UNIVERSIDADE D
COIMBRA

Beatriz da Costa Gomes Leite

PROTEÇÃO DE DADOS E PRIVACIDADE EM LINHA

Dissertação de Mestrado em Ciências Jurídico-Forenses, orientada pelo Professor Doutor Alexandre Libório Dias Pereira e apresentada à Faculdade de Direito da Universidade de Coimbra.

Outubro de 2021

Beatriz da Costa Gomes Leite

Proteção de Dados e Privacidade em Linha

Data Protection and Online Privacy

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º Ciclo de Estudos em Direito (conducente ao grau de Mestre) na Área de Especialização em Ciências Jurídico-Forenses.

Orientador: Alexandre Libório Dias Pereira

Coimbra, 2021.

"A alegria está na luta, na tentativa, no sofrimento envolvido e não na vitória propriamente dita"

Mahatma Gandhi

Agradecimentos

Aqui chegada, tenho muito que agradecer a todos os meus Professores Doutores da Faculdade de Direito da Universidade de Coimbra, a quem muito devo, pois, sem eles, não tinha adquirido as capacidades, sem as quais, não completaria mais um Ciclo de Estudos nesta instituição.

Ao meu Orientador, Senhor Professor Doutor Alexandre Libório Dias Pereira que, aceitou de uma forma célere e afável, orientar a presente dissertação.

À minha família, em especial à minha Mãe, que me apoiou incondicionalmente ao longo de todo o meu percurso académico.

Aos meus sobrinhos, que me proporcionaram pausas e momentos de descontração, importantes para renovar energias e adquirir motivação e inspiração extra.

À minha madrinha e padrinho, que sempre acreditaram em mim, nas minhas capacidades, e que, nunca me faltaram com uma palavra certa nos momentos que mais precisei.

À minha madrinha de praxe, Cristiana Gonçalves, que ao longo de todos estes anos me ajudou a superar todas as dificuldades, acreditando sempre comigo que, não há um desafio que não seja possível de superar.

Às minhas fiéis amigas, Joana Coimbra e Ana Horta, por me acompanharem e apoiarem desde o tempo de caloiras.

À minha Patrona, Dr.ª Vânia Marques, que consentiu em muitas das minhas ausências para que conseguisse concluir este projeto, pela sua postura compreensiva e amável com a qual sempre me tratou, mesmo quando era difícil conciliar a escrita com os trabalhos no escritório e, pela sua infindável partilha de conhecimentos.

Ao meu namorado, que tal como eu, acredita que o melhor investimento que fazemos é em nós, na nossa educação.

Resumo

A presente dissertação versa sobre a Proteção de Dados e Privacidade em Linha (online), a qual tem vindo a ser fortemente discutida, atendendo aos consideráveis avanços tecnológicos que têm ocorrido, mas também, devido à atual necessidade de acesso e tratamento de dados pessoais no combate ao vírus Covid-19 (Pandemia).

Para tanto, o presente trabalho foi dividido em três capítulos, nos quais se pretende realizar uma abordagem gradual do tema.

Primeiramente, explanando sobre a Privacidade e a Proteção de Dados, ou seja, a Privacidade (direito sobre a reserva da intimidade da vida privada) como fonte primária, mas distinta da Proteção de Dados. A origem da Privacidade e a sua Proteção a nível supranacional, europeu e nacional. O Direito de Proteção de Dados e respetiva evolução (nos Estados Unidos da América e Europa). E, por último, as Fontes de Direito de Proteção de Dados (tanto na Europa como em Portugal).

Seguidamente, abordando o Regulamento Geral de Proteção de Dados, os seus conceitos básicos, princípios, âmbito de aplicação material e territorial, os direitos dos titulares de proteção de dados, o responsável pelo tratamento, a autoridade de controlo e a lei de execução.

Por fim, discorrendo acerca do Direito à Proteção de dados em tempos de pandemia, mais concretamente, sobre até que ponto podem ser limitados os direitos de proteção dos dados pessoais aos seus titulares com fundamento na crise de saúde pública e sobre as aplicações de "*contact tracing",* mais especificamente, a StayAway Covid-19.

Palavras-Chave: Privacidade; - Proteção de Dados; - Regulamento Geral de Proteção de Dados (RGPD); Pandemia;

Abstract

This dissertation deals with Online Data Protection and Privacy, which has been strongly discussed, given the considerable technological advances that have occurred, but also due to the current need for access and processing of personal data in the fight against the Covid-19 virus (Pandemic).

To this end, the present work was divided into three chapters, in which a gradual approach to the theme is intended.

First, explaining about Privacy and Data Protection, that is, Privacy (right over the privacy of private life) as a primary source, but distinct from Data Protection. The origin of Privacy and its Protection at the supranational, European and national levels. The Data Protection Law and its evolution (in the United States and Europe). And finally, the Sources of Data Protection Law (both in Europe and in Portugal).

Next, addressing the General Data Protection Regulation, its basic concepts, principles, material and territorial scope, the rights of the data protection owners, the controller, the supervisory authority, the enforcement law.

Finally, discussing the Right to Data Protection in times of a pandemic, more specifically, to what extent can personal data protection rights of data subjects be limited based on the public health crisis and on contact tracing applications, more specifically, StayAway Covid-19.

KeyWords: Privacy; - Data Protection; - General Data Protection Regulation (GDPR); - Pandemic;

Lista Siglas e Abreviaturas

Art.- Artigo;

CRP- Constituição da República Portuguesa;

CC – Código Civil;

DUDH- Declaração Universal dos Direitos do Homem;

CDHLF- Convenção dos Direitos do Homem e das Liberdades Fundamentais;

PIDCP - Pacto Internacional dos Direitos Civis e Políticos;

EUA- Estados Unidos da América;

ONU- Organização das Nações Unidas;

RGPD- Regulamento Geral da Proteção de Dados;

HDSG- *Hessisches Datenschutzgesetz;*

BDSG- *Bundestag;*

OCDE- Organização para a Cooperação e Desenvolvimento Económico;

TJUE- Tribunal Judicial da União Europeia;

TEDH- Tribunal Europeu dos Direitos Humanos;

CEDH- Convenção Europeia dos Direitos do Homem;

CNPD- Comissão Nacional de Proteção de Dados;

LE – Lei de Execução;

TUE – Tratado da União Europeia;

TFUE- Tratado de Funcionamento da União Europeia;

UE- União Europeia;

CEPD- Comité Europeu para a Proteção de Dados;

INESC- Instituto de Engenharia de Sistemas e Computadores;

ISPUP- Instituto de Saúde Pública da Universidade do Porto;

WP 29 - Grupo de Trabalho do Artigo 29º.

Índice

Introdução

A Privacidade é um *direito de personalidade*[1] consagrado no artigo 80º do Código Civil (CC) e, simultaneamente, *um direito fundamental* previsto no artigo 12º da Declaração Universal dos Direitos Humanos (DUDH), no artigo 8º da Convenção dos Direitos do Homem e das Liberdades Fundamentais (CDHLF), no artigo 17º do Pacto Internacional dos Direitos Civis e Políticos (PIDCP) e nos artigos 26º, 34º e 35º da Constituição da República Portuguesa (CRP).

O Direito de Proteção de Dados é um *direito fundamental*[2] previsto no artigo 8º da Carta dos Direitos Fundamentais da União Europeia, e no artigo 35º, nº 2 da Constituição da República Portuguesa.

O Direito à Privacidade (*reserva sobre a intimidade da vida privada*) e o Direito à Proteção de Dados, apesar de aparentarem ter a mesma formulação e alcance, o facto é que, estes são dissemelhantes. O Direito à Proteção de dados é mais abrangente que o Direito à Privacidade, não se limitando a abranger a tutela do direito à privacidade, mas de tantos outros direitos, como por exemplo, o direito à liberdade de expressão, liberdade de transformação, direito à saúde, direito à não discriminação, etc.

Tanto o Direito à Privacidade, como o Direito à Proteção de Dados, têm vindo a sofrer diversas alterações desde a sua origem até à atualidade, por força das transformações

---

[1] *Os Direitos de personalidade* estão consagrados no Direito Civil, pois destina-se a tutelar os sujeitos de agressões provenientes daqueles que são seus pares, ou seja, é uma tutela que recai sobre as relações horizontais (sujeito-sujeito).

O Direito geral à personalidade, adquirido aquando da nascença (artigo 66º do Código Civil), é ilimitado e ilimitável, por forma a abranger todas as manifestações previsíveis e imprevisíveis da pessoa, enquanto ser em constante desenvolvimento e mutação. Abrange tanto a pessoa física, espiritual e psicológica dos indivíduos – artigo 70º, nº 1 do Código Civil – *"A lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral".*

O Direito à personalidade pode revestir vários domínios, direito ao nome, direito à imagem, etc. (artigos 72º a 80º do Código Civil).

[2] *Os Direitos Fundamentais* consistem em posições jurídicas básicas reconhecidas tanto pelo direito português, como o europeu e internacional com vista à defesa dos valores e interesses mais relevantes das pessoas singulares e coletivas. À luz da Constituição da República Portuguesa (CRP) existem duas grandes categorias de direitos fundamentais: os "direitos, liberdades e garantias" (por exemplo, o direito à liberdade e à segurança, à integridade física e moral, à propriedade privada, à participação política e à liberdade de expressão) e os "direitos e deveres económicos, sociais e culturais" (por exemplo, o direito ao trabalho, à habitação, à segurança social, ao ambiente e à qualidade de vida).

Os Direitos fundamentais visam assim, proteger os sujeitos de interações com o Estado, ou seja, nas relações verticais (Estado- sujeito).

provocadas na realidade jurídica, pela evolução humana, informática e tecnológica. A partir do Séc. XX, a evolução tecnológica sofreu diversas transformações, permitindo que as barreiras de tempo e espaço fossem passíveis de serem superadas. Em pleno Séc. XXI é possível, a comunicação em tempo real (videochamada) entre familiares/colegas de trabalho em pontos opostos do mundo; o acesso por toda a comunidade mundial a uma fotografia/ notícia atrás de um simples "*click" (redes sociais)*; residir num país, mas ser estudante noutro (Escola/ Universidade *Online)*; aceder ao banco e realizar compras sem sair do sofá; fazer pesquisas bibliográficas sem necessitar de ir a uma biblioteca física, etc.

Ora, a evolução tecnológica contém vários benefícios para a sociedade, no entanto, comporta riscos, principalmente, o acesso e partilha a dados pessoais sem limites/fronteiras, que fazem urgir uma necessidade indispensável de proteção jurídica sólida, coerente e flexível (compatível com a veloz evolução dos mecanismos tecnológicos por forma a que proteção não se torne obsoleta e ineficaz).

O Regulamento Geral de Proteção de Dados (RGPD), no seu Considerando (6), constata o seguinte, *"A rápida evolução e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados internacionais, assegurando simultaneamente um elevado nível de proteção de dados pessoais".*

Isto posto, considero que, é necessário compreender primeiramente o Direito à Privacidade e o Direito à Proteção de Dados, a sua origem e evolução, para de seguida entender o Regulamento Geral de Proteção de Dados (RGPD), como principal fonte de Direito de Proteção de Dados em vigência na Europa (de aplicabilidade direta nos seus Estados- Membros) e, por último, atentar ao último acontecimento a nível mundial, a Pandemia provocada pela Covid-19, percecionando o impacto que determinados mecanismos tecnológicos podem gerar na proteção dos dados pessoais.

CAPÍTULO I - A PRIVACIDADE E A PROTEÇÃO DE DADOS

O Direito à Privacidade e o Direito à proteção de dados pessoais distinguem-se na sua formulação e alcance.

O *Direito à Privacidade,* é reconhecido no artigo 8º da Convenção Europeia dos Direitos Humanos (CEDH) e no artigo 12º da Declaração Universal dos Direitos Humanos (DUDH), como direito fundamental, logo, a sua limitação só se justificará quando estiver em causa a proteção de um interesse coletivo relevante (por exemplo, a saúde pública).

O *Direito da proteção de dados pessoais* é um direito fundamental, previsto no artigo 8º da Carta dos Direitos Fundamentais da União Europeia e no artigo 35º da CRP. Este consiste num mecanismo de segurança e proteção do titular de dados, ou seja, é um direito (moderno e dinâmico) que é convocado no âmbito de qualquer operação de tratamento de dados pessoais, com um alcance mais amplo que o direito à privacidade, pois, tutela todas as operações e categorias de dados pessoais, independentemente da relação estabelecida com a privacidade e com os impactos de daí possam advir. [3]

1.1. Privacidade

A Constituição da República Portuguesa (doravante CRP), no elenco dos direitos, liberdades e garantias, reconhece o direito à reserva sobre a intimidade privada, *"A todos são reconhecidos os direitos à identidade pessoal, ao 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 à proteção legal contra quaisquer formas de discriminação"* – artigo 26, nº 1 da CRP.

Ora, o direito à reserva sobre a intimidade da vida privada, é um direito de personalidade, consagrado no artigo 80º do CC *"todos devem guardar reserva quanto à intimidade da vida privada de outrem"* que está diretamente ligado ao princípio da dignidade da pessoa humana baseado no pressuposto que beneficia de um espaço de privacidade sob dois "sub- direitos", *i)* o direito de impedir o acesso a terceiros a informações

[3] Dias, Patrícia Cardoso. "Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública*",* pág. 4. Revista Julgar Online. Janeiro de 2021.

sobre a vida privada e familiar; *ii)* o direito a que ninguém divulgue as informações sobre a vida privada de outrem, traduzindo-o numa verdadeira proibição de ingerência na vida particular por terceiros, quer por acesso, quer por divulgação de informação. [4]

1.1.1. Origem

A ideia de privacidade surgiu com a publicação, em 1890, do artigo de Samuel D. Warren e Louis D. Brandeis – *"The right to privacy"* na *Havard Law Review*, no qual, o direito à privacidade era perspetivado como um direito "não-intrusão" (o direito de o indivíduo estar livre de intrusões públicas não autorizadas), de "ser deixado só" – "*The right to be let alone"*.

No século XIX, foram ocorrendo várias transformações sociais, políticas e económicas devido às novas invenções, tais como, a fotografia, que permitia a captação de imagens de forma oculta. Contudo, o reconhecimento do direito à privacidade nos EUA, ainda não era absoluto, nem automático, limitando-se a casos de mero interesse público e a publicações consentidas.

Não obstante, após o grande impacto da publicação do já referido artigo de Samuel D. Warren e Louis D. Brandeis, sucederam-se casos julgados de forma diversa, nomeadamente, o caso "*Flour the Family*"[5] e um outro de escutas telefónicas (no qual o tribunal não reconheceu que, sendo estas o principal meio de prova, não tinham sido obtidas com invasão da propriedade privada).

Ora, as várias limitações e restrições do direito de privacidade dos cidadãos (imagem e propriedade) levaram a que, fosse reconhecido o direito à publicidade – "*right of publicity"* e que, fosse também incorporado na Constituição Norte Americana o "*right of privacy"* na sequência do voto do juiz Douglas (sucessor de Brandeis no Supremo Tribunal dos Estados Unidos) – "*se é que o direito à intimidade significa alguma coisa, é o direito do*

[4] Carvalho, Maria João; Lopes, Paulo Simões, *"Da privacidade à proteção de dados", Coimbra,* 16 de dezembro de 2019 - https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/da_privacidade_a_protecao_de_dados

[5] Publicação não autorizada de uma fotografia do rosto de uma senhora num cartaz publicitário de um fabricante de farinha.

indivíduo, casado ou solteiro, de se ver livre contra intromissões estatais indevidas em assuntos tão fundamentalmente afetos à pessoa como a decisão de ter ou evitar ter filhos"[6].

1.1.2. A Proteção da Privacidade

A proteção da privacidade, no ***Direito Supranacional***, em geral, encontra-se prevista em várias diplomas legais, nomeadamente, na Declaração Americana de Direitos e Deveres do Homem, consagrada na IX Conferência Internacional de 1948, em Bogotá; na Declaração Universal dos Direitos do Homem, adotada pela Organização das Nações Unidas (ONU), em 1948, no seu artigo 12º - *" Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei";* no Pacto Internacional relativo a direitos civis e políticos, aprovada pela Assembleia Geral da ONU em 1976, no seu artigo 17º - *"Ninguém será objeto de ingerências arbitrárias ou ilegais à sua honra e reputação. Toda a pessoa tem direito a proteção da lei contra essas ingerências ou esses ataques".* [7]

*No **Direito Europeu***, encontra-se previsto na Convenção Europeia dos Direitos do Homem, de 1950 no seu artigo 8º, nº 1- " *Qualquer pessoa tem o direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência"* e nº 2 *"Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública para o bem-estar económico do país, a defesa da ordem e prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros".*

*Em **Portugal***, a Constituição da República Portuguesa prevê no artigo 26º, nº1 – "*a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da*

[6] Carvalho, Maria João; Lopes, Paulo Simões "*Da privacidade à proteção de dados", Coimbra,* 16 de dezembro de 2019 - https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/da_privacidade_a_protecao_de_dados

[7] Carvalho, Maria João; Lopes, Paulo Simões "*Da privacidade à proteção de dados", Coimbra,* 16 de dezembro de 2019 - https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/da_privacidade_a_protecao_de_dados

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 à proteção legal contra quaisquer formas de discriminação" e no artigo 35º (utilização informática) no qual prevê a tutela dos direitos pessoais quando os dados pessoais dos cidadãos sejam informatizados (retificação, atualização, conhecer a finalidade, conexão, transmissão, utilização, etc.).

1.2. A Proteção de Dados

O Direito da Proteção de Dados consiste, sinteticamente, na proteção da posição jurídica dos titulares dos dados pessoais e dos seus respetivos direitos, ou seja, consiste num direito à autodeterminação informacional[8].

1.2.1. Estados Unidos da América

A) *Special Subcommitte on Invasion of Privacy*

A proteção de dados contemporânea inicia-se na década de 60 do séc. XX. Contudo, a necessidade de se regular autonomamente a proteção de dados, surgiu apenas com os grandes avanços tecnológicos que, permitiram recolher e tratar dados pessoais em grande escala (bases de dados).

Em 1965, foi constituído pelo Congresso o ***Special Subcommitte on Invasion of Privacy,*** no qual foram realizadas várias audiências, nas quais, foram abordas três questões específicas: *i)* a violação pelas agências federais da privacidade dos cidadãos (*Special Inquiry on Invasion of Privacy- 1965)*; *ii)* a constituição de uma base de dados centralizada, debaixo da alçada do Estado (*The Compute rand Invasion of Privacy – 1966)* ; *iii)* a proteção de dados pessoais de investidores no âmbito das agências de crédito (as *Commercial Credit Bureaus – 1968).*[9]

B) Primeiros diplomas

I. Em 1968, foi apresentado ao Congresso o projeto de lei *Fair Credit Reporting Bill,* cuja intenção era proteger os consumidores individuais, as pessoas coletivas e as demais

[8] O direito à autodeterminação informacional do titular dos dados e a sua proteção assumem um papel essencial no direito de proteção de dados, contudo, não é a sua única finalidade, ou o seu fundamento.

[9] Cordeiro, António Menezes. Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019, pág. 53-57, Almedina.

entidades que não se enquadram no conceito de consumidor. Vindo mais tarde a reconhecer o direito à informação e a estabelecer um regime de coimas e responsabilidade civil.[10]
A 31 de dezembro de 1974, foi aprovado o *Privacy Act*, que regulou a recolha, conservação, utilização e disseminação de informação pelas agências federais, apesar de ser um diploma com um campo de aplicação delimitado, previu um conjunto de princípios que vieram a incorporar o núcleo do Direito de Proteção de Dados.

II. O Direito da Proteção de Dados nos EUA assume uma grande complexidade devido à sua natureza federal e à inexistência de um diploma geral análogo ao Regulamento Geral de Proteção de Dados na Europa.

De entre os vários diplomas federais publicados desde 1978, estão hoje em vigor (com as devidas alterações introduzidas): *Family Educational Privacy Act, 1978; Right to Finantial Privacy Act, 1978; Privacy Protection, 1980; The Electronic Communications Privacy Act, 1986; Video Privacy Protection Act, 1988; Driver´s Privacy Prtoection Act, 1994; Children's Online Privacy Protection Act, 1998.*

Além destes diplomas setoriais, ocorreram grandes reformas legislativas que tiveram um impacto transversal na proteção, ou não, dos dados pessoais, nomeadamente: *Gram leach Bliley Act, 1999; Patriot Act, 2001 e Dodd Franck Act, 2010.*

III. Ora, a publicação do RGPD colocou os legisladores americanos sob pressão, no sentido de elaborarem um diploma transversal, que abarcasse pelo menos o sector privado. O Estado da Califórnia em 2018, deu o primeiro passo com a *California Consumer Privacy Act, 2018,* que entrou em vigor a 01.01.2020[11].

1.2.2. Europa

I. A primeira lei relativa à proteção de dados surgiu na ***Alemanha*** e foi aprovada em 1970 no Parlamento do Estado do Hesse: o *Hessisches Datenschutzgesetz* (HDSG), de 17 §, campo de aplicação material circunscrito à recolha e tratamento de dados por entidades públicas; ausência de previsão dos limites legais do processo de tratamento (lícito) dos

[10] Cordeiro, António Menezes. Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019, pág. 58, Almedina.

[11] Cordeiro, António Menezes. Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019, pág. 58, Almedina.

dados pessoais; atribuição de direitos secundários titulares de dados (de corrigir e restaurar os dados ilicitamente tratados); importância dedicada ao Supervisor de Dados Pessoais (autoridade com competência para supervisionar).

Em Janeiro de 1977, foi aprovado o *Bundesdatenschutzgesetz (BDSG)* – Lei Federal de Proteção de Dados- que consistia num diploma geral, aplicável a todos os tratamentos de dados, independentemente da natureza pública ou privada dos responsáveis pelo tratamento.

Na ***Suécia*** em 1973, surgiu o primeiro diploma de proteção de dados, o *Datalag*, com aplicação nacional e transversal, aplicável quer a entidades privadas, quer públicas.

Ora, a prática de legislar sobre a proteção de dados iniciada pela Suécia e Alemanha, mantém-se, passados várias décadas, como um elemento central da conceção europeia. [12]

II. A partir de 1980, iniciou-se um *período de consolidação* do Direito da Proteção de Dados e dos seus conceitos preponderantes, para o qual, contribuíram dois documentos: as *Guidelines Governing the Protection Privacy and Transborder Flows os Personal Data, da* OCDE, de 23 Setembro de 1980 e, a *Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal* (Convenção 108).

O Direito europeu da proteção de dados surgiu, sob a proteção e amparo do Conselho da Europa, com a Convenção de 108 que, desempenhou um papel decisivo e basilar nos princípios gerais e termos base utilizados no Direito da proteção de dados (conceito de dado pessoal, aplicação transversal a entidades públicas e privadas princípios da licitude, lealdade, limitação das finalidades, minimização dos dados). [13]

III. O Parlamento entre 1975 e 1982, salientou a necessidade de harmonizar os Direitos internos no âmbito do tratamento de dados pessoais, tendo diversas vezes recomendado que se iniciassem esforços nesse sentido. Contudo, a Comissão só em 29 de julho de 1981, passou a recomendar aos Estados- Membros que assinassem e ratificassem a Convenção 108.

A 29 de setembro de 1990, a Comissão avançou duas propostas de Diretrizes: *i) relativa à proteção das pessoas no que diz respeito ao tratamento dos dados pessoais; ii)*

[12]António Menezes Cordeiro, *Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019*, pág. 64-66, Almedina.
[13] Idem, 67.

relativa à proteção de dados pessoais e da vida privada no contexto das redes públicas digitais de telecomunicações, nomeadamente a rede digital de serviços integrados e as redes públicas móveis digitais. A Diretriz 95/46/CE, de 24 de outubro de 1995, foi aprovada após 5 anos após as a apresentação da proposta e extensas negociações[14]. Vindo a ser posteriormente revogada com a discussão legislativa do RGPD.

1.3. As Fontes do Direito de Proteção de Dados

1.3.1. Na Europa

As Fontes do Direito de Proteção de Dados podem ser organizadas em *i) Fontes Paraconstitucionais; ii) Fontes Legislativas;* e *iii) Fontes Infralegislativas.*

I. Fontes Paraconstitucionais – os fundamentos últimos do Direito de proteção de dados pessoais encontram-se positivados na *Carta dos Direitos Fundamentais da União Europeia*, especialmente, no seu artigo 8º - *(Proteção de dados pessoais) –" 1. Todas as pessoas têm direito à proteção de dados de carácter pessoal que lhes digam respeito; 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligados que lhe digam respeito e de obter respetiva retificação; 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente"*[15] –

Este preceito, reconhece a natureza fundamental e universal do direito de proteção de dados[16]; elenca os vários princípios previstos no RGPD (lealdade, licitude e limitação das finalidades); consagra o consentimento como fonte do tratamento lícito dos dados pessoais; identifica alguns direitos dos titulares dos dados pessoais (acesso e retificação); e, por fim, determina a constituição de uma autoridade independente para fiscalizar o cumprimento das regras.

---

[14] Cordeiro, António Menezes, *Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019*, pág. 68, Almedina.

[15] Carta dos Direitos Fundamentais da União Europeia- https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR

[16] Igualmente reconhecida pelo Tratado de Funcionamento da União Europeia, no seu artigo 16º, nº1.

A Carta dos Direitos Fundamentais da União Europeia, no seu artigo 7º prevê ainda que, *"Todas as pessoas têm o direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações"* – o que demonstra a proximidade existente entre o direito à intimidade da vida privada e o direito de proteção e dados.

O *Tribunal Judicial da União Europeia (TJUE),* também releva a proximidade existente entre os direitos referidos anteriormente[17], nomeadamente, no Acórdão *Digital Rights Ireland,* em que sublinha: "*o importante papel desempenhado pela proteção de dados pessoais na perspetiva de direito fundamental ao respeito da vida privada".* e num outro[18], "*A este respeito, cabe recordar que a proteção dos dados pessoais, que resulta da obrigação expressa e prevista no artigo 8º, nº 1 da Carta, assume particular importância para o direito ao respeito da vida privada consagrado no artigo 7º desta."*

A conexão entre o direito da proteção de dados e o direito à intimidade da vida privada tem sido utilizada, não raras vezes, pelo *Tribunal Europeu dos Direitos Humanos (TEDH)* por forma a proteger a esfera jurídica dos titulares dos dados, sendo para tal, invocado o artigo 8º, nº 1 da *Convenção Europeia dos Direitos do Homem (CEDH),* que prevê "*Qualquer pessoa tem o direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência".*

II. Fontes Legislativas **-** O Direito da União Europeia está, hoje, munido de vários diplomas legais afetos ao Direito da proteção de dados, nomeadamente: *i)* o Regulamento (UE), 2018/1807, de 14 de novembro *ii)* Regulamento (UE) 2018/1725, de 23 de novembro; *iii)* Regulamento da (UE), nº 611/2013, de 24 de junho*; iv*) Diretriz (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril; *v)* Diretriz nº2000/31/CE de 8 de junho*; vi)* Diretriz nº2002/58/CE, de 12 de julho.

III. Fontes Infralegislativas **-** O Comité Europeu para Proteção de Dados, organismo independente e dotado de personalidade jurídica, além de supervisionar e promover a aplicação coerente do RGPD, nos termos do artigo 63º do RGPD, também emite recomendações, diretrizes e melhores práticas nos termos do artigo 70º do RGPD. Análogo

[17] *"Este direito fundamental está indissociavelmente relacionado com o direito ao respeito pela vida privada consagrado no artigo 7º, desta mesma Carta"* – TJUE 9- nov-2010, proc. nº C-92/09 E C-93/09, 47.

[18] TJUE 8-abr.-2014, proc. nº C-293/12 e C-594/14, 48.

também o que acontece com a CNPD (Comissão Nacional de Proteção de Dados) que, emite diretrizes, recomendações e melhores práticas.

1.3.2. Em Portugal

O Direito da Proteção de Dados em Portugal está consagrado, *i)* na Constituição*; ii)* Legislação Ordinária; *iii)* Fontes Infralegislativas e *Soft- law*.

i) A Constituição

A Constituição da República Portuguesa (CRP) foi a primeira Lei Fundamental a reconhecer, diretamente, alguma proteção constitucional aos titulares dos dados pessoais[19]. O artigo 35º da versão originária da CRP já contemplava o Direito da Proteção dos Dados – *"1. Todos os cidadãos têm o direito de tomar conhecimento do que constar em serviços mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização; 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos; 3. É proibida a atribuição de um número nacional único aos cidadãos."*

O artigo 35º da CRP, veio a ser atualizado ao longo dos anos por consequência das revisões e alterações efetuadas em 1982, 1989, 1997 que, por um lado promoveram um alargamento progressivo da proteção concedida aos titulares dos dados pessoais e estabeleceram bases fundamentais do Direito da Proteção de Dados, densificadas no RGPD, na LE e na demais legislação extravagante.[20]

ii) Legislação Ordinária

A história mais recente do Direito da Proteção de Dados surgiu com a Lei nº 2/73 de 10 de Fevereiro e com o Decreto-Lei nº 555/73 de 26 de Outubro (que veio a instituir o número nacional de identificação originou a inclusão no artigo 35º na versão original da CRP).

[19] Cordeiro, António Menezes, *Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019,* pág. 73, Almedina.
[20]Cordeiro, António Menezes, *Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019,* pág. 76, Almedina.

No início dos anos 90 do seculo XX, foi aprovada a *Lei da proteção de dados pessoais face à informação* (Lei nº 10/91, de 29 de abril), seguida da *Lei de Proteção de Dados Pessoais* (Lei 67/98, de 26 de outubro), que transpôs a Diretiva nº95/46/CE.

Atualmente, no século XXI, além da Lei de Execução do RGPD, com aplicação maioritariamente transversal, importa também destacar: i) Lei nº 59/2019, de 8 de agosto; Lei nº 41/2004, de 18 de agosto; Lei nº 12/2005, de 26 de janeiro; Lei nº 26/20n16, de 22 de agosto; Leis de Videovigilância: Le nº 1/2005, de 10 de janeiro. [21]

iii) Fontes infralegislativas e soft-law

O RGPD e a LE não contêm, nem sequer preceitos gerais, que atribuam à CNPD competências para elaborar regulamentos ou diplomas legais. Apenas preveem outras formas de intervenção paralegislativa; os pareceres, as orientações e as recomendações genéricas. No entanto, tais pareceres, orientações e recomendações genéricas não têm conteúdo normativo próprio, ou seja, do seu incumprimento não resulta um comportamento juridicamente reprovável, não obstante poder configurar uma efetiva violação do Direito vigente. [22]

[21] Cordeiro, António Menezes, *Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019*, pág. 76-79, Almedina.
[22] Idem, 80.

CAPÍTULO II- O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

2.1. Objetivo

O Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679) consiste numa medida essencial para reforçar os direitos fundamentais das pessoas na Era Digital em que vivemos, e facilitar a atividade comercial mediante o esclarecimento das normas aplicáveis às empresas e aos organismos públicos no mercado único digital. [23]

O objetivo deste diploma resume-se, essencialmente, a um reforço coerente e elevado dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos dados pessoais.

Ademais, a adoção deste ato legislativo único, assegura igualmente a homogeneização sua da aplicação, de forma a evitar a fragmentação da proteção de dados ao nível da União e, consequentemente, a insegurança jurídica. [24]

2.2. Conceitos Básicos

2.2.1. Dados Pessoais

Dados pessoais consistem, de acordo com o previsto no artigo 4º, nº1 do RGPD, na "*informação relativa a uma pessoa singular identificada ou identificável (titular de dados)".*

2.2.2. Titular dos dados

Titular dos dados, "*a pessoa singular que pode ser identificada, direta ou indiretamente*, em especial por referência a um identificador, nomeadamente, um nome, um número de identificação, dados ou localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética (…) etc." – artigo 4º, nº1, 2ª parte do RGPD.

---

[23] A proteção de Dados na UE in https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt

[24] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt

2.2.3. Responsável pelo tratamento

Responsável pelo tratamento, "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais" - artigo 4º, nº 7 do RGPD.

2.2.4. Consentimento

*Consentimento do titular dos dados, é a "*manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais lhe dizem respeito sejam objeto de tratamento" – artigo 4º, nº 11 do RGPD. O consentimento é assim, a principal causa de legitimidade e de licitude do tratamento de dados pessoais – artigo 6º, nº 1, alínea a) do RGPD.

2.2.5. Tratamento

Tratamento, uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados e não automatizados, tais como recolha, registo, organização, estruturação, conservação, adaptação ou alteração, (…) etc – artigo 4º, nº 2 do RGPD.

2.2.6. Subcontratante

Subcontratante, é uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes – artigo 4º, nº8 RGPD.

2.2.7. Violação de dados pessoais

Violação de dados pessoais, é uma violação de segurança que provoque, de modo incidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento – artigo 4º, nº 12 do RGPD.

2.2.8. Dados biométricos

Dados biométricos, dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos – artigo 4º, nº 14 do RGPD.

2.2.9. Dados relativos à saúde

Dados relativos à saúde, dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde – art. 4º, nº 15 do RGPD.

2.3. Princípios

O artigo 5º do Regulamento UE nº 2016/679 (RGPD), prevê os princípios relativos ao tratamento dos dados pessoais, nomeadamente:

a) Princípio da licitude, lealdade e transparência – "objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados" – alínea a) do nº1. [25]

b) Princípio da limitação das finalidades – "recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89º, nº1" – alínea b) do nº1. [26]

[25] A *licitude* do tratamento, de acordo com o n.º 2 do artigo 8º da Carta "… com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto na lei". A *lealdade* no tratamento, é muitas vezes enunciada/ densificada no RGPD com a expressão "tratamento equitativo". A *transparência* engloba tanto o conteúdo das informações a ser transmitidas aos titulares ou a terceiros, como os procedimentos da transmissão.

[26] As *finalidades* devem ser estabelecidas previamente ao tratamento dos dados, não podendo ficar em aberto, adiadas ou condicionadas a qualquer evento futuro. A determinação das finalidades do tratamento, pressupõem que, o responsável pelo tratamento realize um exame prévio, que lhe possibilite identificar e fundamentar os propósitos do tratamento.

c) *Princípio da minimização dos dados* – Os dados pessoais são "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados" - alínea c) do nº1[27].

d) *Princípio da exatidão* – Os dados pessoais são "exatos e atualizados sempre que necessário. Devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora" – alínea d) do nº1.

e) *Princípio da Limitação da conservação* – Os dados pessoais são " conservados de uma forma que permita a identificação dos titulares dos dados durante o período necessário para as finalidade para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89º/1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados" – alínea e) do nº1.

f) *Princípio da integridade e confidencialidade* – *"Os* dados pessoais são tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas" – alínea f do nº1.

g) *Princípio da Responsabilidade* – "O responsável pelo tratamento é o responsável pelo cumprimento do disposto nos princípios anteriores e tem poder comprová-lo". Este princípio consagrado nº2 do art. 5º, em conjugação com o art. 24*º* do RGPD exige, ainda, do Responsável pelo Tratamento de Dados a aplicação de medidas adequadas e eficazes e políticas de proteção de dados com base num critério de risco e de adaptabilidade e proporcionalidade das medidas que garantam o respeito pelos

[27] O princípio da *minimização de dados* é composto por três pilares: a adequação – limitação do tratamento dos dados pessoais às finalidades prosseguidas; a pertinência – limitação das atividades dos responsáveis a tratamentos que contribuam para a prossecução das finalidades; necessidade – inexistência de um método alternativo menos invasivo.

princípios e obrigações do RGPD e, quando solicitado, a sua demonstração às autoridades de controlo.[28]

2.4. Âmbito de aplicação

2.4.1. Material

O RGPD aplica-se ao tratamento de dados pessoais por meios automatizados ou parcialmente automatizados e a tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.[29], mas não se aplica ao tratamento de dados pessoais: *i)* efetuado no exercício de atividades não sujeitas à aplicação do direito da União; *ii)* efetuado pelos Estados-membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; *iii)* Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; *iv)* Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

2.4.1.1. Atividades exclusivamente pessoais ou domésticas

A aplicabilidade do RGPD é limitada quando estejam em causa o tratamento de dados pessoais por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas, mas apesar de, o RGPD prever a expressão "uma pessoa singular", não obsta a que se conclua que a aplicação do RGPD também é limitada a tratamentos realizados por mais do que uma pessoa[30], pois, o seu fundamento são os objetivos subjacentes ao tratamento e não a quantidade de pessoas envolvidas[31]. Contudo, não são abrangidas nesta exceção as pessoas coletivas, inclusivamente, as sem fins lucrativos (associações e fundações).

[28] "Princípios do tratamento de dados" in www.uc.pt/protecao-de-dados/conceitos_basicos/principios_do_tratamento_de_dados

[29] Artigo 2º RGPD

[30] A mesma expressão é utilizada nas versões espanhola, italiana e francesa. A versão inglesa utiliza o pronome indeterminado e a versão alemã o plural.

[31] No Considerando 18 do RGPD é utilizado o plural: "O presente regulamento não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares".

No entendimento do TJUE as atividades pessoais e domésticas devem ser interpretadas como as *"que se inserem no quadro da vida privada ou familiar"*[32], contudo, esta exceção será inadmissível quando se trate de uma divulgação pública de dados, ou seja, para um número indeterminado de pessoas, nomeadamente na *Internet*[33].

Ora, mesmo que, em abstrato, se entenda que ao tratamento para fins exclusivamente pessoais e domésticos não se aplica o RGPD, é de considerar que, em concreto, o tratamento desenvolvido poderá não estar abrangido por esta exceção.

2.4.2. Territorial

O artigo 3º do RGPD constitui um progresso importante da legislação da UE em matéria de proteção de dados em comparação com o quadro definido pela Diretiva 95/46/CE[34], pois, transpõe a intenção do legislador de garantir uma proteção abrangente dos direitos dos titulares de dados da UE e de criar condições equitativas para empresas ativas nos mercados da UE, num contexto de fluxos de dados a nível mundial e, define o âmbito de aplicação territorial do regulamento com base em dois critérios principais: o *critério do "estabelecimento*", nos termos do artigo 3º, nº1; e o *critério do "direcionamento*", nos termos do artigo 3º, nº2.

I) Critério do estabelecimento

Segundo o artigo 3º, nº1, do RGPD, *"o regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União".*

[32] TJUE 16-DEZ.-2008, proc. C-73/07 (*Satamedia): "*esta segunda excepção deve ser interpretada no sentido de que tem apenas por objeto as atividades que se inserem no quadro da vida privada ou familiar dos particulares".

[33] TJUE 6-nov.-2003, proc. C-101/01 (*Lindqvist)*: "Esta exceção deve, portanto, ser interpretada como tendo unicamente por objeto atividades que se inserem no âmbito da vida privada ou familiar dos particulares, o que não é manifestamente o caso do tratamento de dados de carácter pessoal que consiste na sua publicação na *Internet de maneira a que esses dados são disponibilizados a um número indeterminado de pessoas".*

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

Ora, o tratamento de dados efetuado por um subcontratante também poderá estar sujeito ao direito da UE em virtude de o subcontratante possuir um estabelecimento situado na UE. Atendendo que, de acordo com o art. 3º, nº1 do RGPD, "*independentemente do local efetivo em que ocorre o seu tratamento",* aplica-se ao tratamento efetuado por um responsável ou subcontratante o Direito da União, é necessário, e aliás, recomendado pelo CEPD, uma abordagem tripla para se determinar se o tratamento de dados pessoais é ou não abrangido pelo âmbito de aplicação do RGPD nos termos do art. 3º, nº1. [35] *Primeira*, atentando na definição de um "estabelecimento" na união europeia; *Segunda*, analisando aquilo que se entende por "tratamento no contexto das atividades de um estabelecimento na união"; *Terceira*, e última, confirmando que o RGPD se aplicará independentemente de o tratamento efetuado no contexto das atividades desse estabelecimento ter ocorrido na União ou não.

I) " *Um estabelecimento na União"*

Determinar se uma entidade é um responsável pelo tratamento de dados ou um subcontratante para efeitos de legislação da UE em matéria de proteção de dados constitui um elemento central da avaliação da aplicação do RGPD ao tratamento de dados pessoais em questão[36].

O "*estabelecimento principal"* é definido no artigo 4º, nº16, o RGPD, contudo, esta definição deve ser completada com o considerando 22, *"estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto".*

Ora, para se determinar se uma entidade estabelecida da instalação como o exercício efetivo de atividades nesse Estado- Membro das atividades económicas deve adotar-se "*uma conceção flexível do conceito de estabelecimento, que afasta qualquer abordagem formalista segundo a qual uma empresa só se pode considerar estabelecida no lugar em que*

[35] Diretrizes 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3º) de 12 de Novembro de 2019, página 5. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf

[36] GT 29, WP169 — Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante», adotado em 16 de fevereiro de 2010 e em revisão pelo CEPD.

estiver registada", ou seja, o exercício efetivo de atividades nesse Estado-Membro devem ser analisados à luz da natureza específica das atividades económicas e da prestação de serviços em questão, inclusive, as empresas que oferecem serviços exclusivamente em linha[37].

Em certos casos, será também necessário atender a determinadas circunstâncias, pois, o limiar relativo a uma instalação estável é, por vezes, bastante reduzido, principalmente nos casos em que o centro de atividades de um responsável pelo tratamento procede à prestação de serviços em linha. Assim é, quando está presente na União um único funcionário agente de uma entidade extracomunitária, e se considera bastante para a constituição de uma instalação estável, ou seja, equivalente a um estabelecimento para efeitos do artigo 3º, nº1 (desde que esse funcionário ou agente atue com um grau de estabilidade suficiente). Em contrapartida, quando um funcionário se encontra na UE, mas o tratamento diz respeito a atividades do responsável pelo tratamento fora da UE, a sua simples presença na UE não leva a que tal tratamento seja abrangido pelo âmbito de aplicação do RGPD, pois, a simples presença de um funcionário na UE não é, por si só, suficiente para desencadear aplicação do RGPD, dado que, para que seja abrangido pelo âmbito de aplicação do RGPD, o tratamento em questão também tem de ser efetuado no contexto das atividades do funcionário baseado na UE.

Assim, é possível concluir que, o facto de uma entidade extracomunitária responsável pelo tratamento de dados não ter uma sucursal ou filial num Estado Membro, não invalida que nele não possa ter um estabelecimento na aceção da legislação da UE em matéria de proteção de dados. Contudo, não se pode concluir que a entidade extracomunitária tem um estabelecimento na União simplesmente por ser possível aceder ao sítio *Web* da empresa na União.

II) *Tratamento de dados pessoais efetuado "no contexto das atividades de" um estabelecimento*

O próprio artigo 3º, nº1 refere que não é necessário que o tratamento em questão seja efetuado "pelo" próprio estabelecimento na EU, pois, o responsável pelo tratamento ou

[37] Acórdão de 1.10.2015 – Processo C-230/14, WELTIMNO, considerando 29 - https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62014CJ0230&from=PT

subcontratante ficará sujeito às obrigações nos termos do RGPD sempre que o tratamento seja efetuado "no contexto das atividades" do seu estabelecimento na União.

O próprio CEPD defende que, para efeitos do artigo 3º, nº1, o significado de "tratamento no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou subcontratante" deve ser entendido à luz da jurisprudência, nem de uma forma demasiado restrita, nem demasiado ampla, levando à conclusão de que qualquer presença na UE é suficiente para fazer com que tal tratamento seja abrangido pelo âmbito de aplicação de legislação da UE em matéria de proteção de dados.

III) *Aplicação do RGPD ao estabelecimento de um responsável pelo tratamento ou de um subcontratante na União, independentemente de o tratamento ocorrer na União ou não.*

Nos termos do disposto no artigo 3º, nº1 aplica-se o RGPD ao tratamento de dados pessoais no contexto de atividades de um estabelecimento responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União, ou seja, o local onde ocorre o tratamento não é pertinente para determinar se o tratamento efetuado no contexto das atividades de um estabelecimento situado na UE é abrangido pelo âmbito de aplicação do RGPD.

*"**Exemplo**: Uma empresa francesa desenvolveu uma aplicação de partilha de automóveis exclusivamente destinada a clientes de Marrocos, da Argélia e da Tunísia. O serviço apenas está disponível nesses três países, mas todas as atividades de tratamento de dados pessoais são efetuadas em França pelo responsável pelo tratamento de dados. Embora a recolha de dados pessoais ocorra em países terceiros, neste caso o posterior tratamento de dados pessoais é efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento de dados situado na União. Por conseguinte, embora o tratamento diga respeito a dados pessoais de titulares dos dados que não estão situados na União, as disposições do RGPD aplicar-se-ão ao tratamento efetuado pela empresa francesa, em conformidade com o artigo 3.º, n.º 1.*"

***Exemplo**: Uma empresa farmacêutica com sede em Estocolmo decidiu efetuar na sua sucursal, situada em Singapura, todas as suas atividades de tratamento de dados pessoais no atinente aos seus dados de ensaios clínicos. Neste caso, embora as atividades de tratamento ocorram em Singapura, esse tratamento é efetuado no contexto das atividades da empresa farmacêutica situada em Estocolmo, ou seja, por um responsável pelo tratamento de dados estabelecido na União. Assim sendo, as disposições do RGPD aplicam-se a esse tratamento, nos termos do artigo 3.º, n.º 1."*[38]

Ou seja, não deve limitar-se a aplicação do RGPD ao tratamento de dados de pessoas situadas no território da União, mas sim, a todo e qualquer tratamento de dados efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou subcontratante situada na União, independentemente de a localização ou nacionalidade do titular de dados cujos dados pessoais são objeto de tratamento. Esta conclusão, é sustentada pelo considerando 14 do RGPD – *"A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais"*.

IV) *Aplicação do critério relativo ao estabelecimento ao responsável pelo tratamento e ao subcontratante*

As atividades de tratamento abrangidas pelo art. 3º, nº1, são consideradas pelo CEPD como disposições que se aplicam a responsáveis pelo tratamento e subcontratantes[39] cujas atividades de tratamento sejam realizadas no contexto de atividades do seu respetivo estabelecimento situado na UE.

[38] GT 29, WP169 — Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante», adotado em 16 de fevereiro de 2010 e em revisão pelo CEPD, pág. 10

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

O RGPD prevê a aplicação de disposições e de obrigações diferentes e específicas aos responsáveis pelo tratamento e aos subcontratantes, pelo que, no caso de um responsável pelo tratamento ou subcontratante estar sujeito ao RGPD nos termos do artigo 3.º, n.º 1, as obrigações conexas aplicam-se-lhes respetiva e separadamente.

Contudo, o CEPD entende que, um subcontratante situado na UE não deve ser considerado um estabelecimento de um responsável pelo tratamento de dados na aceção do artigo 3.º, n.º 1, simplesmente por força da sua condição de subcontratante em nome de um responsável pelo tratamento, pois, a existência de uma relação entre um responsável pelo tratamento e um subcontratante não resulta necessariamente na aplicação do RGPD a ambos, caso uma dessas entidades não esteja estabelecida na União, mas, sempre que um subcontratante estiver estabelecido na União, ser-lhe-á exigido que cumpra as obrigações que o RGPD impõe aos subcontratantes e, caso o responsável pelo tratamento que dá instruções ao subcontratante também estiver situado na União, também terá de cumprir as obrigações que o RGPD impõe a responsáveis pelo tratamento.

2.5. Os Direitos dos Titulares dos Dados

O RGPD não apresenta uma definição concreta de dados pessoais, referindo apenas indiretamente no artigo 4º, 1) - *"'Dados pessoais', informação relativa a uma pessoa singular identificada ou identificável (titular de dados)".* Contudo, não se poderá negar que, uma pessoa coletiva ou pessoa não identificável não possa ser titular de dados.

Não desconsiderando o supra exposto, a verdade é que, para que um determinado sujeito se possa afirmar como titular de dados (pessoa singular) é necessário, que e este lhe seja aplicado o artigo 3º. Ou seja, de acordo o RGPD será titular de dados, todo aquele, independentemente da sua nacionalidade ou residência, cujos dados sejam objeto de tratamento efetuado no âmbito de atividades desenvolvidas pelo estabelecimento de um responsável pelo tratamento efetuado no âmbito de atividades desenvolvidas por um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado em território da União – artigo 3º/1; e todos os residentes no espaço da União cujos dados pessoais sejam objeto de tratamento nos termos do artigo 3º/2.

Ora, os titulares dos dados pessoas estão previstos no Capítulo III do RGPD – "Direitos do titular dos dados".

Os principais direitos dos titulares de dados são os seguintes: 1) o direito de acesso; 2) o direito de retificação; 3) o direito de apagamento; 4) o direito de limitação do tratamento; 5) o direito de portabilidade; 6) o direito de oposição.

2.5.1. Direito de Acesso

O Direito de Acesso está expressamente consagrado no artigo 15º do RGPD e ramifica-se em *i)* o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento; *ii)* o direito de acesso (*stricto sensu)* aos dados pessoais e informações elencadas nas alíneas a) a h) do artigo 15[40].

A relevância do direito ao acesso manifesta-se na proteção constitucional conferida pelo artigo 8º da Carta: *"todas as pessoas têm o direito de aceder aos dados coligidos que lhe digam respeito" e* no que toca ao pedido de retificação e apagamento; o direito ao esquecimento; ou direito de portabilidade.

2.5.1. Pedido de informação

O direito de acesso circunscreve-se ao pedido efetuado pelo titular de dados ao responsável pelo tratamento, relativamente aos seus dados pessoais presentes e passados, e não a dados pessoais de terceiros.

O Considerando 63 do RGPD[41], prevê, no entanto, que o responsável pelo tratamento de dados pode, quando lhe seja requerida uma elevada quantidade de informação relativa ao titular de dados, solicitar um pedido de esclarecimento em relação aos dados ou tratamento a que o titular de dados se refere. Ou seja, recebido o pedido de informação, deve o responsável do tratamento esclarecer dúvidas que possam existir relativamente ao titular dos dados pessoais, por forma a confirmar a sua identidade – artigo 12º/6 RGPD "*quando o responsável pelo tratamento tiver dúvidas razoáveis quanto à identidade da pessoa singular que apresenta o pedido a que se refere os artigos 15º a 21º, pode solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade dos titular dos dados".*

[40] Cordeiro, António Menezes, *Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019,* pág. 262, Almedina.

[41] Não se poderá esquecer que, os considerandos não têm força de lei, tendo apenas como propósito clarificar o sentido e alcance de uma determinada norma/ ou suas fundamentações.

Neste contexto, o titular de dados poderá aceder às seguintes informações*: i)* as finalidades do tratamento; *ii)* as categorias de dados pessoais em questão; *iii)* os destinatários ou categorias de dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; *iv)* o prazo previsto para conservação de dados pessoais, ou, se não for possível, os critérios utilizados para fixar esse prazo; *v)* aos direitos do titular; *vi)* às origens dos dados, no caso de estes não terem sido recolhidos diretamente junto dos titulares. [42]

I) *As finalidades – o princípio da transparência* – o titular dos dados pessoais tem o direito de saber quais os fundamentos jurídicos que sustentam o tratamento dos seus dados pessoais.

II) *Categorias de dados pessoais em questão –* se, em concreto estão em causa, ou não dados pessoais sensíveis – artigos 13º/1, d) e 14º/1, d) RGPD.

III) *Destinatários ou categorias de destinatários-* o responsável pelo tratamento deve informar o titular de dados dos destinatários passados, presentes e também futuros desde que à data sejam determinados ou determináveis.

IV) *Prazo e critérios de conservação* – o responsável de tratamento deve informar o titular de dados do prazo concreto previsto para a conservação dos dados, contudo, se não for possível deverá informar os critérios utilizados para o fixar.

V) *Direitos dos titulares* – o titular de dados poderá requerer do responsável, informações relativas ao direito de retificação, de apagamento, de limitação de tratamento de dados pessoais, de oposição a esse tratamento, de reclamar junto de uma autoridade pública.

VI) *Origem dos dados* – sempre que os dados pessoais não tenham sido fornecidos pelo seu titular tem este o direito de ser informado sobre a sua origem.

2.5.2. Direito de retificação

O direito de retificação encontra um forte suporte constitucional – art. 35º/1 CRP, como no Direito Europeu- art. 8º/2 Carta e está expressamente consagrado no artigo 16º do RGPD – "*o titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em*

[42] Cordeiro, António Menezes, *Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019,* pág. 267 -268, Almedina.

conta todas as finalidades do tratamento, o titular dos dados tem o direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional".

Ora, o direito de retificação subdivide-se em dois direitos: *i)* o direito a exigir a retificação dos *dados inexatos* - dados pessoais que, em confronto com a informação detida e a informação real resulte uma qualquer desconformidade. Sendo que, esses dados inexatos apenas se circunscrevem aos dados pessoais objetivos, não a dados pessoais subjetivos (opiniões); *ii)* o direito de exigir que os *dados incompletos* - aqueles que, não sejam suficientes para atingir a concreta finalidade do tratamento - sejam completados. Contudo, se a incompletude se demonstrar irrelevante para a prossecução da finalidade em questão, não terá o responsável pelo tratamento, a obrigação de corrigir tais dados. Aliás, há que perspetivar o direito a completar determinados dados pessoais com cautela, pois, quanto mais informação o titular dos dados transmitir, maior é o risco que este poderá estar sujeito.

2.5.3. Direito ao apagamento/ esquecimento

O RGPD nos seus considerandos 65 e 66[43], prevê dois tipos de direitos: o direito a ser esquecido *sui generis* e o direito ao apagamento *stricto sensu* que, conjuntamente corporizam o direito ao apagamento *lato sensu.* [44]

O direito ao apagamento está intimamente ligado ao princípio da minimização dos dados pois, de acordo com o artigo 5º/1/ c) do RGPD, os dados pessoais são "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados". Ora, o tratamento dos dados deverá ser *adequado* – limitado às finalidades que se visam prosseguir; *pertinente* – habilitado a contribuir para a prossecução dessas finalidades;

[43] "Os titulares dos dados deverão ter direito a que os dados que lhe digam respeito sejam retificados e o "direito a serem esquecidos" quando a conservação desses dados violar o presente regulamento ou o direito da União ou dos Estados- Membros aplicável ao responsável pelo tratamento. Em especial, os titulares de dados deverão ter direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento se deixarem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento de dados pessoais que lhes digam respeito ou se o tratamento dos seus dados pessoais não respeitar o disposto no presente regulamento. – Regulamento Geral de Proteção de Dados, considerando 65.

[44] Cordeiro, António Menezes. Direito de Proteção de Dados à luz do RGPD e da Lei nº 58º/2019, pág. 274, Almedina.

limitados - ou seja, o tratamento será apenas aceitável se não existir um método alternativo menos invasivo[45]

O direito ao apagamento *stricto sensu* confere o direito ao titular dos dados de exigir o apagamento dos seus dados pessoais ao responsável pelo tratamento, desde que verificados os requisitos previstos nas alíneas do artigo 17º/1. Enquanto, o direito ao esquecimento concretizado no artigo 17º/2, consiste no direito de exigir exclusivamente do responsável pelo tratamento, e não do público em geral, a comunicação aos demais responsáveis pelo tratamento (individualmente)[46] do pedido de apagamento de ligações, eventuais cópias e reproduções de determinados dados pessoais.

António Menezes Cordeiro (in Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019, pág. 275*)* afirma: "*o direito ao esquecimento surge como um reconhecimento da insuficiência do apagamento dos dados pelo responsável pelo tratamento originário, em face das especificidades da Internet. Como é notório, o simples facto de se apagar uma determinada informação de um sítio não significa que ele tenha sido apagado de toda a Internet."*

Importa ainda referir que, este direito ganhou mais visibilidade com o acórdão *Google Spain* que, decidiu que o motor de busca de internet é também responsável pelo processamento de dados pessoais publicados por terceiros nas suas páginas de *web*, limitando a liberdade de expressão e acesso à informação, em nome do direito de reserva da vida privada. Ou seja, decidiu que o operador do motor de busca está obrigado a eliminar da lista de resultados[47], exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a outras páginas *web* publicadas por terceiros e que contenham informações sobre essa pessoa, incluindo na hipótese de esse nome ou de essas informações

[45] Por exemplo, a anonimização prevista no artigo 32º/1 do RGPD; e a pseudonomização – artigo 25º/1 do RGPD.

[46] "*A comunicação desta intenção não parece sequer fazer emergir na esfera jurídica desses outros responsáveis pelo tratamento uma obrigação (passiva) de apagamento: cabe ao titular dos dados requerê-lo individualmente"* - cit. Barreto Menezes Cordeiro, António, Direito da Proteção de Dados, pág. 275, Almedina

[47] O WP 29 entende que, o motor de busca não tem de fazer um juízo permanente sobre os resultados inscritos, mas apenas remover os resultados cujo apagamento seja pedido pelos interessados

não serem prévia ou simultaneamente apagadas dessas páginas *web* e mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita.[48]

Como explica o WP 29[49], quando uma pesquisa é realizada pelo nome do sujeito, passa a haver uma visão estruturada da informação que pode ser encontrada na internet e que, sem essa indexação no motor de busca, não seria relacionada com o mesmo ou apenas seria com grande dificuldade. Ora, mesmo quando a informação é lícita, a difusão universal e a acessibilidade da informação listada pelo motor de busca pode ser ilícita tendo em conta o impacto desproporcional na privacidade.

2.5.3.1. Âmbito do direito a ser esquecido e fundamentos de recusa do apagamento

O direito a ser esquecido pode abranger, potencialmente, três diferentes categorias de situações[50]. A *primeira, o* direito ao apagamento dos dados colocados online pelo próprio utilizador, uma categoria menos problemática no que toca à exibição pública dos dados, mas mais problemática quanto ao apagamento dos arquivos e a confirmação pelo utilizador de que os conteúdos foram efetivamente apagados. A *segunda,* as situações em que o sujeito publicou um conteúdo online e, posteriormente, um terceiro copia esse conteúdo e publica na sua página. A *terceira*, os casos em que a própria publicação é realizada por um terceiro acerca do sujeito e o último pretende o seu apagamento.

Não obstante, não se pode deixar de atender às exceções consagradas no artigo 3º e nº 3 do artigo 17º do RGPD que elencam o conjunto de fatores que permitem não aceder ao pedido de apagamento dos dados, nomeadamente o tratamento ser necessário ao exercício da liberdade de expressão e de informação; ao cumprimento de uma obrigação legal; por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9º, nº 2, alíneas h) e i), bem como no artigo 9º, nº3; para fins de arquivo de interesse público, para

---

[48] de Oliveira, Ana Perestrelo in "Fintech II- Novos Estudos sobre Tecnologia Financeira", *Direito ao apagamento dos dados ou direito a ser esquecido, pág. 90.*

[49] Após a decisão do TJUE no caso Costeja, foram realizadas e disponibilizadas pelo *Article 29 Protection Working Party,* as *Guidelines on the implementation of the Court of Justice of the European Uniom Judgment "Google Spain and Inc v. Agencia Española de protección de datos (AEPD) and Mario Costeja González", de 26 de novembro de 2014,* visando auxiliar as autoridades de controlo na gestão das reclamações que sejam feitas de recusas de desindexação de resultados.

[50]Fleischer, Peter, F*oggy thinking about the Right to Oblivion,,* http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html

fins de investigação científica, ou histórica ou para fins estatísticos, nos termos do artigo 89º, nº 1, na medida em que o direito referido no nº 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção de benefícios desse tratamento; ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Quanto à exceção "exercício da liberdade de expressão", as *Guidelines* do WP 29 atentam para a necessidade de consideração da liberdade de expressão na decisão da remoção dos resultados. Mas quais são os critérios que podem ou devem ser usados na análise do pedido de desindexação ou na avaliação, pelas autoridades competentes, da decisão do motor de busca?

- O resultado de pesquisa reporta-se a uma pessoa natural e o resultado aparece na lista de resultados quando pesquisada pelo nome da pessoa?

- A pessoa em causa desempenha um papel de vida pública ou é uma figura pública (pessoa que, pelas suas funções, tem um grau de exposição mediática)?

- A pessoa é menor?

- A informação é exata?

- A informação é relevante e não é excessiva?

- A informação é sensível (sexualidade, saúde, religião)?

- As informações reportam-se a crimes?

- A informação causa danos desproporcionais?

2.5.3.2. Comunicação a Terceiros

De acordo com o disposto no artigo 17º/ 2 do RGPD "*quando o responsável pelo tratamento tiver tornado públicos os dados e for obrigado a apagá-los nos termos do nº 1, toma medidas que forem razoáveis, incluído de carácter técnico, tendo em consideração a*

tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais, bem como das cópias ou reprodução dos mesmos". Não obstante, essa obrigação cessar se for impossível ou exigir um esforço desproporcionado.

2.5.3.3. Um direito novo ou uma nova valoração de interesses?

No que toca ao direito ao apagamento de dados ou o direito a ser esquecido não está em causa um novo direito, mas há certamente uma nova valoração dos interesses conflituantes e, uma nova e inequívoca prevalência do direito sobre a reserva da intimidade da vida privada.

Ana Perestrelo de Oliveira in "Fintech II. Novos Estudos sobre Tecnologia Financeira", *Direito ao apagamento dos dados ou direito a ser esquecido*, pág. 101 - *"(...) o "direito a ser esquecido" é mais do que uma expansão modesta dos direitos de privacidade preexistentes (...). Não é como se tem apontado, um direito a reescrever a história, mas – se devidamente aplicado- permite ao sujeito manter o controlo sobre os dados disponibilizados pelo menos no contexto de pesquisa específica que o verse. É um importante avanço. A inflexão esta no facto de não se exigir qualquer dano ou qualquer outra circunstância fundamentadora do apagamento: o simples facto de o sujeito não pretender que os dados estejam disponíveis no motor de busca pelo seu nome, mesmo que não lhe cause qualquer dano, é suficiente para pedir a remoção".*

Pelo exposto, será possível concluir que, o direito ao apagamento ou direito a ser esquecido é um notável avanço na tutela do direito à privacidade na era da internet.

2.5.4. Direito à limitação do tratamento

O titular de dados tem o direito de exigir a limitação do tratamento nas seguintes situações, de acordo com o disposto no artigo 18º, nº 1 do RGPD: *i)* a par da apresentação de um pedido de retificação, a limitação do tratamento dos dados cuja exatidão conteste, durante a pendência de um processo de verificação dessa mesma observância; *ii)* se o tratamento for ilícito; *iii)* se os tratados deixarem de ser necessários para a finalidade que

motivou o tratamento[51]; iv) na pendência de um pedido de oposição intentado ao abrigo do artigo 21º.

2.5.6. Direito de portabilidade

O direito de portabilidade consiste no direito que cada titular de dados possui para controlar os seus dados pessoais– *âmbito individual-*, mas também, num verdadeiro impulso à livre concorrência e a iniciativa económica – *âmbito social.* [52]

Este direito subdivide-se em dois direitos, o direito de receber os seus dados pessoais e o direito a transmitir esses dados para outro responsável.[53] Contudo, para tal é necessária a verificação cumulativa de dois elementos: *i)* o tratamento fundar-se no consentimento do titular*; ii)* o tratamento ser realizado por recurso a meios automatizados[54].

A título exemplificativo, o direito de portabilidade possibilitará que um cliente/ consumidor possa mudar de operador telefónico, de fornecedor de eletricidade ou mesmo instituição de crédito sem perder os seus dados.

Ora, nos termos do disposto no artigo 20º, nº 3 do RGPD, o titular de dados pode simultaneamente com o direito à limitação, exercer o direito ao apagamento previsto no artigo 17º. Contudo, essa possibilidade apenas lhe será negada em relação a tratamentos que sejam necessários para o exercício de funções de interesse público ou ao exercício de autoridade pública.

2.5.6.1. O exercício e o conteúdo do direito de portabilidade

O direito de portabilidade encontra-se limitado aos dados cujo tratamento seja realizado por meios automatizados, e que, tenham como fundamento um tratamento lícito/ consentimento. Ou seja, o responsável pelo tratamento deve entregar os dados pessoais ao titular num formato estruturado, de uso corrente e de leitura automática.

---

[51] O artigo 18º, nº 1 alínea c) prevê uma exceção, na qual o titular dos dados pode, mesmo após os dados não serem necessários para a prossecução de certa finalidade eleita pelo responsável, obter a sua limitação para efeitos de declaração, exercício ou defesa de um direito no âmbito de um processo judicial.

[52]Fidalgo, Palmela, *O direito à portabilidade* cit. 96 ss: análise pormenorizada aos vários propósitos subjacentes à introdução do direito á portabilidade.

[53] Menezes Cordeiro, A. Barreto, *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*, Almedina, pág. 289.

[54]GT 29, *Orientações sobre o direito à portabilidade dos dados (WP 242 ver. 01),* 13 – dez.- 2016, por último revistas a 5-abr.-2017.

Quanto ao formato, ele não se encontra totalmente na disponibilidade do responsável pelo tratamento, pois, *i)* tem de ser estruturado- os dados devem ser organizados através de uma metodologia; *ii)* de uso corrente – deve atender às práticas do mercado, ou seja, ser conhecido; *iii)* de leitura automática – os dados têm que ser passíveis de serem consultados em sistemas de operação.

Nos considerandos que acompanham o artigo 20º do RGPD, apenas é acrescentada uma outra característica iv) interoperabilidade, ou seja, os dados devem ser fornecidos em formatos passíveis de serem consultados em vários e diferentes sistemas operativos.[55] Isso mesmo é sublinhado no artigo 18º, nº 2 da Lei de Execução.

2.5.6.2. A transmissão

A transmissão dos dados pessoais pode ocorrer de duas formais distintas. A *primeira*, consiste quando é o próprio titular dos dados a promover a transferência – artigo 20º, nº 1 RGPD. A *segunda*, consiste em o responsável pelo tratamento originário transferir os dados para um novo responsável pelo tratamento indicado pelo titular – artigo 20º, nº 2 do RGPD. Cabe assim, ao titular optar pela primeira ou segunda forma de transmissão.

2.5.6.3. Os direitos de terceiros

O direito à portabilidade de dados não se limita a satisfazer os direitos do próprio titular dos dados, mas deverá também de acordo com o disposto no artigo 20º, nº 4 salvaguardar os direitos e liberdades de terceiros. [56] Também os interesses do responsável pelo tratamento originário devem ser respeitados.

2.5.7. Direito de Oposição

O direito de oposição, consagrado no artigo 21º do RGPD, permite ao titular opor-se ao tratamento lícito dos seus dados pessoais[57], o qual, pode assumir três concretizações dispares, correspondentes a três regimes específicos: i) direito geral de oposição; direito de oposição relativo à comercialização direta; iii) direito de oposição relativo a tratamentos para fins de investigação científica. [58]

[55] Considerando 68, p.2.
[56] Fidalgo, Palmela, *O direito à portabilidade* cit., 118 ss.
[57] Considerando 69, p.1.
[58] Diretriz nº 95/46/CE, artigo 14º.

I) O *Direito geral de oposição,* permite que o titular se oponha ao tratamento lícito dos seus dados pessoais mediante a verificação dos seguintes requisitos: a) motivos relacionados com a sua situação particular; b) o tratamento de dados que lhe digam respeito com base no artigo 6º, nº 1, alínea e) ou f), ou no artigo 6º, nº 4, incluindo a definição de perfis com base nessas disposições.

Ora, cabe ao titular de dados demonstrar que situação em particular justifica a não realização do tratamento dos seus dados e não a sua licitude. [59] Não obstante, a sua oposição ao tratamento também ser possível se se fundar numa eventual violação de direitos, liberdades e garantias do titular.

Importa também relevar que, o titular dos dados pode invocar o seu direito à oposição contra todos os responsáveis, mas não contra os seus subcontratantes; que o mesmo pode ser exercido a todo o tempo, ou seja, numa fase anterior ao tratamento, durante o tratamento, mas nunca numa fase posterior e, ainda, ser exercido parcial ou totalmente;[60] não produz efeitos retroativos, mas apenas para o futuro; que, o responsável pelo tratamento confrontado com o exercício do direito à oposição, deve analisar o pedido formulado pelo titular de dados[61] e após a análise, deve cessar o tratamento, exceto se, apresentar razões imperiosas e legítimas[62] para a realização em concreto do tratamento e que se sobreponham aos interesses, direitos, liberdades invocadas pelo titular dos dados, ou para o exercício ou defesa de um direito num processo judicial; que, cabe ao responsável o ónus da prova e, em caso de dúvida prevalece o pedido de oposição efetuado pelo titular de dados; e, por fim, que no caso de o responsável não atender ao pedido efetuado pelo titular de dados, não invocando para tal recusa, numa das exceções já mencionadas, o titular de dados poderá recorrer à autoridade de controlo ou aos tribunais.

---

[59] TJUE 13-maio-2014, proc. C.131/12 (*Google Spain),* 76 *"A ponderação a efetuar… permite assim ter em conta, de maneira mais específica, todas as circunstâncias que rodeiam a situação concreta da pessoa em causa".*

[60]Menezes Cordeiro, A. Barreto, *Direito de Proteção de Dados à luz do RGPD e da lei nº 58/2019,* Almedina, pág. 302.

[61] TJUE 13-mai.-2014, proc. C-131/12 (*Google Spain),* 77.

[62] A expressão razões imperiosas e legítimas compreende as razões próprias do titular como de terceiros – Considerando 69, p.2 – pois, os artigos 6º/1, e), f) e 6º/4 do RGPD não permitem uma interpretação diversa.

Acresce ainda que, o responsável pelo tratamento deverá, também, quando assim seja peticionado pelo titular de dados, proceder ao apagamento dos dados pessoais objeto do direito de oposição, conforme o artigo 17º/1, alínea c) do RGPD.

II. Direito de oposição relativo à comercialização direta[63]*, e*m consonância com o disposto no artigo 21º/2 do RGPD, consiste na faculdade de os titulares de dados poderem opor-se ao tratamento dos seus dados pessoais sempre que estes estejam a ser tratados para efeitos de comercialização direta sem necessidade de invocação de algum argumento substantivo, bastando o simples facto de os dados serem utilizados com o propósito de comercialização (direito potestativo clássico).

Contudo, devemos de ter em conta os fundamentos da comercialização direta, pois pode visar um interesse público, e por tal motivo, informar os cidadãos de um determinado perigo ou ocorrência, o titular de dados não deverá poder opor-se, sem mais, a tal comercialização.

III. Direito de oposição relativo a tratamentos para fins de investigação científica – consiste em mais um direito especial de oposição, no qual, cabe ao titular de dados o ónus de prova, ou seja, demonstrar a particularidade da sua situação e ao responsável pelo tratamento para a prossecução de interesses públicos.

2.6. O Responsável pelo tratamento

O Responsável pelo tratamento, como já mencionado no ponto 2.2.3., consiste na pessoa singular ou coletiva, a autoridade publica, a agência ou outro organismo que determina as finalidades e os meios pelos quais os dados pessoais são tratados.

Ora, uma determinada empresa/organização será responsável pelo tratamento se decidir *"porquê"* e *"como"* os dados pessoais devem ser tratados e, de acordo com a natureza, o âmbito, o contexto e as finalidades do tratamento de dados, bem como os riscos

[63] *"A definição comunicações comerciais direta, constantes da proposta de Regulamento relativo à privacidade e às comunicações eletrónicas pode ser empregue como um importante ponto de partida: qualquer forma de publicidade, oral ou escrita, enviada por um ou mais utilizadores finais identificados ou identificáveis de serviços de comunicações eletrónicas, incluindo a utilização de sistemas de chamada e de comunicação automatizados, ou sem interação humana, de correio eletrónico, SMS, etc." in* Direito de Proteção de Dados à luz do RGPD e da lei nº 58/2019.

para os direitos e liberdades das pessoais singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento deverá aplicar as medidas técnicas e organizativas necessárias para assegurar e comprovar que o tratamento é realizado em conformidade com o regulamento, devendo essas medidas ser revistas e atualizadas consoante a necessidade – artigo 24º, nº 1 do RGPD.

2.6.1. Responsáveis conjuntos pelo tratamento

Estamos perante responsáveis conjuntos pelo tratamento quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento. Ou seja, determinada empresa/organização será responsável conjunto pelo tratamento[64] se, determinar em conjunto com uma ou mais organizações, *"porquê"* e *"como"* os dados pessoais devem ser tratados.

Os responsáveis conjuntos, mediante acordo, devem determinar as respetivas responsabilidades pelo cumprimento do RGPD[65], nomeadamente, no que diz respeito aos direitos dos titulares dos dados e aos respetivos deveres de fornecer as informações expressas nos artigos 13º (i*nformações a facultar quando os dados pessoais são recolhidos junto do titular)* e 14º (*informações a facultar quando os dados pessoais não são recolhidos junto do titular)*[66]. Os principais pontos desse acordo devem ser comunicados aos titulares dos dados que são objeto desse tratamento. [67]

---

[64] *Exemplo: "Uma determinada empresa/ organização oferece serviços de babysitting através de uma plataforma em linha. Simultaneamente, a sua empresa/ organização tem um contrato com outra empresa que lhe permite prestar serviços de valor acrescentado. Estes serviços incluem a possibilidade de os pais escolherem, não só a babysitter, mas também alugar jogos e DVD para a babysitter levar consigo. Ambas as empresas participam na configuração técnica do sítio web. Neste caso, as empresas decidiram utilizar a plataforma para ambas as finalidades (serviços de babysitting e aluguer de DVD/jogos) e partilham frequentemente os nomes de clientes. Por conseguinte, as duas empresas são responsáveis pelo tratamento, porque não só concordaram em oferecer a possibilidade de "serviços combinados", como também conceberam e utilizaram uma plataforma comum"* - https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_pt .

[66] Artigo 26º, nº 1 do RGPD.

[67] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_pt;

2.6.2. O subcontratante

O subcontratante (artigo 4º, nº 8 do RGPD) consiste na pessoa singular ou coletiva, a autoridade publica, a agência ou outro organismo que, efetua o tratamento de dados pessoais em nome do responsável pelo tratamento,[68]cujos deveres perante o responsável pelo tratamento devem ser especificados num contrato ou noutro ato jurídico[69].

Neste contexto, o responsável pelo tratamento, deverá assegurar o cumprimento do regulamento de proteção de dados, ou seja, deverá contratar apenas, e se, o subcontratante em questão, oferecer garantias suficientes, especialmente em conhecimentos especializados, fiabilidade e recursos, quanto à execução de medidas técnicas e organizativas que cumpram os requisitos do RGPD, nomeadamente no que se refere à segurança do tratamento. [70]

Não obstante, o subcontratante poderá também subcontratar uma parte das suas tarefas a um outro subcontratante ou nomear um subcontratante conjunto, no entanto, só estará possibilitado a fazê-lo coma autorização prévia, por escrito, do responsável pelo tratamento de dados. [71]

Por fim, após concluir o tratamento por conta do responsável pelo tratamento, o subcontratante deverá de acordo com a vontade daquele, devolver ou apagar os dados pessoais, a menos que seja exigida a conservação de dados pessoais ao abrigo do direito da União ou do Estado- membro a que o subcontratante está sujeito.[72]

---

[68] *Exemplo:* Uma fábrica de sapatos tem muitos trabalhadores e decide assinar um contrato com uma empresa de contabilidade que este efetue o pagamento dos seus salários. A fábrica informa a empresa contabilidade quando os salários devem ser pagos, quando um trabalhador sai da empresa ou recebe um aumento, e fornece todos os restantes dados necessários para a folha de salário e o pagamento. A empresa de contabilidade fornece o sistema informático e armazena os dados dos trabalhadores. A fábrica é a responsável pelo tratamento e a empresa de contabilidade é a subcontratante.

[69] *Por exemplo*, indicar o que acontece aos dados pessoais uma vez terminado o contrato

[70] Considerando 81, RGPD; Artigo 28º,nº 1 do RGPD.

[71]Artigo 28º, nº2 do RGPD; https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_pt.

[72] Considerando 81, *parte final* – RGPD.

2.7. Autoridade de Controlo

2.7.1. Autoridade de Controlo Nacional

A Autoridade de Controlo Nacional consiste na entidade que supervisiona e contribui para a aplicação coerente do RGPD[73] - "as guardiãs dos direitos dos titulares de dados pessoais"[74].

De acordo com o artigo 51º do RGPD, cada Estado- Membro devem estabelecer uma ou mais autoridades públicas independentes, às quais cabe a responsabilidade de fiscalizar a aplicação do RGPD, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União.[75] Para tal, autoridades de controlo devem cooperar entre si e com a Comissão[76].

Isto posto, as autoridades de controlo previstas no artigo 8º/1 da Carta e artigo 16º/2 do TJUE, desempenham um papel fulcral na aplicação do Direito da Proteção de dados a nível europeu e nacional. [77]

2.7.1.1. Independência

As autoridades de controlo agem com total independência na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos, ou seja, os seus membros não estão sujeitos a influências externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes e, não solicitam nem recebem instruções de outrem[78].

Não obstante, os membros das autoridades de controlo devem abster-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não podem desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível.

Ademais, por forma a assegurar a independência das autoridades de controlo, cada Estado-Membro deve assegurar que estas dispõem dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários à prossecução eficaz das suas atribuições e ao exercício dos seus poderes[79].~

---

[73] Artigo 51º, nº 2 do RGPD.
[74] Cordeiro, António Menezes, "Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019, pág. 398, Almedina, Coimbra, 2020
[75] Artigo 51º, nº 1 do RGPD.
[76] Artigo 51º, nº 2 do RGPD.
[77] Cordeiro, António Menezes, "Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019, pág.400, Almedina, Coimbra, 2020
[78] Artigo 52º, nº 1 e 2 do RGPD.
[79] Artigo 52º, n 4 do RGPD.

2.7.2. A Comissão Nacional de Proteção de Dados (CNPD)

2.7.2.1. Noção

A CNPD é uma entidade administrativa independente, com personalidade jurídica de direito público e com poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República[80].

2.7.2.2. Funções

A CNPD controla e fiscaliza o cumprimento do RGPD, da Lei 58/2019, da Lei 59/2019 e da Lei 41/2004, bem como as demais disposições legais e regulamentares referentes à matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos dos seus dados pessoais[81].

Na prossecução das suas atribuições e competências previstas no artigo 57º do RGPD e 6º da Lei 58/2019 e 44º da Lei 59/2019, e no exercício dos seus poderes, conforme os artigos 58º do RGPD, 8º da Lei 58/2019 e 45º da Lei 59/2019, a CNPD atua com independência[82].

2.7.2.3. Composição

A CNPD é composta por sete membros, eleitos e designados nos seguintes termos: a) o Presidente é eleito pela AR; b) a AR elege dois vogais; c) o CSM designa um vogal; d) CSMP designa um vogal; e) o Governo designa dois vogais[83].

O mandato de cada membro é de cinco anos, com a possibilidade de ser renovado por duas vezes[84].

A Lei 58/2019 impôs a designação de um Fiscal Único designado pela AR, a quem cabe controlar a legalidade, a regularidade e a boa gestão financeira e patrimonial da CNPD, conforme o artigo 19º- A da Lei Orgânica da CNPD[85].

---

[80] Artigo 4º, nº 1 da Lei 58/2019.
[81] Parágrafo 2, https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/.
[82] Parágrafo 4, https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/.
[83] Artigo 3º, nº 1 da Lei Orgânica da CNPD.
[84] Artigo 3º, nº 2 da Lei Orgânica da CNPD.
[85] Menezes Cordeiro, António Barreto, *"Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019",* pág. 400, Almedina, Mar. 2020.

2.7.2.4. Competência, atribuições e poderes

2.7.2.4.1. Competência

As autoridades de controlo são competentes para prosseguir as atribuições e exercer os poderes que lhe são conferidos pelo RGPD no território do seu Estado- Membro[86].

No entanto, as autoridades de controlo não têm competência para controlar operações de tratamento efetuadas por tribunais que atuem no exercício da sua função jurisdicional[87].

2.7.2.4.2. Competência da autoridade de controlo principal

De acordo com o disposto no artigo 56º, nº 1 do RGPD, a autoridade de controlo do estabelecimento principal ou do estabelecimento único (em território da União) do responsável pelo tratamento ou do subcontratante é competente para agir como autoridade de controlo principal para o tratamento transfronteiriço realizados por esse responsável ou subcontratante[88].

É possível, na ótica de *António Menezes Cordeiro*, perspetivar a autoridade de controlo principal de um *ponto de vista formal* e de um *ponto de vista substantivo*[89]. Do *ponto de vista formal*, a autoridade de controlo principal é o único interlocutor do responsável pelo tratamento ou do subcontratante no âmbito dos tratamentos transfronteiriços, contudo, do *ponto de vista substantivo,* cabe a esta, liderar todo o processo, em estreita cooperação com as autoridades de controlo interessadas, artigos 56º, nº 6 e 60º, nº 1 do RGPD.

2.7.2.4.3. Atribuições

As atribuições das autoridades de controlo encontram-se consagradas maioritariamente no artigo 57º do RGPD, devendo, no entanto, ser complementadas com o disposto nos artigos 6º e 7º da Lei 58º/2019 e podem ser brevemente sistematizadas em: i)

[86] Artigo 55º, nº 1 do RGPD.
[87] Artigo 55º, nº 3 do RGPD.
[88] Menezes Cordeiro, António, *"Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019",* pág. 411, Almedina, Mar. 2020.
[89] Menezes Cordeiro, António, *"Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019",* pág. 412, Almedina, Mar. 2020.

controlar e executar a aplicação da lei; ii) promover, sensibilizar e informar; iii) aconselhar as autoridades nacionais; iv) acompanhar a evolução do Direito de proteção de dados [90] .

A lista constante no artigo 57º do RGPD é bastante extensa, no entanto, não esgota todas as atribuições das autoridades de controlo, tal como resulta da alínea v) do nº 1 do artigo 57º *"desempenha quaisquer outras tarefas relacionadas com a proteção de dados pessoais".*

Esta alínea, consiste numa cláusula aberta, permitindo que outras atribuições sejam conferidas pelos Direitos nacionais e pelo Direito da União às autoridades de controlo, como também concede às autoridades de controlo uma certa discricionariedade de atuação, dentro dos limites da lei e atendendo às atribuições dos demais sujeitos[91].

2.7.2.4.4. Poderes

O artigo 58º do RGPD atribui às autoridades de controlo três poderes: *i) investigação*; *ii) correção e sanção*; *iii) consultivos e de autorização.*

Os poderes de investigação subdividem-se em três subpoderes: *i)* informação – permitindo que as autoridades de controlo solicitem a prestação de informações e acedam a todos os dados pessoais e informações necessárias (alíneas a) e e) do nº 1 do artigo 58º) ; *ii)* investigação em sentido estrito – possibilidade de realizar auditorias e de aceder às instalações do responsável pelo tratamento e do subcontratante, incluindo os meios de tratamento utilizados (alíneas b) e f) do nº 1 do artigo 58º); *iii)* notificação – poder de notificar os responsáveis e os subcontratantes relativamente a alegadas violações do RGPD (alínea d) do nº 1 do artigo 58º).

Os poderes de correção e sanção estão previstos no nº 2 do artigo 58º do RGPD, de forma gradual, ou seja, da medida menos gravosa para a mais gravosa, podendo consistir numa mera advertência ao responsável pelo tratamento e no limite a aplicação de coimas e suspender o envio de dados para destinatários em países estrangeiros ou organizações internacionais.

[90] Menezes Cordeiro, António, *"Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019",* pág. 414, Almedina, Mar. 2020.
[91] Menezes Cordeiro, António, *"Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019",* pág. 414, parágrafo 2, Almedina, Mar. 2020.

Os poderes consultivos e de autorização previstos no nº 3 do artigo 58º do RGPD, consiste em aconselhar o responsável pelo tratamento; emitir pareceres por iniciativa própria ou por solicitação; autorizar o tratamento previsto no nº 36, nº 5 se a lei do Estado- Membro exigir uma autorização prévia; emitir pareceres e aprovar projetos de códigos de conduta nos termos do artigo 40º, nº 5; acreditar organismos de certificação nos termos do artigo 43º; emitir certificações e aprovar os critérios de certificação nos termos do artigo 42º, nº 5; adotar cláusulas-tipo de proteção de dados previstas no artigo 28º, nº 8 e no artigo 46º, nº 2, alínea d); autorizar as cláusulas contratuais previstas no artigo 46º, nº 3 alínea b); aprovar as regras vinculativas aplicáveis às empresas nos termos do artigo 47º.

2.8. A Lei de Execução (Lei nº 58/2019)

O RGPD é diretamente aplicável em todo o território da União Europeia desde 25 de maio de 2018, porém este atribui uma margem de discricionariedade[92] aos Estados Membros para especificarem algumas das suas regras, nomeadamente, a determinação mais precisa das condições de certos tratamentos de dados pessoais.

É neste contexto que a Lei nº 58º/2019 de 8 de agosto surge, para assegurar a execução do RGPD na ordem jurídica portuguesa, harmonizar a legislação nacional com as disposições já vigentes no RGPD e detalhar a regulamentação da proteção de dados em diferentes matérias que, por um lado, não estão expressamente previstas no RGPD, ou que estão reguladas no RGPD.

A lei de execução veio, desde logo, revogar a Lei de Proteção de Dados Pessoais, proceder a alterações à Lei nº 43º/2004, de 18 de agosto, que regula a organização e o funcionamento da Comissão Nacional de Proteção de Dados (CNPD), bem como a Lei nº 26/2016, de 26 de agosto, que aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos.[93]

---

[92] O Regulamento Geral de Proteção de Dados, de acordo com o artigo 288º do TFUE, tem carácter geral, obrigatório em todos os seus elementos e é diretamente aplicável. Contudo, este contém inúmeras cláusulas de abertura (normas que atribuem competências legislativas ou de outras índoles aos Estados-Membros e à própria União, impondo ou permitindo que estes apliquem medidas concretizadoras, complementares ou modificativas dos próprios regulamentos. (Cordeiro, A.M)

[93] Mota, Joana; Sampaio, Alexandre Pedral. *"Regulamento Geral de Proteção de Dados em Portugal – Alguns apontamentos à sua Lei de Execução",* pág. 2, https://www.uria.com/documentos/publicaciones/6855/documento/port01.pdf?id=9341

2.8.1. Âmbito de aplicação

A Lei de Execução aplica-se a todos os tratamentos de dados pessoais realizados em território nacional, independentemente da natureza privada ou pública do responsável pelo tratamento ou do subcontratante[94], aos tratamentos de dados pessoais tratados fora do território nacional, nomeadamente, no âmbito de uma atividade de um estabelecimento situado em território nacional; que afetem titulares dos dados que se encontrem em território nacional, nos termos do artigo 3º/2 do RGPD; que afetem dados pessoais que estejam inscritos nos postos consulares de que sejam titulares portugueses residentes no estrangeiro.

2.8.2. Alterações introduzidas pela lei de execução ao RGPD

A lei de execução estabeleceu várias alterações fundamentais ao RGPD, nomeadamente, as seguintes[95]:

a) Encarregado de Proteção de Dados – a nova lei adita algumas funções ao regime do encarregado de proteção de dados consagrado no RGPD, nomeadamente, *"assegurar a realização de auditorias, quer periódicas, quer não programadas; sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança; e assegurar as relações com os titulares dos dados nas matérias abrangidas pelo RGPD e pela legislação nacional em matéria de proteção de dados".*

b) Acreditação, certificação e códigos de conduta – a lei determina que a autoridade competente para a acreditação dos organismos de certificação no domínio da proteção de dados é o IPAC, I.P. A certificação é, também, efetuada pelos referidos organismos acreditados pelo IPAC, I.P. O tratamento de dados pessoais por parte da administração direta e indireta do Estado é objeto de código de conduta próprio.

c) Consentimento de menores, consentimento nas relações laborais e renovação do consentimento - o consentimento dos menores foi fixado nos 13 anos de idade, pelo que o consentimento de crianças menos de 13 anos terá de ser prestado pelos respetivos representantes legais. No âmbito das relações laborais, a Lei determina que o consentimento

[94] Artigo 2º, nº 1 da Lei de Execução.

[95] Tecnologia e Privacidade, " Os 12 pontos fundamentais da lei nacional que assegura a execução do RGPD" - https://www.plmj.com/xms/files/03_Novidades_legislativas/2019/008_agosto/NL_Os_12_pontos_fundamentais_da_lei_nacional_que_assegura_a_execucao_do_....pdf

dos trabalhadores não constitui um fundamento de licitude do tratamento, se deste resultar uma vantagem jurídica ou económica para o trabalhador ou se o tratamento estiver abrangido pelo âmbito de execução do contrato de trabalho.

d) A proteção de dados pessoais de pessoas falecidas – a lei consagra uma norma que visa proteger determinados dados pessoais de pessoas falecidas, nomeadamente as categorias especiais de dados pessoais referidas no RGPD e dados que se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações. Nos termos da lei, os direitos de acesso, retificação e apagamento são exercidos por pessoa designada pelo titular, em vida, ou, quando tal não suceda, pelos respetivos herdeiros. Sendo também conferida ao titular a faculdade de determinar a impossibilidade de exercício daqueles direitos após a sua morte.

e) A videovigilância- a lei estabelece alguns limites sobre os quais as câmaras de videovigilância não podem incidir sobre as vias públicas, zonas de digitação de códigos de multibanco ou terminais de pagamento ATM, interior de áreas reservadas a clientes ou utentes como instalações sanitárias ou provadores de vestuário, etc., e salvaguarda que, nos estabelecimentos de ensino aquelas apenas podem incidir sobre zonas externas e de acesso a espaços como laboratórios ou salas de informática. Prevê ainda, a necessidade autorização prévia da CNPD para a instalação de videovigilância de som.

f) Prazo de conservação de dados pessoais – a lei prevê que o *"prazo de conservação de dados pessoais é o que estiver fixado por norma legal ou regulamentar ou, na falta desta, o que se revele necessário para a prossecução da finalidade".* Ora, em matéria contratual, os dados pessoais podem ser conservados até ao termo do prazo de prescrição dos direitos correspetivos. Finda a finalidade, os dados devem ser eliminados ou anonimizados. A lei consagra, porém, uma norma especificamente dirigida à reconstituição das carreiras contributivas, caso em que os dados podem ser conservados sem limite de prazo.

g) Tratamentos de dados por parte de entidades públicas para finalidades distintas das que presidiram à recolha, publicação de dados em jornal oficial e publicação de dados no âmbito da contratação pública – os tratamentos de dados por parte de entidades públicas para finalidades distintas das que presidiram à recolha devem ter como principal fundamento assegurara a prossecução do interesse público que por outra via não poderia ser acautelado. Ademais, a transmissão de dados pessoais entre entidades públicas para

finalidades distintas deve ser objeto de protocolo entre as mesmas. No que diz respeito à publicação em jornal oficial, os dados pessoais só podem ser alterados, rasurados ou ocultados, pois, nesses casos o direito ao esquecimento sofre várias limitações. Relativamente aos lados publicados no âmbito da contratação pública, sempre que o nome seja suficiente para a identificação do contraente público e do cocontratante, não devem ser publicados outros dados pessoais.

h) Tratamento de dados pessoais nas relações laborais – para além das considerações relativas ao consentimento prestado pelos trabalhadores no contexto da relação laboral já afloradas, a Lei também estabelece normas quanto à utilização de meios de vigilância à distância e normas relativas ao tratamento de dados biométricos. No que concerne à utilização de meios de vigilância à distância, a lei estabelece que as imagens ou dados registados só podem ser utilizados no âmbito de processo penal. No que respeita, ao tratamento de dados de natureza biométrica, o mesmo só é considerado legítimo para controlo da assiduidade e controlo de acessos às instalações do empregador.

i) Tratamento de dados de saúde e dados genéticos - a lei estabelece que o tratamento de dados pessoais necessários para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou gestão de sistemas e serviços de saúde ou de ação social, bem como o tratamento de dados pessoais necessário por motivos de interesse público no domínio da saúde pública, deve ser efetuado por profissionais sujeitos a obrigação de sigilo. O acesso aos dados é feito de forma exclusivamente eletrónica, salvo impossibilidade técnica ou expressa indicação em contrário do titular de dados. O responsável pelo tratamento de dados de saúde e genéticos tem que assegurar um mecanismo de rastreabilidade e notificação, uma vez que a lei prevê que o titular dos dados tem o direito a ser notificado de qualquer acesso realizado aos seus dados pessoais.

j) Tratamento para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos - os titulares dos dados poderão ver algum dos seus direitos limitados para efeitos de tratamento de dados pessoais, nomeadamente o direito de acesso, retificação, limitação do tratamento e de oposição.

k) Tutela jurisdicional e legitimidade da CNPD- as ações propostas contra a CNPD são da competência dos tribunais administrativos, incluindo as que se reportem a matéria contraordenacional.

l) Regime sancionatório – Contraordenações: a lei procede a uma graduação das contraordenações em "muito graves" e "graves" e, relativamente aos critérios de determinação da medida da coima, acrescenta aos critérios previstos no RGPD, os seguintes: "*a situação económica do agente, no caso de ser pessoa singular, ou o volume de negócios e o balanço anual, no caso de pessoa coletiva", " o carácter continuado da infração"* e *" a dimensão da entidade, tendo em conta o número de trabalhadores e natureza dos serviços prestados".* A lei estabelece ainda que, a instauração de um processo contraordenacional[96] depende sempre da prévia advertência da CNPD, para cumprimento do prazo razoável da obrigação omitida ou reintegração da proibição violada, exceto nos casos em que haja dolo; *Crimes:* relativamente ao crime de acesso indevido (artigos 9º e 10º do RGPD), a pena é agravada para o dobro; todos os crimes são de natureza pública; a tentativa é sempre punível; a moldura abstrata do crime de violação do dever de sigilo foi reduzida até dois anos de prisão ou até 240 dias de multa até um ano de prisão ou até 120 dias de multa. No que diz respeito a sanções acessórias, a lei prevê a possibilidade de ser ordenada a proibição do tratamento, bloqueio e o pagamento total ou parcial dos dados. E, nos crimes e coimas superiores a 100.000 € a possibilidade de condenação no Portal do Cidadão, por período não inferior a 90 dias.

2.8.3. A deliberação da CNPD sobre a desaplicação de algumas normas da Lei 58/2019

A Comissão Nacional de Proteção de Dados (CNPD) deliberou desaplicar algumas normas da Lei nº 58/2019 de 8 de Agosto, por considerar que estas contradizem manifestamente o estatuído no Regulamento Europeu de Proteção de Dados, o que, por sua vez, viola o princípio do primado da União [97], bem como, afeta seriamente o funcionamento

[96] As coimas aplicam-se tanto a entidades públicas como privadas.

[97] O primado da União europeia consiste numa norma que regula a relação entre o direito europeu e o direito nacional. As normas de direito da União Europeia e as normas nacionais muitas vezes têm como objeto as mesmas situações da vida, pelo que, podem entrar em conflito, na medida em que contenham resoluções incompatíveis entre si. Ora, nestes casos, aplicar-se-á o princípio do primado, ou seja, que em caso de conflito, os Estados têm o dever de aplicar a norma de direito da União Europeia e de desaplicar a nora de direito nacional. Este princípio foi reconhecido pelo TJUE, que o fundamenta com a necessidade de homogeneidade na aplicação do direito europeu e no facto de os EM não poderem invocar direito nacional para fundamentarem o incumprimento das suas obrigações europeias. Este princípio vincula todas as entidades públicas, nomeadamente, a administração pública e os tribunais nacionais. ("*Princípio do Primado do Direito da União Europeia"* in Lexionário; https://dre.pt/web/guest/lexionario/-/dj/153680380/view)

do mecanismo de coerência, que tem como objetivo, uma aplicação uniforme das regras de proteção de dados em todo o espaço da União Europeia.

No entendimento unânime da CNPD, algumas normas da referida lei, põem em causa a aplicabilidade direta do regulamento europeu e, consequentemente, a eficácia e consistência da sua aplicação.

Esta deliberação tem como fundamento o artigo 8º da Constituição República Portuguesa, a qual prevê que, as disposições dos tratados e as normas emanadas das instituições da UE são aplicáveis na ordem jurídica interna nos termos definidos pelo direito da União, e na Jurisprudência da TJUE que determina que as entidades administrativas estão obrigadas a desaplicar as normas nacionais que contrariem o direito da UE. [98]Entre as normas da Lei 58/2019 que a CNPD deliberou desaplicar, nas situações de tratamento de dados pessoais que tenha que apreciar, as seguintes: artigo 2º, nºs 1 e 2; artigo 20º, nº 1; artigo 23º; artigo 28º, nº 3, alínea a); artigo 37º, nº 1, alíneas a), h) e k), e nº2; artigo 38, nº 1, alínea b) e nº 2; artigo 39º, nºs 1 e 3; artigo 61º, nº 2; artigo 62º, nº 2. [99]

Entre as normas referidas destacam-se as seguintes:

i) Artigo 20º, nº1 o qual estatui que "*os direitos de informação e de acesso a dados pessoais previstos nos artigos 13º e 15º do RGPD não podem ser exercidos quando a lei imponha ao responsável pelo tratamento ou subcontratante um dever de segredo que seja oponível ao próprio titular dos dados",* por considerar existir uma restrição legal infundada ao exercício destes direitos por parte dos titulares dos dados;

ii) Artigo 28º, nº 3 alínea a) o qual estabelece que "*salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais: se desse tratamento resultar uma vantagem jurídica ou económica para o trabalhador",* porque limita de forma excessiva a relevância do consentimento do trabalhador, com isso eliminando qualquer margem de livre arbítrio dos trabalhadores mesmo quando há condições para a sua manifestação sem risco para os seus direitos e interesses;

[98] Deliberação/2019/494 da Comissão Nacional de Proteção de Dados, aprovada a 3 de setembro de 2019.
[99] Ibidem.

iii) Artigo 37º, nº 1 alínea a), h) e k) e o artigo 38º, nº 1 alínea b) na medida em que contrariam o elenco taxativo das infrações previstas no RGPD e o respetivo enquadramento sancionatório;

iv) Artigo 37º, nº 2 e o artigo 38º, nº 2 por definirem molduras sancionatórias distintas em função da dimensão das empresas e da natureza coletiva ou singular dos sujeitos que realizem tratamento de dados quando o RGPD não prevê a adoção destes critérios na medida da determinação das sanções aplicáveis.

A consequência da desaplicação das disposições da Lei 58/2019 acima mencionadas, consiste na aplicação direta das regras constantes do RGPD que, de acordo com a Deliberação, estavam manifestamente suprimidas, contrariadas e prejudicadas no seu efeito útil por aquelas[100].

2.8.4. Análise crítica

A lei 58/2019 está longe de ter solucionado alguns problemas interpretativos e lacunas do RGPD ou de concretizações a nível nacional concedidas pelo legislador europeu ao legislador nacional.

"*A lei 58/2019 encaixa-se perfeitamente na expressão "too little too late",* pois assume um teor vago e aberto em muitas das suas disposições, reproduz desnecessariamente o texto do RGPD, nada de novo trazendo face à legislação europeia e algumas opções do legislador nacional são de questionável legalidade ou demonstram pouco rigor técnico relativamente aos conceitos utilizados e previstos no RGPD. [101]

Alexandre Sousa Pinheiro realça na lei 58/2019 algumas incongruências e insuficiências, nomeadamente, resolve alguns problemas de aplicação do RGPD, mas deixa muitos outros sem cobertura legal ou com a regulação deficitária, como por exemplo, o setor segurador (na área da saúde – artigo 9º do RGPD); a matéria relativa a decisões individuais automatizadas (artigo 22º do RGPD) – inteligência artificial; a matéria sancionatória

[100] Mota, Joana; Sampaio, Alexandre Pedral *in "Regulamento Geral de Proteção de Dados em Portugal – Alguns apontamentos à sua Lei de Execução",* pág. 6, https://www.uria.com/documentos/publicaciones/6855/documento/port01.pdf?id=9341.

[101] Mota, Joana; Sampaio, Alexandre Pedral *in "Regulamento Geral de Proteção de Dados em Portugal – Alguns apontamentos à sua Lei de Execução",* pág. 7, https://www.uria.com/documentos/publicaciones/6855/documento/port01.pdf?id=9341.

apresenta um excesso de crimes, devendo alguns subsumir-se a contraordenações; o direito à portabilidade (artigo 18º da lei 58/2019) reduz o âmbito de aplicação do RGPD; as contraordenações não estão suficientemente tipificadas; contrariamente ao RGPD, prevê contraordenações graves a aplicar ao encarregado de proteção de dados (artigo 39º, nº 1, alínea p) da lei), entre outros exemplos[102].

[102] Pinheiro, Alexandre Sousa, em entrevista a ADVOCATUS by ECO a 11 de Set. 2019 Alexandre Sousa Pinheiro Antecipa Conferência "Nova Lei de Proteção de Dados" – ECO (sapo.pt)

CAPÍTULO III – DIREITO DA PROTEÇÃO DE DADOS EM TEMPOS DE PANDEMIA

Nos finais do ano 2019 e inícios do ano 2020, o mundo foi surpreendido e fortemente abalado com o surto Covid- 19, sobre o qual, nada se sabia, nem quanto ao seu alcance, nem consequências.

Perante tal surpresa, o mundo foi reagindo ao comportamento do vírus e, na medida em que este se propagava. Os ordenamentos jurídicos foram adotando medidas preventivas (reativas)[103] que consideraram pertinentes e eficazes para monitorizar, compreender, prevenir e combater a proliferação do vírus. E, Portugal, não foi exceção, pois, ao longo da evolução da situação Pandémica foi adotando várias medidas, nomeadamente, o rastreio de contacto (por forma a identificar e monitorizar qualquer pessoa que possa ter estado em contacto com uma pessoa infetada), restrições de viagens, quarentena, diminuição da lotação em espaços públicos e privados (noutros uma total supressão – discotecas e bares), exames médicos, vacinas, etc.

Ora, para a execução destas medidas é fulcral a obtenção e potencial partilha de informações pessoais, incluindo dados sobre a saúde, viagens, contactos pessoais, emprego do individuo, família e terceiros.

Isto posto, é importante, como também, necessário, refletir acerca da existência, ou não, de um equilíbrio entre a limitação do direito à privacidade e do direito de proteção de dados em prol do interesse público- a saúde pública.

3.1. Dados relativos à saúde

Os dados relativos à saúde, consistem numa categoria de dados sensíveis prevista no artigo 4º, nº 15 do RGPD - "*dados pessoais relativos à saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde que revelem informações sobre o seu estado de saúde".*

[103] Reativas no sentido de que, o combate à propagação do vírus era de tal forma rápida e imprevisível que não permitia aos ordenamentos jurídicos, muitas vezes, anteciparem-se aos efeitos do vírus, restando-lhes apenas reagir.

O Considerando 35do RGPD, completa o referido artigo, " (…) *todos os dados relativos ao estado de saúde de um titular de dados revelem informações sobre a sua saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro (…) inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços na saúde, ou durante essa prestação (…) a essa pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, uma deficiência, um risco de doença, historial clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo medico ou um teste de diagnóstico in vitro".*

Ora, todos os dados recolhidos e tratados pelas *health apps, fitness apps ou smartwatches* são dados relativos à saúde[104]

3.2. A Proteção de Dados na Saúde

I. O Regulamento Geral de Proteção de Dados prevê, especificamente, as crises de saúde pública e disposições relativas ao tratamento de dados pessoais nessas situações.

O ***artigo 6º, nº 1 nas suas alíneas c), d), e) do RGPD*** consagra que, o tratamento de dados pessoais é sempre lícito, mesmo sem consentimento do seu titular, quando este seja necessário para o cumprimento de uma obrigação legal a que o responsável esteja sujeito, para proteger os interesses vitais do titular de dados ou de outra pessoa singular, para o exercício de funções de interesse público ou exercício de autoridade pública de que está investido o responsável pelo tratamento.

O ***Considerando 46***, dispõe que, "*o tratamento de dados pessoais também deve ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do*

[104] Cordeiro, António Menezes, *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*, pág. 141, Almedina.

titular dos dados ou de qualquer outra pessoa singular. (...) Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento necessário para fins humanitários, incluindo a monotorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana."

O ***artigo 9º do RGPD,*** prevê a proibição do tratamento de categorias especiais de dados pessoais sem consentimento explícito do titular, também contempla exceções, nomeadamente, "*por motivos de interesse público importante", "para efeitos de medicina preventiva ou do trabalho (...) diagnóstico médico (...), "por motivos de interesse público ou no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde".*

Os ***Considerandos 52, 53 e 54 do RGPD*** completam ainda as referidas disposições, reconhecendo as necessidades de tratamento de categorias especiais de dados pessoais para a prevenção ou controlo de doenças transmissíveis e outras ameaças à saúde; salientando que esses dados devem ser tratados para fins relacionados com a saúde quando for necessário para atingir os objetivos no interesse das pessoas singulares e no seu todo; e reconhecendo ainda, que o tratamento de categorias especiais de dados pessoais sem consentimento pode ser necessário por razões de saúde pública.

Pelo exposto, podemos afirmar que, os tratamentos de dados de saúde em tempos de pandemia (exceção) devem fundamentar-se na legislação e regulação nela fundada e não no consentimento. [105]

II. Os tratamentos de dados pessoais em estado de emergência/ crise de saúde pública/ pandemia, que acarretem restrições a direitos fundamentais (nomeadamente, o direito à proteção de dados pessoais, previsto no artigo 8º da CEDF), devem respeitar o princípio da proporcionalidade e os direitos concretamente afetados (artigo 52º da CEDF e artigo 9º, nº 2, alínea g) do RGPD).

[105] Alexandre Sousa Pinheiro , *A COVID-19 e a proteção de dados pessoais, in Observatório Almedina – de especialistas para especialistas* - https://observatorio.almedina.net/index.php/2020/04/28/a-covid-19-e-a-protecao-de-dados-pessoais/

Ora, em situação de pandemia, apesar de os tratamentos de dados estarem fundados na lei, interesse público e proteção de interesses vitais, devem prezar pelo cumprimento do princípio da proporcionalidade no tratamento desses dados.

Assim, pode concluir-se que, qualquer direito da proteção de dados pessoais – direito de informação, apagamento, oposição, acesso, retificação, portabilidade, etc.- pode ser afetado, desde que proporcionalmente (***Considerando 73***- *"necessárias e proporcionais numa sociedade democrática"*), quando estejam em causa "*objetivos importantes de saúde pública" – **artigo 23º, nº1, alínea e)*** - ou seja, numa situação de Pandemia. [106]

3.3. As aplicações de "Contact Tracing"

O "C*ontact Tracing"* ficou conhecido nos seguintes países: China, Coreia do Sul, Taiwan, Singapura, Japão e Israel, nos quais, a utilização era imposta. [107]

O fundamento deste mecanismo é a ineficácia e insuficiência do rastreio realizado pelos profissionais de saúde e respetivas entidades públicas, que visam detetar e monitorizar os contactos de uma pessoa infetada.[108] A sua finalidade, em contribuir de forma significativa o combate e monotorização da pandemia.

Assim, as funções deste mecanismo seriam realizadas de forma anónima, sem que se conhecessem os titulares dos dados pessoais. Ou seja, através do uso da geolocalização e tecnologia *Bluetooth*, recolher-se-ia o número de telemóvel de uma determinada pessoa infetada e informar-se-ia (via SMS) de forma anónima, as pessoas que com ela tiveram contacto recente.[109]

---

[106] Alexandre Sousa Pinheiro , *A COVID-19 e a proteção de dados pessoais, in Observatório Almedina – de especialistas para especialistas* - https://observatorio.almedina.net/index.php/2020/04/28/a-covid-19-e-a-protecao-de-dados-pessoais/

[107] Idem.

[108] Alexandre Sousa Pinheiro , *A COVID-19 e a proteção de dados pessoais, in Observatório Almedina – de especialistas para especialistas* - https://observatorio.almedina.net/index.php/2020/04/28/a-covid-19-e-a-protecao-de-dados-pessoais/

[109] Idem.

3.3.1. A aplicação StayAway Covid

Em Portugal, foi desenvolvida a aplicação *"contact tracing"* (sistema digital de rastreio de proximidade) denominada de 'StayAway Covid'.

Esta aplicação foi desenvolvida pelo INESC TEC (Instituto de Engenharia de Sistemas e Computadores) em parceria com o ISPUP (Instituto de Saúde Pública da Universidade do Porto) com a finalidade de detetar e alertar as pessoas quando estivessem em contacto com infetados e, consequentemente, monitorizar e combater o contágio do Covid- 19.

Apesar de esta aplicação ter como fundamento último o combate mais eficaz e rápido ao Covid- 19, o facto é que, não foi muito bem recebida pela maioria dos portugueses. *Alguns* portugueses defendiam a tese de que, os seus dados pessoais iam ser utilizados para outras finalidades, que não, o combate ao Covid-19, e *outros*, apontavam anomalias à *app* que a tornavam ineficaz e pouco segura. [110]

A acrescer a isso, o lançamento oficial da *app* a 1 de setembro de 2020 originou ainda mais polémica, quando o Primeiro-Ministro António Costa afirmou que o uso da aplicação era um "dever-cívico", propondo que o seu uso fosse obrigatório e prevendo multas até 500 euros para quem não procedesse à sua instalação[111], apesar de, a própria CNPD na Deliberação/2020/277, em junho de 2020, já ter dado o seu parecer prévio: *"29. Com a evolução da pandemia do vírus SARS-CoV-2, multiplicaram-se no mundo as soluções tecnológicas, em particular associadas à localização das pessoas como forma de identificar e reduzir a disseminação do contágio, o que suscitou desde logo um grande leque de preocupações do ponto de vista da proteção de dados e da privacidade, por porem em causa direitos fundamentais, havendo ainda afetação de outros direitos fundamentais, como sejam o direito de não discriminação, o direito de circular anonimamente, o direito de reunião."*

---

[110] "*A D3 recorda ainda o episódio da falha de segurança grave nos equipamentos Android, que permitia o acesso indevido a dados pessoais dos utilizadores. Uma vulnerabilidade descoberta no final de abril e que esteve ativa ao longo de quase todo o ciclo de vida da app (...)" in "Stayaway Covid: um ano depois a app de contacto está "morta". Mas de quem é a culpa?"* https://tek.sapo.pt/mobile/apps/artigos/stayaway-covid-um-ano-depois-a-app-de-contacto-esta-morta-mas-de-quem-e-a-culpa

[111] "*Uma das "facadas" na aplicação foi quando António Costa colocou na mesa o seu uso obrigatório durante o estado de calamidade, propondo depois multas até 500 euros para quem não a utilizasse, mesmo depois afirmasse que "ninguém iris fazer revistas" para confirmar quem a tinha instalado. A iniciativa fez estalar o verniz com reações negativas, acusações de ser inconstitucional, antiética e antidemocrárica, não demorando muitos dias para que o Primeiro-Ministro recuasse nas decisões de a tornar obrigatória"" in "Stayaway Covid: um ano depois a app de contacto está "morta". Mas de quem é a culpa?"* https://tek.sapo.pt/mobile/apps/artigos/stayaway-covid-um-ano-depois-a-app-de-contacto-esta-morta-mas-de-quem-e-a-culpa

; *"30. Sem dúvida que a adoção de medidas que, independentemente da sua conceção técnica, representam sempre um risco de rastreamento da localização e movimentação dos cidadãos, não devem ter um carácter obrigatório, imposto pelas autoridades públicas, porque claramente violadoras do princípio da proporcionalidade num Estado de Direito Democrático. Mesmo estando em causa uma situação excecional de emergência de saúde pública, a imposição de tal tipo de controlo- como se de uma panaceia se tratasse- não cumpriria os princípios da adequação, necessidade e proporcionalidade".*

Pelo exposto, a aplicação *Stayaway Covid*, apesar de prometer uma relevante contribuição para a monitorização e combate ao Covid- 19, facto é que, não registou uma adesão adequada[112], era demasiado complexa, não era acessível à maioria da população[113] (a mais empobrecida, envelhecida, pouco instruída tecnologicamente) e, apresentava riscos para a proteção dos dados pessoais dos seus titulares (nos dispositivos Android). Ora, apesar de bem-intencionada, não resultou em Portugal, ao contrário das aplicações de combate à Pandemia, utilizadas e bem-sucedidas, na Alemanha e Suíça.[114]

[112] Para que fosse eficaz no rastreio dos contágios, a *app* tinha de ser instalada por 60% dos utilizadores. – *in "Proteção de Dados em tempos de Covid-19- Breves Reflexões"* https://www.e-publica.pt/volumes/v7n1a09.html

[113] "(…) *Importa ainda assinalar a delimitação da imposição daquela obrigação apenas às pessoas que sejam possuidoras de equipamento que permita cumprir essa obrigação. Ainda que, por hipótese absurda, se tivesse como adequada e necessária uma tal imposição, e meso considerando que uma obrigação não deva ser importa a quem não tem meios para a cumprir, não pode deixar de se sublinhar que infligir uma restrição a direitos, liberdades e garantias com este grau de impacto apenas a alguns cidadãos traduz uma restrição desigual e discriminatória" – in* Parecer/2020/129 da CNPD, ponto 2.3, pág. 14.

[114] https://eco.sapo.pt/2021/05/12/governo-admite-que-app-stayaway-covid-nao-funcionou/

Conclusão

Após a análise/ leitura da presente dissertação é passível de se concluir que, Privacidade e a Proteção de Dados, estão intimamente ligados, mas têm objetos jurídicos diferentes.

A *Privacidade* é, um direito fundamental e de personalidade (*direito à reserva sobre a intimidade da vida privada)* cuja origem remonta ao ano 1890 com a publicação do artigo por Samuel D. Warren e Louis D. Brandeis nos EUA, ao direito à não ingerência, direito a não ser incomodado, mas que, devido aos avanços científicos e tecnológicos tornou-se mais estruturado para precaver violações, dado que os riscos foram cada vez sendo mais exponenciados. Atualmente, encontra-se consagrado a nível internacional, europeu e internacional.

A *Proteção de Dados* é, um direito fundamental, mais abrangente que o direito de privacidade, que confere direitos aos titulares dos dados pessoais contra ingerências do Estado e de terceiros nos seus dados pessoais.

O Direito à Proteção de Dados, tal como o direito à privacidade, tem sido aperfeiçoado à medida que o tempo passa e que as necessidades legislativas vão surgindo. A partir do ano 1980, iniciou a sua fase de consolidação na Europa (*Governing The Protection Privacy and Transborder Flows as Personal Data; Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal – Convenção 108)* e atualmente, desde 2016, encontra-se uniformizado na União Europeia pelo *Regulamento Geral de Proteção de Dados.*

O *Regulamento Geral de Proteção de Dados* (2016), atento à rápida evolução tecnológica e a globalização, que gerou novos desafios em matéria de proteção de dados pessoais, mais concretamente, a recolha, partilha, tratamento e utilização (por entidades públicas e privadas) de dados pessoais sem qualquer tipo de fronteiras (global), encetou um reforço quanto à sua proteção e promoveu a livre circulação dos dados.

Para tanto, o RGPD determinou o *consentimento (livre e esclarecido) como requisito de legalidade do tratamento;* elencou diversos *princípios para o tratamento de dados (*licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade, confidencialidade, responsabilidade*)* para a realização do tratamento pelo responsável pelo tratamento dos dados; definiu o *âmbito de*

*aplicação material (*tratamento de dados realizado por meios automatizados, não automatizados ; delimitou *o âmbito de aplicação territorial* (critério do estabelecimento); consagrou vários *direitos dos titulares de dados* (acesso, limitação do tratamento, portabilidade, oposição, retificação, apagamento/esquecimento); concebeu as figuras do *responsável pelo tratamento* (entidade pública ou privada/ conjuntos), *do subcontratante; e* estabeleceu *Autoridades de Controlo* (nacional e europeia).

O RGPD de carácter geral, obrigatório em todos os seus elementos, diretamente aplicável (art. 288º do TFUE), contém várias cláusulas de abertura, ou seja, normas que atribuem competências legislativas ou de outras índoles aos Estados-Membros e à própria União, impondo ou permitindo que estes apliquem medidas concretizadoras, complementares ou modificativas dos próprios regulamentos.

Ora, é nesta senda, que urge a Lei de Execução do Regulamento, aplicada a todos os tratamentos de dados realizados em território nacional, independentemente da natureza privada ou pública do responsável pelo tratamento ou subcontratante, no âmbito de uma atividade com estabelecimento em território nacional, ou tratamentos que afetem titulares de dados, visando assegurar a execução do RGPD na ordem jurídica portuguesa, harmonizar a legislação nacional com as disposições já vigentes no RGPD, detalhar a regulamentação da proteção de dados em diferentes matérias, e prever outras. A qual, foi alvo de várias críticas por, não raras vezes, contrariar normas consagradas no RGPD e extravasar a discricionariedade conferida pelo RGPD, apresentar uma ausência de rigor técnico nos conceitos utilizados e previstos no RGPD, ou seja, por estar ferida de várias incongruências e insuficiências.

Por último, a Pandemia provocada pelo Covid-19, veio levantar várias questões quanto à aplicação do direito da proteção de dados, principalmente, no âmbito de dados sensíveis - o direito à saúde (artigo 4º, nº 15 do RGPD), pois, foram sendo encetadas várias medidas preventivas de combate à proliferação do vírus Covid-19, dentro das quais, aplicações de "*Contact Tracing"* que visavam detetar e monitorizar os contactos efetuados por uma pessoa infetada e assim, contribuir de forma significativa para o combate e monotorização da pandemia. Portugal não ficou aquém, desenvolveu a aplicação "StayAway Covid", esta ferida de várias anomalias, risco na proteção dos dados pessoais dos seus utilizadores, discriminatória (a maioria da população portuguesa é envelhecida) e assim, malograda.

Concisamente, o direito à privacidade e o direito à proteção de dados apresentam-se, hoje, mais coerentes e abrangentes, em muito devido ao RGPD. Todavia, tratando-se de direitos fundamentais, estão sempre carecidos de uma atenção redobrada, principalmente, nas crises de saúde pública em que são admissíveis restrições aos direitos dos titulares dos dados, e que, evidentemente, requerem a averiguação *in concreto* da proporcionalidade destas.

Bibliografia

- REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados);
- MENEZES CORDEIRO, ANTÓNIO (2020). Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019.
- PINHEIRO, ALEXANDRE SOUSA. A COVID-19 e a proteção de dados pessoais. Observatório Almedina: *https://observatorio.almedina.net/index.php/2020/04/28/a-covid-19-e-a-protecao-de-dados-pessoais/*.
- PARECER/2020/129 da CNPD.
- NUNES, FLÁVIO. "Governo admite que a app StayAway Covid não funcionou em Portugal" (12 maio 2021): https://eco.sapo.pt/2021/05/12/governo-admite-que-app-stayaway-covid-nao-funcionou/.
- PINHEIRO, ALEXANDRE SOUSA, em entrevista a ADVOCATUS by ECO a 11 de Set. 2019: Alexandre Sousa Pinheiro Antecipa Conferência "Nova Lei de Proteção de Dados" – ECO (sapo.pt).
- PARREIRA, RUI. "Stayaway Covid: um ano depois a app de contacto está "morta". Mas de quem é a culpa?" *https://tek.sapo.pt/mobile/apps/artigos/stayaway-covid-um-ano-depois-a-app-de-contacto-esta-morta-mas-de-quem-e-a-culpa.*
- MOTA, JOANA; SAMPAIO, ALEXANDRE PEDRAL. "Regulamento Geral de Proteção de Dados em Portugal – Alguns apontamentos à sua Lei de Execução", pág. 6, https://www.uria.com/documentos/publicaciones/6855/documento/port01.pdf?id=9341.
- DELIBERAÇÃO/2019/494 da Comissão Nacional de Proteção de Dados, aprovada a 3 de setembro de 2019.
- EGÍDIO, MARIANA MELO. "Proteção de Dados em tempos de Covid-19- Breves Reflexões" https://www.e-publica.pt/volumes/v7n1a09.html
- Carta dos Direitos Fundamentais da União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR

- REIS, DANIEL; COSTA, RITA DE SOUSA. Tecnologia e Privacidade, " Os 12 pontos fundamentais da lei nacional que assegura a execução do RGPD" - https://www.plmj.com/xms/files/03_Novidades_legislativas/2019/008_agosto/NL_Os_12_pontos_fundamentais_da_lei_nacional_que_assegura_a_execucao_do_....pdf
- DIAS, PATRÍCIA CARDOSO; "Proteção de dados pessoais no contexto da pandemia provocada pelo novo coronavírus SARS-COV-2: aspetos ético-jurídicos relevantes da proteção de dados de saúde no âmbito da emergência de saúde pública", Revista Julgar Online, Janeiro de 2021.
- "A proteção de Dados na UE" : https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt.
- "Princípios do tratamento de dados": www.uc.pt/protecao-de-dados/conceitos_basicos/principios_do_tratamento_de_dados.
- FLEISCHER, PETER. Foggy thinking about the Right to Oblivion,, http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html.
- DIRETIVA 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
- DIRETRIZES 3/2018 SOBRE O ÂMBITO DE APLICAÇÃO TERRITORIAL DO RGPD de 12 de Novembro de 2019: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf
- GT 29, WP169 — Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante», adotado em 16 de fevereiro de 2010 e em revisão pelo CEPD.
- DE OLIVEIRA, ANA PERESTRELO (2019). Direito ao apagamento dos dados ou direito a ser esquecido. Fintech II- Novos Estudos sobre Tecnologia Financeira.
- GT 29, Orientações sobre o direito à portabilidade dos dados (WP 242 ver. 01), 13 – dez.- 2016.
- DIAS PEREIRA, ALEXANDRE. Big Data, E-Health e «Autodeterminação Informativa». A Lei 67/98, a Jurisprudência e o Regulamento 2016/679. Lex

Medicinae- Revista Portuguesa de Direito da Saúde- Ano 15- nº29- janeiro/ junho 2018. Instituto Jurídico/ Faculdade de Direito da Universidade de Coimbra.

- DIAS PEREIRA, ALEXANDRE. O responsável pelo tratamento de dados segundo o regulamento Geral de Proteção de Dados. Coimbra, 2019.
- SOARES FARINHO, DOMINGOS. Intimidade da vida privada e media no ciberespaço. Coimbra, Almedina, 2006.
- SAWARIS, ADRIANA. A tutela do direito à reserva sobre a intimidade da vida privada no regulamento no. 2016/679 da União Europeia, Dissertação apresentada à FDUC, junho de 2017.
- ZANINI, LEONARDO ESTEVAM DE ASSIS. O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. Revista de Doutrina da 4.ª Região, Porto Alegre, n.64, fev. 2015 http://www.revistadoutrina.trf4.jus.br/artigos/edicao064/Leonardo_Zanini.html.
- GARRIGA DOMINGUES, ANA. Nuevos retos para la proteccion de datos personales: en la era del big data y de la computacion ubicua. Madrid, Dykinson, 2015.
- MOTA PINTO, PAULO. O direito à Reserva sobre a Intimidade da Vida Privada, Boletim da FDUC LVIX (1993).

Jurisprudência

- Acórdão do TJUE, no Processo C-507/17, de 24 de Setembro;
- Acórdão do TJUE, no Processo C-136/17, de 24 de setembro de 2019;
- Acórdão do TJUE, no Processo C-398/15, de 9 de março de 2017;
- Acórdão do TJUE, no Processo C-131/12, de 13 de maio de 2014;
- Acórdão do TJUE, no Processo C-73/07, de 16 de dezembro de 2008;
- Acórdão do TJUE, no Processo C-101/01, de 6 de novembro de 2003.