi originariamente recolhida, assim como o direito de oposição,[112] como forma de colocar barreiras necessárias à comercialização deste tipo de informação. Porque, como afirma Miguel Batista (citado em Pereira, 2002, p. 243) "*A conversão da informação em mercadoria armazenada com fins lucrativos é sinónimo de degradação e de enfraquecimento da corrente contínua, que deve irrigar a sociedade.*"

[110] Cf. Guerra (1999, p. 109).
[111] *Ibidem.*
[112] Cf. RGPD (2016, artigos 5º e ss; 12º e ss).

Entretanto, numa economia com um mercado sem barreiras alfandegárias de qualquer espécie, em que os dados pessoais são a matéria-prima mais comercializável e rentável, os fornecedores de serviços procuram recolher esses dados de maneira ainda mais sistematizada, para melhor conhecer o perfil dos utilizadores e facilitarem a personalização dos serviços, criando aquilo a que Gonçalves (2003, p. 122) chama de uma verdadeira "*economia de vigilância*".

A "*economia de vigilância*", como é designada por Pereira (2003), permitiu aparecimento de empresas que vão ter como produto os dados. Algumas empresas vão dedicar-se à recolha e tratamento de dados sobre os consumidores, particularmente no que se refere a gosto, preferências dos consumidores. Com efeito, vão poder oferecer aquilo que os clientes realmente precisam, sem perda de tempo, com a qualidade e o efeito desejado.

As empresas tendo estas e outras informações vão poder elaborar os perfis dos titulares de dados, que são consumidores, podendo desta forma personalizar os seus serviços e poder praticar o *marketing one to one.*

Esta é uma prática a que as empresas recorrem com relativa frequência e que todos os utilizadores das redes sociais atualmente estão, consciente ou inconscientes, sujeitos. Veja-se o caso do *Facebook*, recentemente multada pelas autoridades europeias, por ter-se apoderado dos dados dos seus utilizadores, violando os princípios do consentimento e da limitação. Outro exemplo dessa prática consiste no facto de a banca utilizar dados dos clientes, principalmente dos melhores cumpridores para reduzir os juros ou atribuir outras vantagens para estes clientes, fidelizando-os. Com isto, fica evidente que as empresas fazem recolha e tratamento, com ou sem consentimento, dos dados dos consumidores dos seus serviços e assim melhorar os seus serviços e produtos.

A prova de que as empresas fazem tratamento dos dados pessoais dos consumidores, em alguns casos com acesso inclusive a dados sensíveis, foi o facto reportado em 2012 pelo *the new York times* numa reportagem, em que uma empresa, através de um *software* previu que uma consumidora estaria grávida através da análise de compras de loções. Com efeito, a empresa poderia, na posse destas informações, tirar vantagens em relação à concorrência e modelar as compras futuras desta consumidora.

Portanto, estas práticas, próprias da atual "*economia de vigilância*", com os dados a serem transformados em matéria-prima para a criação de perfis de comportamento, de consumo e de opções culturais e políticas,[113] evidenciam que nem toda a recolha e análise de dados são realizadas em respeito ao equilíbrio que deve existir "*entre os interesses relativos ao processo económico e o desenvolvimento do comércio, que prejudicasse a defesa e respeito pelos direitos fundamentais das pessoas singulares*" (Guerra, 1999, p. 109).

Note-se, portanto que as empresas procuram cada vez mais recolher e armazenar dados pessoais, que, com o desenvolvimento crescente e linear das tecnologias de informação e comunicação e sua massificação, têm aumentado a cada milissegundo, aumentando, por um lado, a disponibilidade desta nova matéria-prima e alargar o seu mercado, e, por outro os riscos que a sua recolha e tratamento têm para a privacidade dos titulares dos dados pessoais.

O crescimento do mercado de dados pessoais tem pela frente um ingente que é a garantia do direito à privacidade. Ou melhor, o mercado de dados para crescer tem de driblar os direitos dos titulares de dados pessoais, em especial o direito à privacidade dos titulares de dados.

Portanto, a questão que se coloca é como conseguir esse equilíbrio referido por Guerra (1999) entre os interesses de desenvolvimento económico e a garantia dos direitos fundamentais.

Se a economia atual faz-se com e através de dados, sua recolha e tratamento, com implicações diretas e imprevisíveis para os direitos dos seus titulares e a concorrência necessária ao equilíbrio do próprio mercado, torna-se imperativo controlar e regular o acesso, recolha, utilização, armazenamento, partilha e outras formas de tratamento de dados pessoais, permitindo o desenvolvimento das economias, mas em observância dos princípios fundamentais de tratamento de dados e respeito pelos direitos dos seus titulares.

Para isso, entidades com responsabilidades em matéria de proteção dos dados e defesa dos direitos fundamentais, em especial o direito à privacidade, devem atuar e fazer cumprir os

[113] Nos casos em que os clientes querem ser tratados como "VIP" (Personalidade de Primeira Classe) ou desejam serem lembradas em ocasiões ou datas especiais, disponibilizam às empresas informações pessoais, como número de telefone, data de nascimento, endereço, entre outros dados pessoais, que são recolhidas e armazenadas pelas empresas, permitindo que criem perfis destes clientes e poder disponibilizá-los os melhores serviços e a melhores preços.

normativos existentes sobre esta matéria. Além disso, se os dados podem ser transacionados ou comercializados "*o direito à privacidade, [sendo um direito fundamental], não pode ser cedido por quem dele beneficia, nem mesmo mediante uma contrapartida*" (Belleil, 2001, p. 27).

Ora, a Constituição da República Portuguesa, no artigo 26º reconhece a todos que:

> *Os direitos (...) à reserva da intimidade da vida privada e familiar (...). A mesma lei fundamental, no artigo 35º, nº 1, 2 e 3, determina que todos os cidadãos têm o direito de acesso aos dados informáticos que lhes digam respeito, podendo exigir a sua retificação e atualização (...), de conhecer a finalidade a que se se destina (...), [que] a lei determina as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização e garante a sua proteção (...) [que] A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidárias ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular (...) com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis*.

Outrossim, o legislador teve a preocupação de definir os dados pessoais, de modo a permitir uma aplicação clara e eficaz da lei de proteção de dados e garantir o direito à privacidade e outros direitos dos titulares de dados consagrados na constituição e na lei. Para isso, a Diretiva 95/46/CE, de 24 de outubro, define dados pessoais como "*qualquer informação relativa a uma pessoa singular identificada ou identificável (...) é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social"*.

Importa, no entanto, observar que a lei a Lei 67/98, de 26 de outubro, e o Regulamento Geral de Proteção de Dados, na linha da Diretiva 95/46/CE, de 24 de outubro, definem também dados pessoais.

Assim, a Lei 67/98, de 26 de outubro, define como dados pessoais "*qualquer informação, de qualquer natureza e independentemente do respetivos suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerável identificável a pessoa que possa ser identificada direta ou indiretamente,*

designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica cultural ou social."[114]

Por sua vez, o Regulamento Geral de Proteção de Dados, considera dados pessoais "*informação relativa a uma pessoa singular identificada ou identificável (titular dos dado); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um indentificador, como por exemplo um nome, um número de identificação dados de localização, identificadores por via eletrónica ou a um mais elemento específicos da identidade física, fisiológica, genética, metal, económica, cultural ou social dessa pessoa singular*"[115]

Note-se, portanto, que estas definições apresentam algumas particularidades que importam aqui identificar e analisar.

Os dados pessoais referem-se a «*qualquer informação*». Pode-se ver que a expressão «*qualquer pessoa*» é abrangente, na medida em que abrange toda a informação sobre uma pessoa, quer seja sobre a sua vida privada quer seja sobre a sua atividade profissional ou ainda relacionada com o comportamento económico e social do titular, não se importando, portanto, com a veracidade ou não desta informação.

Importa, portanto, que sejam dados referentes a uma pessoa e que permitam, com relativa precisão, identificar, direta ou indiretamente, uma pessoa determinada. Com efeito, sempre que informações sobre uma «*coisa*» permitem, ainda que indiretamente identificar, com alguma precisão, uma pessoa determinada, estas informações têm natureza de dados pessoais.[116]

[114] Cf. Lei a Lei 67/98, de 26 de outubro, artigo nº 3º, alínea a).
[115] Cf. Regulamento Geral de Proteção de Dados (2016, artigo 4º, no 1).
[116] O valor da casa permite, por exemplo, determinar a capacidade do proprietário em pagar o imposto. Esta informação é considerada dados pessoais relativo a uma pessoa determinada, conforme a definição que a Diretiva 95/46/CE, de 24 de outubro, dá de dados pessoais. Nos termos da Lei são exemplos de dados pessoais, o nome, a morada, o telefone, o endereço eletrónico, os dados tratados para efeito de envio de uma comunicação, através de uma rede de comunicação eletrónica, como a sua duração, o tempo ou volume da comunicação, o protocolo utilizado, a localização do equipamento terminal do expedidor ou destinatário, a rede de onde provem ou onde termina a comunicação, o início, o fim ou a duração da ligação, o formato em que a comunicação é enviada pela rede, também o IP do computador, as sequencias de cliques estabelecidas durante a navegação na *world wide web*, bem como os dados de localização.

Uma outra particularidade merecedora de referência é o facto os dados serem referentes a *"pessoa singular identificada ou identificável".* Com isso, são dados pessoais as informações que permitam distinguir com relativa precisão uma pessoa singular de outras pessoas.[117] Isto é, são informações que permitem identificar determinada pessoa "*merecedora de respeito as suas liberdade e os seus direitos fundamentais* (…) *independentemente da sua nacionalidade ou residência"* e que *"têm o direito a serem reconhecidas como sujeitos perante a lei*"[118] de outras pessoas.

Neste sentido, para efeito de recolha, tratamento, armazenamento ou transferência, só são consideradas as informações referentes a pessoa singular possível de ser direta ou indiretamente identificada, ficando fora desta classificação os dados referentes a pessoas coletivas e os dados anónimos.

Pelo contrário, os dados pessoais das crianças mereceram uma proteção especial, por se considerar que desconhecem de todo os riscos, "*as consequências e garantias*," bem como os direitos que lhes assistem.[119]

Na verdade, os dados das pessoas coletivas, bem como os dados anónimos de uma pessoa singular não se encontram protegidos por nenhum dos dispositivos normativos acima referidos, especialmente a Diretiva 95/46/CE, de 24 de outubro, talvez por considerar *"não ser possível identificar a pessoa através de dados anónimos, quer seja pelo responsável pelo tratamento ou por qualquer outra pessoa."*[120] Lembre-se que o Regulamento Geral de Proteção de Dados só se aplica a dados pessoais, deixando também fora do seu âmbito de aplicação os dados de pessoas coletivas e os dados anónimos.

Ora, o facto de os dados anónimos e os referentes a pessoas coletivas estarem fora do âmbito de aplicação das legislações existentes em matéria de proteção de dados, especialmente da Lei 67/98, de 26 de outubro e do Regulamento Geral de Proteção de Dados, poderá significar

---

[117] Cf. Parecer 4/2007, de 20 de junho, sobre o conceito de dados pessoais, acedido em https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf, a 20 de dezembro de 2019.
[118] Declaração Universal dos Direitos Humanos, artigo 6º e Diretiva 95/46/CE, de 24 de outubro, artigo 2º.
[119] Cf. RGPD (2016, Considerando nº 38).
[120] Cf. Diretiva 95/46/CE, de 24 de outubro, Considerandos 24 e 26 "*a proteção das pessoas coletivas relativamente ao tratamento de dados que lhes dizem respeito não é afetada pela presente diretiva;" (…) "os princípios da proteção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável."*

uma fragilidade legal, permitindo a prática de alguma ilicitude em matéria de tratamento de dados pessoais, como se verá se seguir.

Os dados pessoais têm aumentado de forma exponencial. Por conseguinte, aumentaram também os processos e mecanismos relativos ao seu processamento, tratamento, transmissão e armazenamento.

A Lei nº 67/98, de 26 de outubro, considera que há tratamento de dados pessoais quando se proceda qualquer operação ou conjunto de operações, com ou sem meios automatizados, tais como "*a recolha, o registo, a organização, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição.*"[121]

Já o Regulamento Geral de Proteção de Dados estabelece que o tratamento de dados é uma "*operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjunto de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.*[122]

Numa primeira leitura, pode-se entender que qualquer operação que tenha como objeto dados pessoais, seja *"a recolha, o registo, a organização, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão"*[123] é considerada tratamento. Com efeito, numa altura em que os dados pessoais aumentam a grande velocidade, sendo também uma nova matéria-prima da "economia de vigilância", será necessário que estas operações sejam realizadas, como já se referiu anteriormente, em respeito do equilíbrio necessário entre os interesses comerciais e o respeito pelos direitos fundamentais, com especial atenção para o direito à privacidade.

[121] Cf. Lei nº 67/98 de 26 de outubro, artigo 3º, alínea a).
[122] Cf. RGPD (2016, artigo 4º, nº 2).
[123] Cf. Lei nº 67/98 de 26 de outubro, artigo 3º, alínea a).

Para tanto, os instrumentos normativos existentes determinam que "*o tratamento de dados deve ser de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais".*[124]

Porém, a massificação da Internet, aliada ao desenvolvimento de tecnologias de 4ª e 5ª gerações, aumentou as operações sobre os dados pessoais, a nova matéria-prima, que passam a ser mais sofisticadas pelo que desafiam as autoridades nacionais e transnacionais à criação de instrumentos sofisticados de controlo da legalidade das operações e dos riscos sempre presentes nos processos de recolha, organização, atualização, armazenamento e portabilidade de informações referentes a pessoas singulares.

Refira-se que os instrumentos legislativos existentes, na sua maioria, recentemente aprovados, além de apresentarem âmbito de aplicação alargado em matéria de tratamento e esclarecerem alguns dos conceitos, como dados pessoais, tratamento, entre outros conceitos, têm-se mostrado bastante para estabelecer a proporcionalidade entre tratamento de dados e garantia dos direitos fundamentais. Com efeito, permitiram também que os Estados instalem instituições vocacionadas para controlarem a observância da lei e proteção dos dados pessoais e da reserva da vida privada, com são as Comissões Nacionais de Proteção de Dados (CNPD).

O RGPD, de validade supranacional, isto é, em todos os Estados-membros da União Europeia (UE), aplica-se "*ao tratamento de dados pessoais por meios total ou parcialmente automatizados ou por meios não automatizado, ou seja, dados contidos em ficheiros estruturados."*[125] Dessa forma, afirma Saldanha (2018, p. 69), "*Permitir que o RGPD se aplicasse apenas a dados automatizados seria deixar um a porta aberta, o que permitiria controlar facilmente as restrições impostas pelo RGPD.*"

Na verdade, o RGPD estatui em que situações os dados pessoais devem ser tratados. Por isso, os dados pessoais não podem ser objeto de qualquer operação se não se verificarem pelo menos uma das situações seguintes: *"o consentimento inequívoco do titular dos dados; necessidade do tratamento para efeito de execução do contrato; cumprimento de uma obrigação jurídica; defesa de interesses vitais do titular dos dados ou de terceiro; exercício de funções do interesse público ou ainda em caso de um interesse legítimo prosseguido pelo*

[124] Cf. Lei nº 67/98 de 26 de outubro, artigo 2º.
[125] Cf. RGPD (2016, artigo 2º).

responsável pelo tratamento, desde que não prevaleçam interesses, direitos ou liberdade fundamentais do titular."[126]

De referir, portanto, que em se tratando de informações de natureza sensíveis, como por exemplo os dados relacionados com origem racial ou étnica, opiniões políticas, convicções políticas ou relativos à saúde, assim como dados pessoais relacionados com a condenação pena e infrações ou medidas de segurança ligadas à proteção de dados, estas só podem ser objeto de qualquer operação *"se o titular der o seu consentimento explícito, para fins específicos; for necessário para proteger interesses vitais do titular, no caso de este estar impossibilitado de dar o seu consentimento; se for efetuado no âmbito de atividades legitimas, ligadas as associações ou outros organismos sem fins lucrativos ou se esses dados foram manifestamente tornados público pelo titular"*[127], entre outras situações semelhantes, e sob a supervisão e controlo de uma entidade pública, que deve acautelar e proteger as garantias necessárias dos direitos e liberdades dos titulares dos dados.

Todavia, pode-se perguntar como será possível garantir que organizações, empresas, entidades ou autoridades não desenvolvem qualquer operação sobre os dados pessoais sem o consentimento expresso dos titulares dos dados, sendo este um dos requisitos legais imprescindível ao tratamento de qualquer dados pessoais, numa era em que o desenvolvimento acelerado das tecnologias de informação e comunicação e das plataformas digitais, redes sociais, têm permitido às pessoas, por motivos profissionais, de entretenimento, saúde, compras *online* ou mesmo em tarefas simples do dia-a-dia, como levantar dinheiro nas caixas ATM ou carregar telefones, a disponibilizarem seus dados pessoais, em tempo real, a instituições, entidades, organizações de natureza diversa.

Pois, se é verdade que as legislações em matéria de proteção de dados determinaram as situações em que os dados pessoais devem ser tratamentos e fixaram os limites desse tratamento, colocando restrições a esse tratamento, não é menos verdade que, por vezes de forma legal, as entidades, empresas ou organizações responsáveis pelo tratamento dos dados pessoais acedem, sem conhecimento e consentimento, a dados pessoais e, com isto, causar danos físicos, materiais ou imateriais como perdas financeiras e com riscos de natureza social

[126] Cf. RGPD (2016, artigo 6º).
[127] Cf. RGPD (2016, artigo 9º e Considerando nº 51 e seguintes).

ou pessoal como desempenho no tratamento, situação económica, interesses pessoais, deslocações para definir ou fazer uso de perfis.

Na verdade, a lei determina as finalidades e os meios de tratamento de dados pessoais, e atribui ao responsável pelo tratamento, entre outras obrigações, *"a aplicar medidas técnicas e organizativas adequadas para assegurar e comprovar que o tratamento seja efetuado em conformidade com o regulamento; adotar medidas de proteção desde a conceção e por defeito;* [e], *em caso de violação de dados pessoais, notificar a autoridade de controlo e ao titular dos dados."*[128]

Ora, a lei determina que cabe ao responsável pelo tratamento dos dados pessoais solicitar o consentimento do titular de dados e, em caso de violação dos dados pessoais, notificar as autoridades de controlo e comunicar o titular dos dados pessoais. Mais, é ao responsável pelo tratamento que cabe *"avaliar se irão cumprir todos os requisitos para obter o consentimento válido",* devendo também *"observar os princípios da lealdade, da necessidade e da proporcionalidade e à qualidade dos dados."*[129]

Sendo assim, pode-se perceber que, sendo os dados pessoais matéria-prima de grande valor económico, e estando a obrigação de obter consentimento, bem como de comunicar as finalidades e, em caso de violação, participar tal facto às autoridades de controlo, as empresas, organizações e entidades responsáveis pelo seu tratamento poderão, sempre que for possível e lhes seja conveniente, contornar tais procedimentos, ainda que sem prejuízos materiais ou pessoais evidentes para os titulares dos dados.

Além disso, o facto de o consentimento, "*qualquer manifestação de vontade, livre, especifica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento*" ou "*manifestação de vontade, livre, especifica, informada e explicita pelo titular dos dados, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*"[130], poder ser obtido oralmente e *"através da conversa telefónica desde que as informações acerca da escolha sejam leais, inteligíveis, claras e solicitada uma confirmação específica ao titular dos dados"*[131], poderá

[128] Cf. RGPD (2016, artigos 24º e ss e Considerandos 74 e ss).
[129] Cf. RGPD (2016, artigo 5º, 9º e 22º, alínea c)).
[130] Cf. Diretiva nº 95/46/CE, de 24 de outubro, artigo 2º, alínea h) e RGPD (2016, artigo 4º, nº 11).
[131] Cf. RGPD (2016, artigo 4º, nº 11).

abrir espaço para que o tratamento se faça fora do quadro legal existente, sendo assim, com riscos para tratamento indevido e abusivo dos dados, constituindo uma violação dos direitos fundamentais dos titulares de dados pessoais.

Pelo acima exposto, pode-se inferir que sendo os dados uma matéria-prima de grande valor económico é evidente que haverá grande interesse de instituições e organizações diversas e até de Estados em recolher, organizar, atualizar, transferir e armazenar dados, particularmente os dados pessoais, para fins diversos, podendo estas operações, sempre que possível serem efetuadas fora do quadro legal, quanto mais não seja numa economia marcadamente digital, um mercado cada vez mais global e um *"mundo de vidro e pessoas eletrónicas"*, com riscos evidentes para os direitos, liberdades e garantias.

Se por um lado, os responsáveis pelo tratamento de dados, considerando os interesses económicos e lucros associados aos dados, poderão procurar, sempre que possível, esquivar os mecanismos de controlo existentes, em especial o consentimento, pilar fundamental no que toca à proteção de dados, por outro lado caberá as autoridades com responsabilidade em matéria de defesa e garantia dos direitos fundamentais, quais sejam o direito à privacidade e à segurança, a efetivação das liberdades e garantias, características dos Estados de Direito Democrático.

5.2. Transferência de Dados para Países Terceiros

Atualmente, como resultado do desenvolvimento tecnológico e da globalização do mercado, as circulações dos dados pessoais tornaram-se comuns, principalmente no mercado digital. Pois, a evolução da tecnologia possibilitou a recolha, armazenamento e partilha dos dados em quantidade e velocidade *record*, o possibilita o desenvolvimento do comércio e da cooperação internacionais. Com isso, a proteção dos dados tornou se um desafio no que toca a garantia do nível de proteção dentro e fora da UE.

Visando a proteção de dados face ao intenso fluxo transfronteiriço dos dados, o RGPD veio estabelecer um conjunto de regras para a circulação dos dados pessoais fora do espaço da UE, isto é, para países terceiros.[132]

[132] O RGPD, no artigo 4º, nº 2, define países terceiros como países não pertencentes ao espaço da União Europeia.

Assim, o RGPD, no artigo 44º, estabelece que "*as transferências de dados para os países terceiros só podem ser realizadas de forma assegurar com o mesmo nível de proteção, tendo como objetivo garantir que as proteções concedidas aos dados na União Europeia os acompanhem, caso sejam objeto de tratamento apos a transferência ao país terceiro*."

Com efeito, "*as transferências de dados entre Estados-membros da União Europeia para os países terceiros devem ser feitas mediante uma decisão da Comissão que ateste a adequação do nível de proteção do país terceiro*."[133] Para isso, a Comissão Europeia deve analisar a ordem jurídica e das práticas do país terceiro e, de seguida, emitir uma decisão que indica a adequação do nível de proteção de dados que existe no país terceiro, no qual se encontra o recetor da transferência dos aludidos dados[134].

Além disso, o RGPD, no artigo 45º, nº 2, alíneas a), b), e c), prevê três dimensões fundamentais a serem consideradas pela Comissão quando da adequação do país terceiro. A primeira dimensão de análise prende-se com a verificação da existência do primado da Estado de direito e o respeito pelos direitos humanos e liberdades fundamentais, tendo em consideração as normas aplicáveis em matérias de segurança pública, defesa, segurança nacional e o direito penal, como também das legislações referentes ao "*acesso das autoridades públicas aos dados pessoais; das regras de proteção de dados; regra de profissionais e medidas de segurança, bem como das legislações referentes à transferência de dados pessoais para o país terceiro*."

Por outro lado, ainda no âmbito do quadro legal existente, a Comissão deverá ter em conta a jurisprudência e as vias de recurso administrativo e judicial que poderão ser utilizadas pelos titulares dos dados. Deverá, igualmente, certificar da existência de autoridades independentes que poderão garantir a observância e a aplicação das normas referentes à proteção de dados pessoais, devendo ser dotadas de poderes coercitivos para prestar auxílio necessário ao titular dos dados quando do exercício dos seus direitos.

Por fim, ainda no quadro das exigências de transferência de dados pessoais para países terceiros, haverá que considerar o grau de assunção de compromissos internacionais, convenções internacionais ou instrumentos jurídicos vinculativos, como também a participação

[133] Cf. RGPD (2016, artigo 45º).
[134] In Comunicação da Comissão ao Parlamento Europeu e ao Conselho (2017), *intercâmbio e proteção de dados num mundo globalizado*, Bruxelas, de 10 de janeiro, acedido em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52017DC0007, consultado em 15 de abril de 2019.

em sistema multinacionais ou regionais, especialmente aqueles relativos a proteção de dados pessoais.

Portanto, é feita uma avaliação global do recetor dos dados, analisando desde a existência de um quadro legal que garanta a proteção dos dados pessoais, a existência de autoridades que garantam a aplicação e a observância das normas de proteção dos dados, bem como a adoção de sistemas através dos quais os titulares dos dados possam fazer valer os seus direitos.

Depois de verificadas as condições no quadro da legislação existente no país terceiro e analisadas o seu grau de compromisso internacionais em termos de proteção de dados pessoais, se a Comissão entender que o país terceiro não reúne os elementos suficientes para garantir uma adequada proteção dados pessoais, emitirá a decisão de adequação que permitirá a transferência dos dados em apreço e só depois o exportador ficará isento de apresentar outras garantias ou autorização para realizar a transferências dos dados.

Pelo contrário, se os referidos elementos não se encontrarem presentes, a Comissão deverá consultar o país terceiro para que corrija os fatores que afetam o nível de adequação dos dados e se nada for feito no sentido de sua adequação a Comissão deverá então revogar, alterar ou suspender a sua decisão de adequação a depender da situação.

Todavia, ainda que não tenham sido feitas as adequações necessárias, anteriormente referidas, poderá a Comissão decidir favoravelmente pela transferência, mas nunca sem que sejam apresentadas as garantias de os titulares dos dados poderem se opor e esteja comprovada a existência de medidas jurídicas corretivas eficazes.[135]

Por sua vez, as clausulas inseridas nos contratos celebrados entre entes privados ou as disposições a prever nos acordos administrativos entre autoridades e organismos públicos, depois de autorizadas pelas autoridades de controlo competente, legitimam as transferências internacionais de dados pessoais. Igualmente, as transferências de dados *"poderão ser realizadas com base num acordo internacional, como por exemplo um acordo de assistência*

[135] Cf. RGPD (2016, artigo 46º, nº 1).

judiciária mútua, em vigor entre os estados membros, a união europeia e os países terceiros."[136]

Porém, na falta de decisão de adequação da Comissão, de garantias adequadas e de acordo internacional, *"as transferências de dados ainda assim serão possíveis com base no consentimento explícito do titular dos dados, apos ter sido informados dos possíveis riscos de tais transferências à privacidade."*[137] Ou ainda, *"poderão realizar-se as transferências de dados necessários para a celebração ou execução de contrato ou diligências prévias pedidas pelo titular dos dados.*"[138]

Além disso, as transferências de dados poderão realizar-se quando forem necessárias para importantes razões públicas, para a declaração, exercício de defesa ou direitos em processos judiciais, para a proteção de interesses vitais dos titulares de dados e dos terceiros e nos casos em que os dados são públicos. Por fim, as transferências serão permitidas se não forem repetitivas e forem oferecidas garantias adequadas, previstas no RGPD (artigo 49º, nº 1, alíneas d), e), f) e g)).

Note-se que sobre esta problemática, o Grupo de Trabalho do Artigo 29.º, antecessor do Comité Europeu para a Proteção de Dados (CEPD), defendeu, durante algum tempo, que a melhor prática consistiria numa abordagem das transferências por níveis, num total de quatro, a começar primeiramente por analisar se o país terceiro tem um nível de proteção adequado, de seguida assegurar que os dados exportados serão devidamente protegidos no país terceiro.

No entanto, se o nível de proteção não for adequado, atendendo todas as circunstâncias, o exportador de dados deve considerar a possibilidade de apresentar garantias adequadas.

Por conseguinte, os exportadores de dados devem começar por procurar enquadrar a transferência no quadro dos mecanismos previstos nos artigos 45.º e 46.º do RGPD e, na sua falta, recorrer às derrogações estabelecidas no artigo 49.º, n.º 1 do mesmo documento.

[136] Cf. RGPD (2016, artigo 48º).
[137] Cf. RGPD (2016, artigo 49º, nº 1, alínea a)).
[138] Cf. RGPD (2016, artigo 49º, nº 1, alíneas b) e c)).

Para tanto, as derrogações previstas no RGPD e acima referidas são exceções à aplicação do princípio geral de que os dados pessoais só podem ser transferidos para países terceiros se estes oferecerem um nível de proteção adequado, ou se tiverem sido apresentadas garantias adequadas e os titulares dos dados usufruírem de direitos efetivos e oponíveis, que lhes permitam continuar a beneficiar dos seus direitos e garantias fundamentais.

De referir, portando, que as derrogações devem ser interpretadas de forma restritiva, para que a exceção se não torne na regra, uma vez que as derrogações não proporcionam aos dados pessoais transferidos nem proteção adequada nem garantias adequadas, e o facto de as transferências baseadas numa derrogação não estarem sujeitas a qualquer tipo de autorização das autoridades de controlo, podendo acarretar riscos acrescidos para os direitos e liberdades dos titulares dos dados em causa.

Outrossim, os exportadores de dados devem estar igualmente cientes de que, na falta de uma decisão de adequação, o direito da União ou de um Estado-membro pode, por razões importantes de interesse público, limitar expressamente as transferências de categorias específicas de dados pessoais para países terceiros ou organizações internacionais.[139]

Ainda em relação às transferências de dados para países terceiros, o RGPD, no artigo 48º, introduz uma nova disposição que tem de ser tida em conta na ponderação de transferências de dados pessoais.

Assim, determina o RGPD, no artigo 48º, que "*as decisões de autoridades e órgãos jurisdicionais de países terceiros não constituem, por si só, um fundamento legítimo para transferências de dados para países terceiros*." Consequentemente, as transferências em resposta a decisões de autoridades de países terceiros só serão, em qualquer caso, legítimas se satisfizerem as condições pré-estabelecidas. Ou seja, quando exista um acordo internacional, como um acordo de assistência judiciária mútua, as empresas da UE devem, de um modo geral, recusar os pedidos diretos e remeter a autoridade requerente do país terceiro para o acordo existente.

[139] RGPD (2016, artigo 49.º, n.º 5).

Lembre-se que este entendimento está em estreita consonância com o artigo 44º do referido regulamento, que estabelece um princípio geral aplicável a todas as disposições do capítulo V, a fim de evitar que seja comprometido o nível de proteção das pessoas singulares garantido pelo RGPD.

Portanto, as condições gerais para que o consentimento seja considerado válido estão definidas no RGPD, artigos 4º, nº 11, e 7º. Por outro lado, o Grupo de Trabalho do Artigo 29.º formula um conjunto de orientações sobre essas condições gerais em documento separado.

De referir que essas condições se aplicam igualmente ao consentimento no contexto do RGPD, artigo 49.º, n.º 1, alínea a). Contudo, existem outros requisitos específicos necessários e exigidos para que o consentimento seja considerado um fundamento legal válido e as transferências internacionais de dados para países terceiros e organizações internacionais sejam realizadas dentro do quadro legal estabelecido.

Importa, no entanto, observar também que as garantias adequadas aplicáveis às empresas, nas transferências de dados pessoais para países terceiros ou organizações internacionais, só poderão ser efetuadas se *"o titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas.*"[140]

Na verdade, o consentimento, por força da lei, deve ser livre, específico, informado e explícito. Este requisito também é um fundamento válido e deve ser dado especificamente para essa transferência, ou conjunto de transferências, de dados.

O elemento «*especificidade*», constante da definição de «consentimento» visa assegurar ao titular dos dados um certo grau de controlo do utilizador e a transparência. Para tanto, deve ser específico o que, por vezes não é possível obter, sobretudo se, à data da recolha dos dados para uma transferência futura, a ocorrência e as circunstâncias concretas de uma transferência não forem conhecidas à data em que o consentimento.

[140] Cf. RGPD (20116, 49º, nº 1).

Imagine-se que uma empresa da União Europeia (UE) procedeu a recolha dos dados dos seus clientes para um fim específico sem prever, nessa altura, a transferência desses dados para países terceiros e, anos depois, essa empresa é adquirida por uma outra empresa de um país terceiro e esta empresa pretende transferir os dados pessoais dos seus clientes para outra empresa fora da UE. Para que a transferência seja válida ao abrigo da derrogação baseada no consentimento, o titular dos dados deve dar o seu consentimento para essa transferência específica no momento da sua previsão.

Por conseguinte, o consentimento dado à data da recolha dos dados pela empresa da UE não é suficiente para justificar o recurso a esta derrogação para uma transferência posterior dos dados pessoais para fora da União. O exportador dos dados tem, pois, de se certificar de que obtém um consentimento específico antes de a transferência ser decidida, ainda que tal aconteça depois de a recolha dos dados ter sido efetuada.

Na verdade, o consentimento deve ser informado, em particular quanto aos possíveis riscos da transferência. Esta condição é particularmente importante na medida em que reforça e precisa o requisito geral do «consentimento informado», aplicável a qualquer consentimento.

Além do mais, se forem transferidos dados pessoais para um país terceiro ao abrigo do artigo 49.º, n.º 1, alínea a) do RGPD, os titulares dos dados devem, por força desta disposição, ser igualmente informados dos riscos específicos resultantes do facto de os seus dados serem transferidos para um país que não oferece um nível adequado de proteção dos dados e de não serem dadas garantias adequadas dessa proteção.

Deve-se observar que a comunicação destas informações é essencial para que o titular dos dados possa dar o seu consentimento com pleno conhecimento das circunstâncias específicas da transferência, pelo que, se lhe não forem comunicadas essas informações, a derrogação não será aplicável.

Ademais, se a transferência for efetuada depois da recolha dos dados pessoais, o exportador de dados deve informar o titular sobre a transferência e os seus riscos, antes de a efetuar, para obter o seu consentimento explícito para a transferência «*prevista*».

Importa, portanto, dizer que as derrogações relativas à execução de um contrato são limitadas pelos critérios da «*necessidade*» e das «*transferências ocasionais*». Exige, por isso, uma ligação estreita e substancial entre a transferência de dados e as finalidades do contrato.

Neste caso, a derrogação não pode ser utilizada para fins empresariais, se tiver centralizado num país terceiro as funções de pagamento e de gestão de recursos humanos de todo o seu pessoal, e não existir uma ligação direta e objetiva entre a execução do contrato de trabalho e essa transferência.

Porém, poderão ser adequados para essa transferência específica outros fundamentos para transferências, como os das cláusulas contratuais normalizadas e das regras vinculativas aplicáveis às empresas.

Assim, esta derrogação não pode ser aplicada a transferências de informações complementares que não sejam necessárias para a execução do contrato ou para diligências prévias à celebração do contrato, solicitadas pelo titular dos dados.

Neste contexto, pode considerar-se que uma transferência é ocasional se, por exemplo, os dados pessoais de um gestor de vendas, que, no âmbito do seu contrato de trabalho, visite diversos clientes em países terceiros, forem enviados a esses clientes para organização das reuniões.

Poderá também ser considerada ocasional a transferência, por um banco estabelecido na UE, de dados pessoais para um banco estabelecido num país terceiro, a fim de executar a ordem de pagamento dada por um cliente, desde que essa transferência não ocorra no âmbito de uma relação de cooperação estável entre os dois bancos.

Pelo contrário, se uma empresa multinacional que organize cursos de formação num centro de formação de um país terceiro e transfira sistematicamente os dados pessoais dos trabalhadores que frequentem um curso de formação, essas transferências não podem ser consideradas «*ocasionais*».

Pois, as transferências regulares de dados no âmbito de uma relação estável são consideradas sistemáticas e repetidas, porquanto não têm caráter «*ocasional*».

Por conseguinte, além do «*critério da necessidade*», também neste caso só é possível transferir dados pessoais ao abrigo desta derrogação se a transferência for ocasional.

Se uma organização tiver, para fins empresariais, externalizado atividades como a gestão dos salários a prestadores de serviços estabelecidos fora da UE, esta derrogação não serve de base para transferências de dados com tais fins, porquanto não ser possível estabelecer se uma ligação estreita e substancial entre a transferência e um contrato celebrado no interesse do titular dos dados, mesmo que o fim último da transferência seja a gestão do salário do trabalhador.

Acresce que os dados pessoais só podem ser transferidos ao abrigo desta derrogação se a transferência for ocasional. Assim, para se verificar se tal transferência é ocasional, deve aplicar-se os mesmos critérios anteriormente referidos, porque, caso contrário, esta derrogação não pode ser aplicada, nem em a atividades exercidas por autoridades públicas na sua esfera de competências.

Contudo, para que a derrogação seja aplicada, não basta que a transferência de dados seja pedida (por exemplo, por uma autoridade de um país terceiro) para fins de um inquérito que sirva um interesse público de um país terceiro, que, em termos abstratos, também exista no direito da UE ou do Estado-Membro.

Em suma, a transferência de dados pessoais para países terceiros deve respeitar um conjunto de critérios que são controlados pelo país exportador e exigidos ao país recetor, desde consentimento dos titulares, critério fundamental da licitude do ato e da proteção dos dados, bem como as garantias de adequação pelos países terceiros, como as garantias na ordem jurídicas que devem ser verificadas no sentido de garantia de existência de um Estado de Direito e, por outro existência de garantias efetiva de defesa dos direitos dos titulares dos dados, como também o grau de compromisso do país terceiro no que respeita às convenções internacionais, entre outros instrumentos internacionais com força de vinculação interna.

5.3. Fiscalização e Sanções

A violação de dados pessoais é "*violação de segurança que provoque, de modo acidental ou ilícito, a destruição, perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer tipo de tratamento*".[141]

É neste sentido que o RGPD, no artigo 33º, determina que, em caso de violação de dados pessoais, fica o responsável pelo tratamento *obrigado "a notificar a autoridade de controlo competente, no prazo de 72 horas apos o conhecimento da violação, sem demora injustificada e ou acompanhada de justificação dos motivos do atraso"*[142].

Da referida notificação deve constar, entre outras informações, *"descrição da natureza da violação de dados; categorias e o número aproximado de registo de dados pessoais afetados; nome e os contactos do DPO, assim como a descrição das consequências prováveis da violação* [e] *das medidas tomadas/proposta pelo responsável pelo tratamento, para reparar a violação de dados pessoais, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos negativos."*[143]

Todavia, se a violação de dados recair sobre informações suscetíveis de representar um alto risco para os direitos e liberdade dos seus titulares, deve o responsável pelo tratamento comunicar a tal violação ao titular dos dados em linguagem clara e simples.

Refira-se, portanto, que existem situações em que a notificação ao titular não é obrigatória, como quando a violação reporta a *"dados que tenham sido, objeto de medidas adequadas de proteção, tornando-os incompreensíveis para quem violou esses dados ou quando forem tomadas de imediato medidas para mitigar totalmente o risco para os direito e liberdades dos titulares dos dados*, bem como se *"a violação implicar um esforço desproporcionado, casos em que é necessário recorrer a comunicação pública para informar os titulares dos dados da violação*"[144].

[141] Cf. RGPD (2016, artigo 4º, nº 12).
[142] Cf. RGPD (2016, artigo 33º).
[143] Cf. Saldanha (2018, p. 97).
[144] Cf. RGPD (2016, artigo 34º) e Considerando nº 85 e ss.

Em matéria de violação dos dados pessoais o RGPD, no artigo 35º introduziu uma inovação importante, que é a Avaliação de Impacto da Proteção de Dados (AIPD) como *"um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face aos riscos"*[145].

Por outro lado, a AIPD tem uma abrangência sobre todas as *"operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação*"[146]. Isto é, uma única AIPD pode ser utilizada para avaliar múltiplas operações que o tratamento seja semelhante, quanto a natureza, âmbito, contexto, finalidade e riscos.

Portanto, concentrar numa única entidade o controlo de todas as operações sobre os dados pessoais poderá ter ganhos em termos de unidade de decisões e evitar conflitos de competências, mas poderá não representar ganhos em termos de garantias dos direitos dos titulares de dados e riscos associados às operações de tratamento, pese embora a realização de AIPD não seja obrigatória em todas as operações de tratamento, mormente nas operações que não impliquem elevados riscos para os direitos e as liberdades das pessoas singulares.

Pelo contrário, nas operações de tratamento de dados "*suscetíveis de implicar um elevado risco para os direitos liberdades das pessoas singulares*" estão sujeitas à realização da AIPD e devem ser considerados, entre outros critérios, as *"Decisões automatizada que produzam efeito jurídicos ou afetem significativamente de modo similar; Controlo sistemático; Dados sensíveis ou de natureza altamente pessoal; Dados tratados em grande escala; Tratamento que estabeleçam correspondências ou combinem conjuntos se dados; Dados relativos a titulares de dados vulneráveis; Utilização de soluções inovadoras ou aplicações de novas soluções tecnológicas ou organizacionais;"* [especialmente] *"Quando o próprio tratamento impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um controlo."*[147]

[145] O RGPD (2016, no artigo 35º, nº 7) define formalmente a Avaliação de Impacto da Proteção de Dados (AIPD).
[146] Cf. RGPD (2026, artigo 35º, nº 1).
[147] O grupo de trabalho do art.º 29 "*orientações relativas à avaliação de impacto sobre a proteção de dados e que determinam se o tratamento é suscetível de resultar num elevado risco" para efeitos do Regulamento (EU) 2016/679* " acedido em https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf, consultado em 2 de setembro de 2018.

Pois, para o Grupo de Trabalho do artigo 29º, *"quanto mais critérios forem satisfeitos pelo tratamento maior é a probabilidade de este implicar um elevado riscos para os direitos e as liberdades dos titulares dos dados e consequentemente necessitar de uma AIPD, independentemente das medidas que o responsável pelo tratamento adotar*"[148].

Porém, o Grupo de Trabalho do Artigo 29º considera, por outro lado, que AIPD não é obrigatório quando, entre outras situações, o tratamento não for "*suscetíveis de implicar um elevado riscos para os direitos e liberdades das pessoas singulares"* ou "*a natureza, o âmbito, o contexto e as finalidades do tratamento forem muito semelhantes ao tratamento em relação ao qual tenha sido realizada uma AIPD, podendo utilizar os resultados da AIPD realizada para o tratamento semelhante.*"[149]

Todavia, sempre que necessária, a AIPD deve ser realizada antes de se iniciar o tratamento e continuamente ao longo do ciclo de vida do processo, garantindo assim, a proteção dos dados e a privacidade dos dados, devendo ser realizada responsável pelo tratamento, com o encarregado do tratamento dos dados e os subcontratantes[150].

No que respeita aos mecanismos de garantia de proteção dos dados pessoais e da privacidade dos titulares, o RGPD estabelece as penalizações a aplicar em caso de incumprimento das disposições legais que regulam as operações que tenham como objeto dados pessoais.

Quanto a fiscalização, a autoridade de controlo tem a responsabilidade pela fiscalização da aplicação do regulamento, visando defender os direitos e liberdade fundamentais das pessoas singulares relativas ao tratamento de dados e facilitar a livre circulação desses dados na União europeia. Podendo ainda, afirma Pereira e Magalhães (2018, p. 63) "aplicar uma coima e as medidas corretivas conforme a gravidade da violação."

Assim, determina o RGPD, sem prejuízo da intervenção da autoridade de controlo ou cumulativamente com esta, qualquer interessado poderá, em caso de violação dos seus direitos

[148] O grupo de trabalho do art.º 29 "*orientações relativas à avaliação de impacto sobre a proteção de dados e que determinam se o tratamento é suscetível de resultar num elevado risco*" para efeitos do Regulamento (EU) 2016/679 " acedido em https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf, consultado em 2 de setembro de 2018.
[149] Cf. RGPD (2016, artigo 35º, nº1).
[150] Cf. Grupo de Trabalho do Artigo 29º, sobre o encarregado da proteção de dados, 16/EN WP 243.

recorrer às instâncias jurisdicionais e de responsabilidade intentar contra o responsável pelo tratamento dos dados, ao subcontratante e a qualquer outro terceiro que trata ou conserva dados pessoais.

De referir que a lei determina um conjunto de responsabilidades a aplicar no tratamento de dados, como sejam a "*Responsabilidade criminal decorrente da prática de crimes; Responsabilidade contraordenacionais; Responsabilidade civil; Responsabilidade social e disciplinar*."[151]

Além de a lei determinar um conjunto de responsabilidades aos responsáveis de tratamento de dados pessoais em caso de violação, prevê igualmente espaço à contestação e recursos, podendo ser pela "*via administrativa, reclamação apresentada à autoridade de controlo do Estado-Membro, da sua residência, do seu local de trabalho, ou do local onde foi praticado a violação dos dados pessoais, e a via judicial, recurso aos tribunais, em que os titulares dos dados ao considerarem ter havido a violação dos seus dados nos termos do RGPD, na sequencia do tratamento dos seus dados, tem direito de apresentar ações judiciais contra o responsável pelo tratamento dos dados ou subcontratante*." Neste caso, as ações, determina a lei, "*devem ser interpostas nos tribunais do Estado-Membro ou no Estado-Membro onde o titular tenha a sua residência*"[152].

Pois, a finalidade das ações administrativa ou judicias é o reconhecimento da existência de um dano material ou imaterial consequência da violação, devendo desses danos o titular dos direitos violados receber uma indeminização do responsável pelo tratamento dos dados ou subcontratantes, uma vez que toda e qualquer violação da Lei é punida.

Neste sentido, o RGPD, no artigo 84º, para além das coimas impõe sanções e determina que "*os Estado-Membro estabelecem as regras relativas às outras sanções aplicáveis em caso de violação do disposto no presente regulamento, nomeadamente às violações que não são sujeitas a coimas nos termos do artigo 83º, e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas*".

[151] Cf. RGPD (2016, artigos 77º e ss).
[152] *Ibidem.*

Para isso, o RGPD impõe *sanções penais*, cabendo assim *aos Estados- Membros definirem quais as sanções penais, aplicáveis por violação do RGPD; sanções administrativas* em que as autoridades de controlo têm o poder de advertir, repreenderem, ordenar ou impor uma certa atuação, e por fim, *sanções pecuniárias* em que serão aplicadas uma "*coima até 10 000 000 Euro ou, no caso de empresa, até 2% do seu volume de negócio anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado*:

a) *As obrigações do responsável pelo tratamento e do subcontratante nos ternos dos artigos 8º, 11º, 25º, a 39º, e 42º e 43º;*
b) *As obrigações dos organismos de certificação nos termos dos artigos 42º e 43º;*
c) *As obrigações do organismos de supervisão nos termos do art.º 41º nº 4."*[153]

Já nos casos de violação dos princípios, de direitos individuais, de regras respeitantes a transferência de dados ou ainda violada uma ordem imposta pela autoridade de controlo:

> *A coima até 20 000 000 euro, no caso de uma empresa, até 4% do seu volume de negócio anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado:*
> *a) Os principais básicos do tratamento, incluindo as condições de consentimento, nos termos dos artigos 5º, 6º, 7º, e 9º;*
> *b) Os direitos dos titulares dos dados nos termos 12º a 22º;*
> *c) As transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional nos termos dos artigos 44º a 49º;*
> *d) As obrigações nos termos do direito do Estado-Membro adotado ao abrigo do capítulo IX;*
> *e) O incumprimento de uma ordem de limitação, temporária ou definitiva, relativa ao tratamento ou à suspensão de fluxos de dados, emitida pela autoridade de controlo nos termos do art.º 58º, nº 2, ou facto de não facultar acesso, em violação do artigo 58º, nº1*[154].

Note-se que o RGPD, no artigo 83º, nº 2, prevê também coimas pesadas para situações de *"incumprimento de uma ordem emitida pela autoridade de controlo a que se refere o artigo 58º, nº 2, está sujeito, em conformidade com o nº2 do presente artigo, a coima até 20 000 000 EUR ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado*[155]*"*.

[153] Cf. RGPD (2016, artigo 83º).
[154] Cf. RGPD (2016, artigo 83º nº 5).
[155] Cf. RGPD (2016, Considerando nº148 e ss).

Em síntese, pode-se afirmar que a fiscalização das operações que têm como objeto os dados pessoais tem constituído um desafio das autoridades com responsabilidade na proteção dos dados pessoais e, em consequência, redução dos riscos associados e garantia dos direitos fundamentais.

As legislações existentes, em termos de âmbito de aplicação, têm conseguido responder ao desafios e a responsabilidade dos Estados-Membros e não só, no que respeita à proteção dos dados pessoais e garantir que tratamento se faça em observância das lei, de forma adequada e correta durante todo o processo, sendo certo que existem ainda alguns aspetos que, consequência do desenvolvimento tecnológico e com ele a diluição das barreiras, dificultam, em alguns casos, a aplicação das legislações e a atuação das autoridades, no sentido de garantirem uma proteção efetiva dos dados pessoais de tratamentos indevidos, responsabilizando os responsáveis, civil e criminalmente, ressarcindo os titulares de dados em caso de dados materiais e/ou outros.

Conclusão

Quando se partiu para a elaboração deste trabalho de investigação, abordando a problemática da proteção de dados e do direito à privacidade na era digital, a primeira preocupação foi a de tentar perceber em que medida o desenvolvimento da tecnologia de informação e comunicação e, sobretudo, da internet poderão ter alterado a fronteira da vida privada, com prejuízos para o direito à privacidade.

A resposta a esta pergunta foi apresentada através da hipótese formulada na parte inicial da presente dissertação em que se pretendeu saber se os mecanismos institucionais existentes, em especial os normativos são suficientes perante os desafios da atual sociedade de informação (mundo digital) em matéria de proteção de dados pessoais e, em consequência, o direito a privacidade.

O direito a privacidade é tutelado em vários instrumentos jurídicos internacional como nacional. A nível nacional na ordem jurídica portuguesa é tutelado por toda ordem jurídica, desde a Constituição da República, no direito civil, direito penal e administrativo, encontrando a sua proteção, de forma particular, com a sua regulamentação no RGPD.

Atualmente, com o avanço da tecnologia, da administração pública eletrónica, entre outros, o conceito da privacidade não reside mais na garantia de isolamento físico e segredo, mas sim no poder de controlar as informações sobre si que os outros possam ter ou tenham acesso, assim como a finalidade que é dada as mesmas.

Vive-se, como é evidente, numa era assente na tecnologia digital, onde facilmente são recolhidos dados pessoais e outros independentemente do espaço físico, quer se esteja dentro ou fora de casa. Com efeito, nas ruas é vigiado pelas camaras de videovigilância, nos transportes públicos os passes recolhem as informações pessoais, no trabalho a entrada é controlada através do registo eletrónico de dados biométricos, e nem em casa se está a salvo dessas «*perseguições*».

Por outro lado, vive-se numa época em que se assiste, como afirma Correia (2016, p.87) um certo "*show* do eu", em que as pessoas, voluntariamente, consentem a divulgação dos seus dados, sem consciência das reais implicações desses atos. Este é apenas um dos muitos

exemplos de como, voluntária ou involuntariamente, independentemente do lugar físico a privacidade fica comprometida por conta dos dados recolhidos.

Com a globalização o conceito da privacidade vai além do que é feito de portas fachadas, com implicações também na intimidade, ou seja, a *"esfera do não dito não revelado"*, onde estão os dados mais sensíveis. De facto, aos poucos vai-se cedendo, restringindo e comprimindo o direito à privacidade, passando a viver como um mero objeto de informação.

Visando a salvaguarda dos direitos fundamentais e o respeito pelo princípio da dignidade da pessoa humana, as Constituições e as leis têm velado pela sua garantia, foram introduzidos vários instrumentos legislativos, internacionais e nacionais, que tutelam a proteção de dados pessoais, como a Constituição da República, a Diretiva 95/46/CE, de 24 de Outubro, a Lei nº 67/98, de 26 de Outubro, Lei de Proteção de Dados Pessoais, e o Regulamento Geral de Proteção dos Dados.

De certa forma, as referidas legislações foram se adaptando ao desenvolvimento tecnológico, como consequência do surgimento e massificação do acesso a Internet e, não permitindo que o mundo digital se transformasse num espaço sem regulamentação.

Na verdade, o uso das tecnologias da informação e de comunicação expõe o indivíduo no seu núcleo pessoal, o que resulta em vulnerabilidade, do ponto de vista da privacidade, face aos que detêm a informação pessoal, com repercussão nos direitos fundamentais, chegando, por vezes, a gerar conflitos só possíveis de resolução com recurso à teoria dos limites imanentes dos direitos constitucionais para a sua resolução.

Pois, pode-se constatar que, em determinadas situações, valores fundamentais como o direito a privacidade e o direito a segurança não podiam ser asseguradas de forma efetiva e ao mesmo tempo. Uma situação que se consubstancia numa tensão entre esses direitos ou valores de igual valor constitucional, uma vez que o exercício do direito a privacidade poderá colidir com o exercício do direito a segurança, gerando uma situação de tensão, solucionada com recursos a diversos critérios, especialmente pelo princípio da proporcionalidade, teorizado por autores como Alexy (2008), Bobbio (2004) e também presente no RGPD, em que perante princípios equivalentes abstratamente, prevalecerá, no caso concreto, o que tiver maior peso diante das circunstâncias.

Ao longo do presente trabalho, analisou-se também o mercado de dados pessoais, como nova matéria-prima, constituindo, por isso, um risco maior para a privacidade, visto que empresas, organizações e entidades diversas poderão proceder ao seu tratamento fora do quadro legal existente e beneficiarem com as possibilidades de recolhas e tratamento dos dados, enquanto mercadoria.

Na verdade, com o aumento do fluxo de dados, em consequência do desenvolvimento tecnológico, é possível, através de dados pessoais, analisar a situação económica dos clientes, assim como o perfil dos consumidores passando a fazer marketing *«one to one»*.

A transferência de dados pessoais para países terceiros, ainda que com consentimento explícito do titular, um dos fundamentos importantes para a licitude do processo de tratamento de dados pessoais, deve ser realizada dentro do quadro legal existente, com garantias das condições de adequação e sem quaisquer riscos para os titulares.

Pelo contrário, em caso de violação dos dados pessoais, os responsáveis pelo tratamento, quer no país exportador quer no país recetor, são responsabilizados com sanções e coimas, sendo ainda garantidas aos titulares os meios de reclamação, no sentido de serem ressarcidos pelos dados causados.

Contudo, na era digital, em que a vida privada poderá facilmente ser exposta, em consequência de os dados se encontrarem ao alcance de um clique, fica evidente que apesar de existir um quadro legal abrangente e atualizado, os riscos associados ao tratamento dos dados pessoais, com consequências para os direitos fundamentais, são reais e com repercussão no próprio Estado de Direito.

Porém, não será abusivo afirmar que somente a regulamentação não será suficiente para fazer face as violações dos direitos fundamentais e da proteção dos dados. Pensa-se, pois, que a sensibilização e a tomada de consciência da parte dos titulares dos dados para a importância de se precaverem dos seus direitos, em especial o direito à privacidade, será a primeira forma de proteção.

À guisa da conclusão, parece possível afirmar que a dissertação, apesar das várias dificuldades encontradas no âmbito da investigação, conseguiu encontrar repostas para as perguntas inicialmente formuladas e que serviram de base para a elaboração deste trabalho.

No entanto, a mestranda está consciente de que esta dissertação constitui apenas o ponto de partida para um estudo superior, certamente mais complexo e completo, sobre a problemática da proteção de dados e dos direitos fundamentais, em especial do direito à privacidade na era digital.

Bibliografia

Alexy, R. (2008). *Teoria dos Direitos Fundamentais*. São Paulo: Malheiros Editores Ltda.

Belleil, A. (2001). *@- privacidade, o mercado dos dados pessoais: proteção da vida privada na internet.* Lisboa: Instituto Piaget.

Bobbio, N. (2004). *Era dos Direitos.* 7ª Tiragem. Rio de Janeiro: Editora Campus/ Elsevier.

Canotilho, J. J. & Moreira, V. (2007). *Constituição da República Portuguesa Anotada*. (Vol. I). 4.ª ed. rev.). Coimbra: Coimbra Editora.

_____ (1997). *Direito Constitucional e Teoria da Constituição.* (4. ed.) Coimbra: Almedina.

Castro, C. S. e. (2005). *Direito da Informática, Privacidade e Dados pessoais.* Coimbra: Edições Almedina, SA.

Correia, M. P. (2009). *Conformação de contratos pela publicidade na Internet*. In Ascensão, J. O. coord. – Direito da Sociedade da Informação. (Vol. VIII). Coimbra: Coimbra Editora.

Farinho, D. S. (2006). *Intimidade da vida privada e media no ciberespaço*. Lisboa: Edições Almedina.

Frada, J.J.C. (1991). *Guia prática para elaboração de teses e trabalhos científicos*. Lisboa: Cosmos.

Gonçalves, M. E. (2003). *Direito da Informação. Novos direitos e formas de regulação na sociedade da informação*. Coimbra: Almedina.

Guerra, A. (1999). *Informática e privacidade – Nova lei de proteção de dados e a lei de proteção de dados no sector de telecomunicações*. Lisboa: Vislis Editores Lda.

_____ (2001). *A lei da proteção de dados pessoais.* In Direito da Sociedade da Informação. (Vol. II). Coimbra: Coimbra Editora.

Magalhães, F. M, & Pereira, M. P. (2018). *Regulamento Geral de Proteção de Dados- Manual Prático*. (2ª ed.). Porto: Vida Económica – Editorial, SA.

Marques, G. & Lourenço, M. (2006). *Direito da Informática.* (2.ª ed. rev. e act.) Coimbra: Edições Almedina, SA.

Martins, A.G. L. (2003). *Criminalidade Informática.* In Direito da Sociedade da Informação. (Vol. IV). Coimbra: Coimbra Editora.

Pereira, A. D. (2002). *Bases de Dados de Órgãos Públicos: O Problema do Acesso e exploração da Informação do Sector Público na Sociedade da Informação* In Direito da Sociedade de informação. (Vol. III). Coimbra: Coimbra Editora.

Reis Novais, J. (2004). *Os Princípios Constitucionais Estruturantes da República Portuguesa*. Coimbra: Coimbra Editora.

Saldanha, N. (2018). *Novo Regulamento Geral de Proteção de Dados. O que é? A quem se aplica? Como implementar?* Lisboa: FCA- Editora de Informática, LDA.

_____ (2019). *RGPD – Guia para uma auditoria de conformidade – Dados, privacidade, implementação, controlo, compliance. Lisboa: FCA – Editora de Informática Lda.*

Sampaio, J.A.L, (1998). *"Direito à Intimidade e à vida privada".* Belo Horizonte: Del Rey

Vaz, A. (2007). *Segurança da informação, proteção da privacidade e dados pessoais*. In Nação e Defesa. Nº 117, 3ª Série.

Bibliografia Consultada não Citada

Ascensão, J. O. (2003). *A distribuição de mensagens de correio eletrónico indesejadas (Spam)*. In Direito da Sociedade da Informação. (Vol. IV). Coimbra: Coimbra Editora.

_____ (2009). *Publicidade na Rede*. In Direito da Sociedade da Informação. (Vol. VIII). Coimbra: Coimbra Editora.

_____ (2009). *A sociedade digital e o consumidor*. In Direito da Sociedade da Informação. (Vol. VIII). Coimbra: Coimbra Editora.

_____ (2009). *Dispositivos tecnológicos de proteção, direitos de acesso e uso dos bens*. In Direito da Sociedade da Informação. (Vol. VIII). Coimbra: Coimbra Editora.

Ferreira, P. (2006). *A Proteção de Dados Pessoais na Sociedade de Comunicação: Dados de Tráfego, Dados de Localização e Testemunho de Conexão.* Lisboa: O Espírito das leis editora, Lda.

Leitão, A. M. (2003). *Metatags e correio eletrónico entre os novos problemas do direito da internet*. In Direito da Sociedade da Informação. (Vol. IV). Coimbra: Coimbra Editora.

Lisboa Neto, A. (2010). *Código Civil anotado.* (17.ª ed. rev e act.) Lisboa: EDIFORUM Edições Jurídicas.

Miranda, J. (2012). *Manual de Direito Constitucional.* Tomo IV. (5.ª ed.). Coimbra: Coimbra Editora.

Pina, P. (2009*). Direitos do autor, autodeterminação informativa e panoptismo digital.* In Direito da Sociedade da Informação. (Vol. VIII). Coimbra: Coimbra Editora.

Pinheiro, A. S. (2015). *Privacy e Proteção de dados pessoais: a construção dogmática do direito à identidade informacional.* Lisboa: Associação Académica da Faculdade de Direito de Lisboa.

Rodrigues, L. S. (2003). *Os consumidores e a sociedade da informação.* In Direito da Sociedade da Informação. (Vol. IV). Coimbra: Coimbra Editora.

Serra, C. S. (2003). *Publicidade ilícita e abusiva na internet.* In Direito da Sociedade da Informação. (Vol. IV). Coimbra: Coimbra Editora.

Silva, P. C. e (2003). *A contratação automatizada.* In Direito da Sociedade da Informação. (Vol. IV). Coimbra: Coimbra Editora.

Verdelho, P. (2009*). Phishing e outras formas de defraudação nas redes de comunicação.* In Direito da Sociedade da Informação. (Vol. VIII). Coimbra: Coimbra Editora.

Legislações

Constituição da República Portuguesa (2010).

Código Civil de Português (1966).

Diretiva 95/46/CE, de 24 de outubro de 1995, relativa à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Lei nº 67/98, de 26 de outubro, Lei de Proteção de Dados Pessoais.

Lei nº 58/2019, de 8 de agosto, Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Documentos Eletrónicos, Revistas e Publicações Oficiais

- Comissão Nacional de Proteção de Dados - Fórum de Proteção de dados nº 01 Julho 2015 Semestral " *O Novo Quadro Legal Europeu*" [Em linha].Lisboa CNPD.[Consult.07/02/2018].Disponível em https://www.cnpd.pt/bin/revistaforum/forum2015_1/files/assets/basic-html/page-1.html

- Comissão Nacional de Proteção de Dados - Fórum de Proteção de dados nº 02 Janeiro 2016 Semestral "40 Anos da Constituição e do Direito à Proteção de Dados" [Em linha].Lisboa CNPD.[Consult.07/02/2018].Disponível em https://www.cnpd.pt/bin/revistaforum/forum2016_2/files/assets/basic-html/page-I.html#

- Comissão Nacional de Proteção de Dados - Fórum de Proteção de dados nº 03 Julho 2016 Semestral "*Geolocalização*" [Em linha].Lisboa CNPD.[Consult.07/02/2018].Disponível em https://www.cnpd.pt/bin/revistaforum/forum2016_3/files/assets/basic-html/page-I.html

- Comissão Nacional de Proteção de Dados - Fórum de Proteção de dados nº 04 Julho 2017 Semestral, "*Inteligência Artificial*" [Em linha].Lisboa CNPD.[Consult.07/02/2018].Disponível em https://www.cnpd.pt/bin/revistaforum/forum2017_1/files/assets/basic-html/page-I.html#

- Comissão Nacional de Proteção de Dados - Fórum de Proteção de dados nº 05 Novembro 2018 Semestral, "*RGPD Desafios do Mecanismos de Coerência*" [Em linha].Lisboa CNPD.[Consult.07/01/2018].Disponível em https://www.cnpd.pt/bin/revistaforum/forum2018_5/index.html

- Lei nº 67/98, de 26 de outubro [Em linha]. Diário da República 1ª serie Nº247. (26/10/1998) p. 5536-5546. [consult.02/04/2018]. Disponível em https://dre.pt/application/conteudo/239857

- Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados, Documento de trabalho sobre questões relativas à proteção de dados no âmbito da tecnologia RFID (WP 105), adotado em 19 de janeiro de 2005, disponível em http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinionrecommendation/files/2005/wp105_en.pdf.

- Grupo de Trabalho do Artigo 29º para a Proteção de dados, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 Adotadas em 4 de abril de 2017 Revistas e adotadas pela última vez em 4 de outubro de 2017 consultado disponível https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pd

- Grupo de Trabalho do Artigo 29º para a Proteção de dados, Orientações sobre o direito à portabilidade dos dados Adotadas em 13 de dezembro de 2016 Com a última redação revista e adotada em 5 de abril de 2017, consultado 15/10/2018, disponível em https://www.cnpd.pt/bin/rgpd/docs/wp242rev01_pt.pdf

- Parecer 8/2006 sobre a revisão do quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, com destaque para a Diretiva relativa à privacidade e às comunicações eletrónicas (WP 126), de 26 de Setembro de 2006, disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp126_pt.pdf .

- Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde eletrónicos *(RSE)* (WP 131), de 15 de fevereiro de 2007, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_pt.pdf

- Parecer 4/2007 sobre o conceito de dados pessoais (WP 136), de 20 de junho de 2007, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pt.pdf

- Parecer 2/2008 sobre a revisão da Diretiva 2002/58/CE relativa à privacidade no sector das comunicações eletrónicas (Diretiva Privacidade Eletrónica) (WP 150), de 15 de maio de 2008, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_pt.pdf

- Parecer 1/2009 sobre as propostas de alteração da Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (diretiva da privacidade eletrónica) (WP 159), de 10 de fevereiro de 2009, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_pt.pdf

- Parecer 15/2011 sobre a definição de consentimento Adotado em 13 Julho de 2011 disponível em https://www.gpdp.gov.mo/uploadfile/others/wp187_pt.pdf

- Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante» Adotado em 16 de Fevereiro de 2010 disponível em https://www.gpdp.gov.mo/uploadfile/others/wp169_pt.pdf

- Parecer 3/ 2013 sobre limitação da finalidade adotado em 2 de abril de 2013 disponível em https://www.gpdp.gov.mo/uploadfile/2017/0127/20170127113320522.pdf

- Parecer 03/2014 relativo à notificação da violação de dados pessoais Adotado em 25 de março de 2014 disponível em https://www.gpdp.gov.mo/uploadfile/2016/0112/20160112121813272.pdf

- Parecer 03/2014 relativo à notificação da violação de dados pessoais Adotado em 25 de março de 2014, consultado 03/05/2018, disponível em https://www.gpdp.gov.mo/uploadfile/2016/0112/20160112121813272.pdf

UNIÃO EUROPEIA. Grupo de Trabalho do Artigo 29º- Parecer 5//2012 relativo a computação em nuvens.01037/12/PT GT 196 [Em linha]. Bruxelas : Grupo de Trabalho, (01/07/2012) [Consult.08 fev. 2018]. Disponível em https://www.gpdp.gov.mo/uploadfile/others/wp196_pt.pdf.

- Anuário de Proteção de Dados de 2018 disponível em http://cedis.fd.unl.pt/blog/project/anuario-da-protecao-de-dados-2018/

- Anuário de Proteção de Dados de 2019 disponível em https://www.dpo-portugal.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf

- Comissão nacional de Proteção de dados, relatórios de atividades 2017-2018, disponível em https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201718.pdf

Jurisprudências e Acórdãos

- Tribunal Europeu dos Direitos do Homem. Processo n.º 27798/95, [Em linha] (16/02/2000) [Consult. 15 Jan. 2017]. Disponível em http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"appno":["27798/95"]}

- Tribunal da Relação de Guimarães: Processo n.º 1341/08.4TAVCT, relator (a) Anselmo Lopes, Tribunal da Relação de Guimarães, [Em linha] (12/04/2010) [Consult. 20 Junho de 2019]. Disponível em www.dgsi.pt.

- Tribunal da Relação de Guimarães: Processo n.º 2013/04-1, relator (a) Francisco Marcolino [Em linha] (10/01/2005) [Consult. 20 junho de 2015]. Disponível em www.dgsi.pt.

- Tribunal da Relação de Lisboa: Processo n.º 1695/09.5PJLSB.L1-9, relator (a) Margarida Vieira de Almeida [Em linha] (19/06/2014) [Consult. 25 Nov. 2019]. Disponível em www.dgsi.pt.

- Tribunal da relação de Évora: Processo n.º789/13.7TMSTB-B.E1, relator (a) Bernardo Domingos [Em linha] (25/06/2015) [Consult. 15 de Mar. 2018]. Disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/7c52769f1dfab8be80257e830052d374.

- Acórdão do Tribunal Constitucional: n.º 403/2015 Processo n.º 773/15 Acordam, em Plenário, no Tribunal Constitucional[Em linha] [Consult. 29 de fev. 2020] Disponível em https://dre.pt/application/conteudo/70300353

Índice Remissivo

A

Alexy, Robert - 44, 45, 96

B

Belleil, Arnaud - 40, 69, 73

Bobbio, Norberto - 44, 45, 96

C

Canotilho, José Joaquim Gomes - 22, 35, 37, 44, 52

Castro, Catarina Sarmento e - 19, 23, 25, 29, 41, 49, 52, 54, 59, 61

Clive Humby - 69

Correia, Miguel Pupo - 34, 36, 38, 40, 42, 52, 95

D

Dias, José Eduardo Figueiredo - 51

F

Farinho, Domingos Soares - 46, 53

Frada, João José Cúcio - 17

G

Gonçalves, Maria Eduarda - 35, 41, 51, 71

Guerra, Amadeu - 35, 70, 72

L

Louis Brandeis, 34

Lourenço, Martins - 18, 27, 28, 29, 34, 35, 37, 52, 57

M

Machado, - 52

Magalhães, Filipa - 53, 56, 57, 91
Marques, Garcia - 18, 27, 28, 29, 34, 35, 37, 51, 52
Miguel Batista - 70
Moreira, Vital - 22, 35, 37

N

Novais Reis, José - 53

P

Paulo Mota Pinto - 35, 38, 52, 53
Pereira, Alexandre Dias - 53, 56, 70, 91

S

Saldanha, Nuno - 28, 32, 48, 52, 62, 65, 89
Sampaio, José Adércio Leite - 34
Samuel Warren - 34

V

Vasconcelos, Pedro Bacelar - 38, 39
Vaz, A - 47, 49