UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

A PROTEÇÃO DE DADOS E OS MECANISMOS DE GEOLOCALIZAÇÃO

Mara Érica Rupia Lopes

MESTRADO EM CIÊNCIAS JURÍDICO-FORENSES

DISSERTAÇÃO ORIENTADA PELO PROFESSOR DOUTOR ALEXANDRE SOUSA PINHEIRO

Lisboa

2018

Ao António, à Josefa, à Mónica e à Miriam.

Ao Rui.

Ao Nuno e à Carla.

RESUMO

Através do presente trabalho, correspondente à dissertação a ser apresentada no âmbito do Mestrado, temos o propósito de debater a proteção da privacidade e dos dados pessoais, especialmente no que se refere aos dados de localização tratados no âmbito das comunicações eletrónicas.

Procurámos analisar o quadro regulatório existente, dando especial foco à legislação comunitária e portuguesa. Portanto, a investigação inicia-se com uma contextualização acerca da sociedade da informação, internet, privacidade e dados pessoais. Procedemos a uma excursão sobre a evolução histórica dos mais relevantes sistemas de proteção de dados, que culminaram nos principais diplomas atualmente vigentes em matérias de proteção de dados e a privacidade.

Ainda no que se refere ao regime geral da proteção de dados, destaca-se a importância da autodeterminação informacional e o contributo prestado pelo *Datenschutz* alemã.

Toda a informação é valiosa, mas esta informação será muito mais valiosa na medida em que tiver o devido enquadramento geográfico. Nesse sentido, existem cada vez mais serviços assentes no tratamento de dados de localização. Tais serviços incluem serviços de cartografia e navegação, os serviços geopersonalizados (inclusive os que indicam pontos de interesse nas proximidades), os serviços de realidade aumentada, a geomarcação de conteúdos na Internet, o controlo de crianças e a publicidade baseada na localização. É a crescente evolução tecnológica e a cada vez maior massificação da utilização de dispositivos móveis inteligentes que estimulam o surgimento desta nova categoria de serviços assentes na localização e vem motivar a análise específica conduzida no presente trabalho sobre o tema.

Entrando no tema específico deste trabalho, analisamos os principais mecanismos de geolocalização e a legislação aplicável. Notamos que não serão abordados determinados serviços assentes no tratamento de dados de localização, tais como sejam as questões específicas de geolocalização no contexto laboral, a geomarcação

associadas à chamada Web 2.0 e outras tecnologias de geolocalização utilizadas para interligar dispositivos em zonas reduzidas.

Palavras-chave: Proteção de dados, direitos fundamentais, dados de localização, comunicações eletrónicas.

ABSTRACT

Through the present work, corresponding to the dissertation to be presented in the scope of the Law Master, we have the purpose of discussing the protection of privacy and personal data, especially with regard to the location data processed in the scope of electronic communications.

We have sought to analyze the existing regulatory framework, with special focus on Community and Portuguese legislation. Therefore, the investigation begins with a contextualization about the information society, internet, privacy and personal data. We toured the historical evolution of the main data protection systems, which culminated in the main diplomas currently in force in matters of data protection and privacy.

Also with regard to the general data protection regime, the importance of informational self-determination and the contribution made by the German *Datenschutz* stands out.

All information is valuable, but all information can be of a much higher value as long as it has the proper geographical setting. In this sense, there are more services based on the handling of location data each day. Such services include mapping and navigation services, geo-personalized services (including those indicating nearby points of interest), augmented reality services, geotagging of Internet content, child control and location-based advertising. It is the growing technological evolution and the increased massification of the use of intelligent mobile devices that stimulate the emergence of this new category of services based on location and motivate the specific analysis conducted in the present work on the subject.

Entering the specific theme of this work, we analyze the main geolocation mechanisms and the legislation applicable to them. We note that certain services based on the handling of location data, such as geolocation-specific issues in the workplace, geolocation associated with the so-called Web 2.0, and other geolocation technologies used to interconnect devices in confined areas will not be addressed.

Key words: Data protection, fundamental rights, location data, electronic communications.

SIGLAS E ABREVIATURAS

Autoridade Nacional De Comunicações – Anacom

Bundesgerichtshofs (Supremo Tribunal Federal Alemão) – BGH

Carta Dos Direitos Fundamentais Da União Europeia – CDFUE

Comissão Nacional De Proteção De Dados – CNPD

Comunidade Económica Europeia – CEE

Constituição Da República Portuguesa – CRP

Convenção Europeia Dos Direitos Do Homem – CEDH

Declaração Universal Dos Direitos Do Homem – DUDH

Diário Da República – DR

Espaço Económico Europeu – EEE

Estados Unidos Da América – EUA

Grundgesetz (Constituição da República Federal da Alemanha de 1949) – GG

Global Positioning System – GPS

Global System for Mobile Communications (Sistema Global para Comunicações Móveis) – GPS

Internet Service Provider – ISP

Medium Access Control (Controlo de Acesso ao Meio) – MAC

Número – N.º

Organização Das Nações Unidas – ONU

Página – P.

Páginas – Pp.

Radio Frequency Identification – RFID

Regulamento Geral da Proteção de Dados – RGPD

Seguintes – ss.

Tratado Sobre o Funcionamento da União Europeia – TFUE

Tratado da União Europeia – TUE

Tribunal De Justiça Da União Europeia – TJUE

Tribunal Europeu Dos Direitos Do Homem – TEDH

União Europeia – UE

ÍNDICE

PRIVACY 11

"**The Right to Privacy**", de Samuel Warren e Louis Brandeis 11

DATENSCHUTZ 19

O impacto da Jurisprudência 21

A EVOLUÇÃO DA PROTEÇÃO DE DADOS NO DIREITO INTERNACIONAL 36

ONU 36

CONSELHO DA EUROPA 37

A proteção de dados na jurisprudência do TEDH 40

UNIÃO EUROPEIA 41

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 41

Outros instrumentos 50

A Carta dos Direitos Fundamentais da União Europeia e o Tratado de Lisboa 51

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 53

A EXPERIÊNCIA PORTUGUESA EM PROTEÇÃO DE DADOS 79

A EVOLUÇÃO: DA CONSTITUIÇÃO DE 1976 AOS DIAS DE HOJE 79

A LEI N.º 67/98, DE 26 DE OUTUBRO 83

OS MECANISMOS DE GEOLOCALIZAÇÃO 89

DADOS DAS ESTAÇÕES DE BASE 90

TECNOLOGIA GPS 91

PONTOS DE ACESSO WIFI 91

A GEOLOCALIZAÇÃO NO RGPD E NA DIRETIVA PRIVACIDADE E COMUNICAÇÕES ELETRÓNICAS 92

Tratamento realizado por operadores de telecomunicações 93

Tratamento realizado por fornecedores de serviços da sociedade da informação 94

A GEOLOCALIZAÇÃO NO ÂMBITO DA LEGISLAÇÃO PORTUGUESA 97

Tratamento realizado por operadores de telecomunicações 98

O CASO ESPECÍFICO DOS CARROS VEÍCULOS SEM CONDUTOR E DOS VEÍCULOS CONECTADOS 100

CONCLUSÕES 105

INTRODUÇÃO

A sociedade atual vive em constante mudança, fruto dos avanços da tecnologia, que moldam a forma como comunicação e partilhamos: partilhamos cada vez mais, através de mais plataformas e mais meios de comunicação. É nesse contexto de partilha de informação que a proteção de dados surge como direito incontornável e inalienável, que permite ao indivíduo controlar a partilha de informação que lhe diz respeito, limitando o seu âmbito e o objeto.

Nesta sociedade de informação, é comummente reconhecido que a informação vale ouro, pelo que se impunha o estabelecimento de regras que protegessem os dados pessoais, incluindo dos dados de localização pois, com a rápida evolução tecnológica e a cada vez maior massificação da utilização de dispositivos móveis inteligentes, surge uma nova categoria de serviços assentes na localização. Tais serviços incluem serviços de cartografia e navegação, os serviços geopersonalizados (inclusive os que indicam pontos de interesse nas proximidades), os serviços de realidade aumentada, a geomarcação de conteúdos na Internet, o controlo de crianças e a publicidade baseada na localização.

O objetivo da presente dissertação consiste em clarificar o quadro jurídico aplicável à proteção de dados e em concreto aos serviços de geolocalização, com limitação aos serviços de localização disponíveis através da utilização de dispositivos móveis inteligentes. Note-se, desde já, que o referido quadro jurídico, além de revestir especial complexidade, foi alvo de alterações significativas e que impõem a necessidade de estudo aprofundado. Adicionalmente, a matéria da proteção de dados apresenta uma natureza interdisciplinar, conjugando as disciplinas do Direito e das Tecnologias da Informação, e outros saberes tais como a Ética ou as Ciências Sociais. Mais, a sua natureza interdisciplinar tem reflexo na sua incidência transversal ao ser aplicável aos diversos sectores da economia. Por outro lado, a proteção de dados, também em resultado da sua interdisciplinaridade, obriga à sua emancipação das restantes disciplinas tradicionais, que embora úteis para a análise, ficam aquém na resolução das questões colocadas.

Nesse sentido, o presente trabalho começa por descrever a evolução história da proteção de dados, deste a *privacy* e da *Datenschutz* ao atual panorama regulatório vigente, quer no direito internacional quer na legislação portuguesa. Em seguida, iremos identificar e analisar o quadro regulatório aplicável à proteção de dados, apresentando conclusões respeitantes à aplicação das disposições legais pertinentes. Por último, concluímos com a análise da regulação específica da geolocalização, tanto no direito comunitário como no direito português.

Em conformidade com o âmbito do presente trabalho, não iremos analisar algumas questões específicas de geolocalização no contexto laboral. Ficará também de fora a geomarcação associadas à chamada Web 2.0, mediante as quais os utilizadores integram informações georreferenciadas em redes sociais. Também não iremos analisar em pormenor outras tecnologias de geolocalização utilizadas para interligar dispositivos numa zona relativamente pequena (centros comerciais, aeroportos, edifícios de escritórios, etc.), nomeadamente etiquetas RFID assentes nas tecnologias Bluetooth, ZigBee, geodelimitação e WiFi.

A EVOLUÇÃO DA PROTEÇÃO DE DADOS

Quando se fala na evolução da proteção de dados, devemos destacar dois paradigmas distintos que irão dar origem às duas grandes correntes relativas a este tema: a *privacy*[1] nos Estados Unidos da América, que posteriormente difundiu--se para os países que adotam o sistema da *common law;* e a *Datenschutz* na Alemanha, que vai evoluir e conformar o paradigma europeu. Importa então destacar os recortes principais destes dois modelos.

PRIVACY

"**The Right to Privacy**", de Samuel Warren e Louis Brandeis

À *privacy* norte-americana pode ser atribuído um texto fundador: o artigo "the Right to Privacy", de Samuel Warren e Louis Brandeis[2]. Este artigo surge no contexto dos Estados Unidos da América de finais do século XIX, no qual já eram visíveis os avanços da tecnologia, e as consequentes massificação, explosão demográfica e mutação de valores, que daqueles resultavam. Foi em relação a um destes avanços, o da imprensa escrita, que nascem os primeiros desejos pela *privacy*: as classes médias e altas procuravam proteger-se da exposição e da publicidade que evoluíam a par do desenvolvimento da imprensa escrita e

---

[1] O vocábulo inglês originalmente utilizado era "*privace"* e originou no século XV, decorrente do latim "*privates*" que significa separado do resto. A significação original não tem correspondência no atual conceito de *privacy,* conforme melhor explicado adiante. WEBB, Diana – ***"Privacy and Solitude"***. Londres/Nova Iorque: Hambledon Continuum, 2007, pp. XVI-XVII.
É importante observar que o termo inglês "privacy" não pode nem deve ser confundido com a expressão "privacidade" da língua portuguesa. De fato, resulta do artigo de Warren e Brandeis e das primeiras decisões sobre a matéria que a *privacy* assumiu, desde o início, vocação para ampla tutela dos valores da personalidade, não se limitando apenas à tutela da privacidade. Nesse sentido, FESTAS, David de Oliveira – ***Do conteúdo patrimonial do direito à imagem***. Coimbra: Coimbra Editora, 2009, p. 32). Desse modo, considerando a dificuldade na tradução do termo, que não se confunde com a privacidade e nem com os direitos da personalidade, preferimos utilizar nesse trabalho, para não incorrermos em nenhuma imprecisão, a expressão em inglês. WARREN, Samuel D. e Brandeis, Louis D. - ***The Right to Privacy***, in Harvard Law Review, Volume IV, n. º 15, 15 de dezembro de 1890. p. 11.
[2] WARREN, Samuel D. e BRANDEIS, Louis D, op. cit.

desencadeia-se uma discussão entre a liberdade de imprensa e o pretenso direito à proteção da vida privada[3], alicerçada na *privacy.*[4]

É de salientar que ainda antes do artigo de Warren e Brandeis[5], a ideia de *privacy* já estava presente no sistema jurídico dos Estados Unidos[6], tendo inclusive o *Supreme Court* se pronunciado sobre o *right to be let alone*[7] *(direito a ser deixado sozinho)*. No entanto, o conceito de *privacy* e o respectivo *right to privacy* não chegaram a receber o reconhecimento formal da comunidade jurídica como um direito, o que somente veio a verificar-se com a publicação do artigo de Warren e Brandeis[8][9].

No seu artigo, Warren e Brandeis, colocam em evidência a ocorrência de diversas transformações a nível social, político e económico, que, conjugadas com o

---

[3] O *Supreme Court* analisou a compatibilidade entre a primeira emenda e a *privacy*, nos casos *Paker Corporation v. Utah* (1932) e *Kovacs v. Cooper* (1949).Estes casos estão disponíveis para consulta em https://supreme.justia.com/cases/federal/us/285/105/ (17.03.2018) e https://supreme.justia.com/cases/federal/us/336/77/case.html (17.03.2018).

[4] Sobre o assunto, ver SOLOVE, Daniel J. e SCHWARTZ, Paul M. – ***Privacy and the Media***. Austin, Boston, Chicago e Nova Iorque: Wolters Kluwer, 2008.

[5] Em Julho de 1890, e antecedendo o artigo de Warren e Brandeis, o advogado e jornalista Edward Lawrence Gorkin publicou um artigo seu na Scribner's Magazine, subordinado ao título "***Rights of the Citizen – IV – To his own reputation***", no qual aborda os perigos da imprensa que vinha corroendo a privacidade da sociedade em geral, e em especial da "aristocracia social", utilizando já o conceito de "right to privacy", o qual se assumia como um "direito natural".

[6] A ideia de privacy começa a aflorar em 1669 e 1776, com a Constituição de Locke para a Carolina do Norte e no *Bill of Rights*, respetivamente, através de menções aos direitos privados de personalidade.

[7] No século XIX é possível reconher uma primeira manifestação do direito individual de "*ser deixado só*" no caso *Wheaton v. Peters (1834)*, decidido pelo *Supreme Court.* A decisão está disponível para consulta em http://www.bc.edu/bc_org/avp/cas/comm/free_speech/wheaton.html (17.03.2018). Este direito também foi abordado na obra do juiz Thomas Cooley, publicada em 1880, sob o título "***A Treatise on the Law of Torts"***. Ainda que o trabalho fosse sobre responsabilidade civil (*torts*), pode ler-se na obra o seguinte trecho: "*The right to one's person may be said to be a right of complete immunity: to be let alone*".

[8] Apesar de muitos estudiosos admitirem na *common law* o reconhecimento jurisprudencial do right of privacy antes do artigo de Warren e Brandeis, a matéria não é, contudo, isenta de discussões. De facto, um grupo considerável de estudiosos vê nos casos apontados pelo artigo de Warren e Brandeis como casos de reconhecimento da *privacy* apenas por referência à aplicação de outros institutos, tais como o direito de propriedade, a violação de contrato, a violação de confiança ou mesmo a ocorrência de difamação, sendo que a eventual proteção da privacy, a existir, é apenas incidental. Afirma-se ainda que os argumentos utilizados por Warren e Brandeis para a construção do *privacy* partiram da errônea compreensão dos precedentes examinados. Nesse sentido, ver FESTAS, David de Oliveira, op. cit., p. 156-157.

[9] PRATT, Walter F.- ***Privacy in Britain***. Londres: Bucknell University press, 1979, p.37, do qual se retira o seguinte trecho "*Warren and Braindeis want a right that would prevent the publication of a picture of anyone without the consent of that person or of an article about Warren's entertaining guests (…). In the areas of the Law discussed by Warren and Brandeis there were no precedent for a right to privacy*".

surgimento de novas invenções, com especial relevância para a fotografia[10], contribuíram para o surgimento de violações da privacidade dos indivíduos[11]. Estas violações à privacidade foram assumidas pelos autores simultaneamente como ponto de partida e ao mesmo tempo como pressuposto para o seu artigo, deduzindo então a existência de um princípio geral na *common law*, o *right of privacy*. Utilizando o conceito do "*right to be let alone*", Warren e Brandeis propõem um novo "tort", ou seja, um novo ilícito civil, que seria a invasão do "privacy" e que constituiria uma ofensa à própria pessoa, sobre sua independência, individualidade, dignidade e honra[12].

Para os autores, o *right to privacy*, apesar de resultar da *common law*, não estava nela especialmente previsto[13] mas era sim uma consequência de diversos *torts* que funcionavam para a proteger. Fazendo uma distinção clara entre o *right to property* e o *right to privacy*, Warren e Brandeis defendem a autonomia própria do *tort* do *right to privacy* e dos *remedies* que podiam ser aplicados para a sua tutela. Este direito, fundamentado no direito à vida, expressamente enunciado na Declaração de Independência dos Estados Unidos e formalmente reconhecido pela quinta emenda da Constituição, visa conferir ao indivíduo uma garantiria contra intromissões não desejadas na sua vida privado, tutelando seus pensamentos, sentimentos, emoções, dados pessoais e o nome.

---

[10] A imagem também foi incluída no âmbito de proteção do *privacy*, destacando-se que os avanços da fotografia tornaram possível a captação de forma oculta dos traços pessoais, pelo que se fazia necessária a utilização da lei de *torts* diante dos riscos inerentes a este progresso.

[11] É em resultado destes avanços tecnológicos e das constantes violações que deles advinham que Warren e Brandeis consideraram o right to *privacy* uma necessidade de forma a garantir uma esfera privada do indivíduo que seria protegida do meio social: "*The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury*". WARREN e BRANDEIS – op. cit., p. 196.

[12] SOMA, John T – ***Privacy law***. St. Paul: Thomson/West, 2008, p. 11.

13 Os autores entendem que os princípios da *privacy* decorrem da *common law*, particularmente no que diz respeito à proteção do domicílio, sendo que o desenvolvimento tecnológico veio tornar necessário reconhecer expressa e separadamente esta proteção sob o nome de *privacy*.

As críticas a Warren e Brandeis

O artigo de Warren e Brandeis, ainda que tendo causado um impacto considerável no sistema jurídico norte-americano, não foi acolhido de forma imediata. De fato, num primeiro momento, verificou-se alguma hesitação por parte da doutrina quanto à *privacy* e ao seu fundamento: a doutrina dividiu-se entre aqueles que negaram energicamente as novas ideias de Warren e Brandeis e aqueles outros que defenderam o instituto com entusiasmo[14].

Nos tribunais, o efeito do artigo também não foi imediato, uma vez que os primeiros casos julgados após a sua publicação não reconheceram a existência da *privacy*.

O artigo também foi alvo de pesadas críticas, dentro das quais se podem assinalar as seguintes:

- Anita L. Allen e Erin Mack assinalaram que "The Right of Privacy" era um texto indiferente a questões de género, não tendo sido pensado numa estrutura de género[15].
- Diane L. Zimmerman[16] defendeu que o artigo de Warren e Brandeis era desadequado aos problemas da *privacy* existentes no contexto em que o artigo foi publicado, devido às dificuldades tanto de aplicação prática do *right to privacy* conforme ali delimitado como de compatibilização da criação de um ilícito que visasse proteger uma área privada da personalidade com a primeira emenda à Constituição.
- James H Barron censura o artigo de Warren e Brandeis por limitar a *privacy* à revelação de factos privados da vida do indivíduo, fazendo colidir este direito com as liberdades de expressão e de informar, reconhecidas pela primeira

[14] PROSSER, William Lloyd **– *Privacy*.** California Law Review, vol. 48, 1960.
[15]ALLEN, Anita L. e MACK, Erin **– How Privacy Got its Gende.** Northen Illinois Law Review, vol. 10, 1999-2000, p. 477.
[16] ZIMMERMAN, Diane L. **– Requiem to a Heavyweight: A Farewell to Warren and Brandeis**. Connecticut Law Review, vol. 68, 1982-83.

emenda, sem que os autores tivessem fornecido quaisquer critérios que permitissem harmonizar o *right to privacy* e a primeira emenda[17].

- A generalidade dos autores entendia que o artigo estava endereçado a um universo elitista de pessoas, às classes média e alta[18], ainda que não declarasse expressamente.

Contudo, a ideia foi aos poucos sendo adotada e até expandida pelos tribunais estaduais e federais, sendo ainda de ressalvar que, nas primeiras décadas de existência, o *right of privacy* foi defendido ao abrigo da *property theory*, sendo que apenas décadas depois passou a ser classificado como um direito pessoal autónomo[19].

Ainda assim, as maiores críticas ao artigo de Warren e Brandeis vieram de Prosser e Bloustein, que exerceram, como passaremos a explicitar, indiscutível influência nos desenvolvimentos posteriores da *privacy*[20].

William Prosser[21] apresentou em 1960 um estudo bastante preciso acerca das decisões proferidas sobre o *right of privacy*. Nele, Prosser procurou evidenciar as regras emanadas de cada caso e os desenvolvimentos jurídicos que decorriam daquelas decisões jurisprudenciais[22]. Após a análise do acervo jurisprudencial disponível, Prosser tentou sistematizar a matéria da *privacy*, face à confusão e inconsistências constatadas no desenvolvimento da *privacy*. Segundo Prosser, a *privacy* não se limitava a ser apenas um *tort*, mas sim quatro categorias diversas de *torts*, cada um deles correlacionado com a lesão de diferentes tipos de interesses protegidos[23]: 1) interesse na preservação do interesse do indivíduo quanto a

---

[17] BARRON, James H. **– Warren and Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890): Desmystifying a Landmark Citation.** Suffolk University Law Review, vol. XIII, 1979, p. 880 e 881, p. 214.

[18] Este entendimento é defendido por Alan Westin e Don R. Pember nas suas respetivas obras.
WESTIN, Alan, **– Privacy and Freedman**. Londres: The Bodley Head, 1970, p. 348.
PEMBER, Don R. **– Privacy and the Press. The Law, The Mass Media and the First Amendment.** Seatle/Londres: University of Washington Press, 1972, p. 23.

[19] FESTAS, David de Oliveira, op. cit., p. 164-165.

[20] DIONISOPOULOS, Allan e DUCAT, Craig R. **– The Right to Privacy, Essays and Cases**, p. 25-26.

[21] William Prosser foi um aclamado professor da California School of Law (Berkeley) e era uma das maiores autoridades em responsabilidade civil (*tort law*) na época.

[22] PROSSER, William Lloyd, op. cit., p. 804.

[23] Note-se que Prosser não foi o primeiro a apresentar uma classificação do *right of privacy* em diferentes categorias. No entanto, o seu trabalho é tão mais relevante na medida em que não se limita a desenvolver uma classificação que impôs ordem e clareza à matéria, mas também por ter

intrusões alheias ("*intrusion upon the plaintiff's seclusion or solicitude, o rinto his private affairs*"); 2) interesse na não-publicação de factos privados não pretendidos pelo indivíduo ("*public disclosure of embarrassing private facts about the plaintiff*"); 3) interesse na não-divulgação de factos privados que possam criar uma imagem pública falsa ("*publicity in a false light in the public eye*"); 4) interesse na não-divulgação do nome ou imagem do indivíduo ("*appropriation for the defendant's advantage of the plaintiff's name or likeness*").

A sistematização de Prosser não foi isenta de críticas, tais como as perpetradas por Edward Bloustein[24], que defendia que a análise da *privacy* por categorias de violações, tais como apresentadas por Prosser, contrariava o que Warren e Brandeis defendiam, denotando ainda a incapacidade dos tribunais de continuarem o desenvolvimento da *privacy* sem que fosse necessário o apoio nas figuras jurídicas tradicionais, como o direito à propriedade e à honra[25]. Nessa linha, Bloustein destacou a existência de uma considerável confusão no que toca à natureza do bem jurídico protegido pela *privacy*, entendendo que Prosser remete esse direito novamente às antigas instituições jurídicas, contrariamente ao pensamento de Warren e Brandeis, que viam na *privacy* uma figura jurídica nova e unitária.

Partindo destas observações, Bloustein propõe uma teoria geral da *privacy*, tomando como pressuposto para tal o bem jurídico protegido em todas as categorias de lesões: a dignidade humana[26]. Segundo Bloustein, a dignidade humana seria o bem jurídico protegido pela *privacy*, e funcionaria simultaneamente como perspetiva unificadora do *right of privacy*, vínculo que Prosser não havia conseguido estabelecer. Bloustein acrescenta ainda que a *privacy* não está limitada à *common law*, mas abrange o direito como um todo, incluindo as disposições constitucionais e de direito processual penal[27]. Para comprovar tal afirmação, e a proteção do *right of privacy* de forma independente e

---

identificado o bem jurídico protegido em cada uma das hipóteses apresentadas. Sobre a matéria, conferir KAMLAH, Ruprecht **- Right of privacy**, 1969, p. 72.

[24] BLOUSTEIN, Edward J. **- Privacy as an aspect of human dignity: an answer to dean Prosser**. New York University Law Review, v. 32, 1964, pp. 962 e ss.

[25] KAMLAH, Ruprecht, op. cit., p. 73.

[26] BLOUSTEIN, op. cit., pp. 962 e ss.

[27] KAMLAH, Ruprecht, op. cit., p.74.

não somente limitada à proteção civil contra atos ilícitos, Bloustein alicerceia-se na existência de diversa legislação mais recente que regulava o uso de sistemas eletrónicos de vigilância ou que proibia a intercetação telefónica de conversas.

A decisão do *Supreme Court* no caso *Griswold v. Connecticut*

A discussão e correspondente divergência doutrinária e jurisprudencial arrastar-se-ão até à decisão do *Supreme Court* no caso *Griswold v. Connecticut (1965)*[28]. Nesta decisão, o *Supreme Court* procede ao desenvolvimento da complexidade na classificação da *privacy*, sendo que o papel de destaque recai sobre o Juiz Douglas que apresenta uma nova fundamentação para a existência da *privacy*: para o Juiz Douglas, nas garantias de direitos fundamentais reconhecidas pelas emendas à Constituição podem ser encontradas *zones of privacy,* através de processos de interpretação da 1.ª emenda (que reconhece a liberdade de expressão), da 3.ª emenda (relativa à restrição ao aquartelamento de soldados em casas particulares), da 4.ª emenda (que procede à proibição de busca e apreensões ilícitas), da 5.ª emenda (que reconhece o direito à não autoincriminação), da 9.ª emenda (que declara que os direitos não especificados na *Bill of Rights* também são por ela abrangidos e protegidos) e da 14.ª emenda (que reconhece o direito dos cidadãos a um *due process*)[29]. Assim sendo, apesar da *privacy* não estar expressamente prevista, ela decorre dos direitos reconhecidos pela Constituição e pelo Bill of Rights.

Ora, tal como tem vindo a ser evidenciado, esta não foi a primeira decisão do *Supreme Court* sobre questões relacionadas com a *privacy*, no entanto a inovação de *Griswold v. Connecticut (1965)* prende-se com a *decisional privacy* e com a classificação do *right to privacy* como um *fundamental right.*

[28] O caso está disponível em http://caselaw.findlaw.com/us-supreme-court/381/479.html.
Quanto aos factos subjacentes ao caso, a legislação do estado de Connecticut proibia o acesso e uso por parte de pessoas casadas a contracetivos e a informação sobre o controlo da natalidade. A discussão abordava a legitimidade do Governo invadir a esfera íntima e privada dos cidadãos casados, impondo restrições e condicionantes à sua vida sexual.
[29] RICHARDS, Neil M. **- Griswold v. Connecticut**, in Encyclopedia of Privacy, vol. I, p. 263

A doutrina procedia de forma recorrente à classificação da *privacy* entre *decisional privacy* e *informational privacy*. Por um lado, a *informational privacy* está vinculada à forma de tornar pública uma informação, determinando os casos em que a publicidade de determinados factos devesse depender do consentimento do titular da informação. Por outro lado, a *decisional privacy* refere-se a comportamentos do indivíduo, aos seus atos pessoais e sociais tomados de forma autónoma[30].

A decisão do Juiz Douglas não foi aceite de forma pacífica, recebendo votos desfavoráveis por parte de dois juízes e ainda declarações de voto de seis dos juízes que votaram favoravelmente[31]. Ainda assim, a partir da decisão *Griswold v. Connecticut (1965)*, a *privacy* como um direito fundamental vai ser desenvolvida e consolidada por diversas decisões do Supreme Court.

Apesar de não diretamente abordada na decisão *Griswold v. Connecticut (1965)*, a *informational privacy* viria a ser incluída na legislação, com especial relevância para a legislação aplicável ao crédito, à investigação criminal e à segurança nacional. De facto, foram posteriormente aprovados os seguintes diplomas:

- **Fair Credit Reporting Act (1971)** – este diploma visava regular as relações entre as instituições de financeiras ou comerciais e os consumidores, garantindo a estes últimos o direito a ser informado sobre a informação financeira contida no seu relatório de crédito e a impugnar a precisão dessa mesma informação[32].
- **Privacy Act (1974)** – este diploma tem por objetivo ser uma *privacy bill* e surge na sequência das interceções ilegais de comunicações praticadas no caso Watergate[33]. O seu âmbito não inclui o sector privado e não prevê a criação e

[30] PINHEIRO, Alexandre S., "Privacy e Protecção de Dados Pessoais: a Construção Dogmática do Direito à Identidade Informacional, Lisboa: AAFDL, 2015, pp. 365-366.
[31] Segundo Garrow, o projecto de decisão não foi bem acolhido pelos membros do Tribunal; GARROW,David J. – **Liberty and Sexuality. The Right to Privacy and making of Roe v. Wade**. Berkeley, Los Angeles e Londres: University of California Press, p. 249.
[32] National Consumer Law Center – **Fair Credit Reporting Act**, Connecticut: Grolier Educational Corporation, 1988, p.20.
[33] O caso Watergate foi um escândalo político ocorrido na década de 1970 nos Estados Unidos que, ao vir à tona, acabou por culminar com a renúncia do presidente Richard Nixon, eleito pelo Partido Republicano. Durante a campanha para a eleição de 1972, verificou-se uma invasão aos escritórios do Partido Democrata em Washington, no conjunto de edifícios Watergate. Esta invasão pretendia instalar aparelhos para a interceção de comunicações do Partido Democrático.

funcionamento de uma agência federal à qual ficassem incumbidos os assuntos da *informational privacy*[34].

DATENSCHUTZ

A par do desenvolvimento da *privacy* nos Estados Unidos, na Alemanha foi-se desenvolvendo a Datenschutz[35], tendo sido aprovada em 1970, pelo estado federal de Hessen, uma lei estadual pretendia ser de aplicação geral às operações informáticas exercidas sobre dados pessoais[36]. Tanto esta lei como o desenvolvimento da *Datenschutz* surge no contexto ***i)*** de um Estado Social que prestava bens e serviços, necessitando para tal de ter informação sobre a sua população, e ***ii)*** da existência de várias entidades do sector privado que detinham um vasto conjunto de informação. Estas novas realidades, aliadas à existência de tecnologia mais avançada que permitia receber, enviar e tratar grandes quantidades de informação de natureza variada, alertaram para a necessidade de regular e combater os abusos que daí podem advir[37].

---

[34] PINHEIRO, Alexandre S., op. cit. pp. 421 e ss.

[35] Segundo Sousa Pinheiro, a terminologia Datenschutz "*é efetivamente uma "palavra errada" para o que pretende abranger, porém, provavelmente, no léxico do início dos anos 70 do século passado "altura errada" era a que melhor se adequava a necessidade de equipar o Direito com instrumentos próprios de proteção relativamente aos "perigos da informática".* PINHEIRO, Alexandre Sousa – op. cit., p. 430.

Em comparação ao caso norte-americano, a Datenschutz corresponderia à *informational privacy*, "*embora o paralelo não possa ser aprofundado, tendo em conta a maior profusão de direitos associados à proteção de dados no caso europeu, relativamente aos aspetos informacionais da legislação americana, (…) razão que explica o facto de os Estados Unidos não serem considerados um país que garanta proteção adequada*". PINHEIRO, Alexandre Sousa – op. cit., p. 430.

[36] Para o autor Alexandre Sousa Pinheiro, a Lei de Hessen "*fixou dois aspetos originais que posteriormente transmigraram para a legislação federal, e vieram a ser recolhidos pela Diretiva n.º 95/46/CE, de 24 de outubro: a criação de entidades administrativas com competência para fiscalização em sede de proteção de dados, e o estabelecimento de que os tratamentos de dados pessoais dependiam essencialmente do consentimento ou de disposição legal*". PINHEIRO, Alexandre Sousa – op. cit., p. 556.

A Lei de Hessen tinha como aspetos fundamentais os seguintes: *"(i) aplicação a pessoas coletivas públicas; (ii) transferência de dados de modo a impedir a alteração ou destruição destes; (iii) inclusão do direito de correção dos titulares dos dados em casos de erro ou incompletude do registo; (iv) restabelecimento, sempre que possível, da situação anterior ao erro".* PINHEIRO, Alexandre Sousa – op. cit., p. 516.

Adicionalmente, esta lei procedeu à criação de um organismo de controlo, a Entidade de Inspeção de Dados (*Datainspektionen*), com competência para autorizar tratamentos de dados pessoais.

[37] PINHEIRO, Alexandre S., op. cit. p. 427.

"*[O] estado da doutrina germânica quer no que respeita aos direitos fundamentais, quer no que tange às teses sobre os direitos da personalidade (...) permitiram o rápido enquadramento dos novos desafios no contexto de uma sólida dogmática*"[38]. De facto, foram as construções doutrinárias originárias da criação e desenvolvimento dos direitos subjetivos, quando harmonizados com o "direito da personalidade" ou com o "direito geral da personalidade", que pavimentaram o percurso para o debate da *Datenschutz* no contexto da automatização por meio do recurso a máquinas, como proteção aos dados armazenados em sistemas informáticos.

Sousa Pinheiro refere ainda a relevância da jurisprudência francesa e da sua lei de 1868[39]. De facto, os bens protegidos em cada um dos ordenamentos eram essencialmente a "imagem" e, de modo mais genérico, os bens de personalidade.

A discussão subjacente à construção da *Datenschutz* foi essencialmente sobre a admissibilidade de ressarcir ofensas a bens da personalidade e sobre a existência de um "direito geral da personalidade". Aquando da discussão e elaboração da Lei Fundamental da República Federal da Alemanha de 1949, este assunto foi especialmente discutido, principalmente no que toca à articulação da interpretação do § 829.1 do *Bürgerliches Gesetzbuch* e do número 1 do artigo 2.º do texto constitucional[40] [41].

Quanto à admissibilidade dos "direitos de personalidade" ou de um "direito geral de personalidade", importa analisar brevemente a doutrina alemã estabelecida quanto à distinção entre entre *absolute Rechte* (*Herrschaftetsrechte*) e *relative Rechte* (*Anspriíche*). A construção subjacente ao direito subjetivo, de acordo com a

---

[38] Idem, op. cit. p. 428.
[39] Sobre o tema, o autor cita LINDON, Raymond – ***Une Création Prétorienne: Les droits de la Personnalité***", Paris: Dalloz, 1974.
[40] No número 1 do artigo 2.º da Lei Fundamental pode ler-se que "*[t]odos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral*".
Por outro lado, o artigo 829 do BGB dispõe que "*[u]ma pessoa que, pelas razões citadas nas seções 827 e 828, não seja responsável pelos danos por si causados às instâncias especificadas nas seções 823 a 826 deve, no entanto, compensar o dano, a menos que a compensação por danos possa ser obtida de um terceiro com um dever de supervisão, na medida em que nas circunstâncias, incluindo, sem limitação, as circunstâncias das partes envolvidas, o património requeira indenização e o sujeito não seja privado dos recursos necessários para uma manutenção razoável e para o cumprimento dos seus deveres legais de manutenção*".
[41] PINHEIRO, Alexandre S., op. cit. p. 433.

doutrina de Savigny, era um grande entrave à admissibilidade de direitos de personalidade ou de um direito geral de personalidade. Savigny baseava a sua dogmática sobre os direito subjetivo identificando três tipos de relações: "*as da pessoa (einege Person), as estabelecidas com a natureza (unfreie Natur) e as fundadas com outras pessoas (fremde Personen)"*[42]. Nesta medida, é compreensível que a doutrina de Savigny não admita um direito de personalidade no âmbito dos direitos subjetivos, pois os direitos subjetivos pressupõem uma relação de domínio da pessoa sobre um "objecto" (Rechtsobjekt) ou "bem jurídico" (Rechtsgut). Inerente ao direito subjetivo está a vontade humana e o poder de agir sobre o objeto, isto é, a "personalidade autónoma" do indivíduo[43]. Com estas premissas como base, afigura-se difícil configurar a proteção de um direito da pessoa sobre si mesma, sendo esta tanto titular do direito como objeto do próprio direito. Posteriormente, a construção de Savigny sobre os direitos subjetivos é abandonada porque não oferecia tutela suficiente e efetiva para proteger bens jurídicos até então sem qualquer relevância, mas que se viam ameaçados pela evolução tecnológica.

O impacto da Jurisprudência

O reconhecimento pelo direito alemão de "novos bens jurídicos" resulta também da atividade jurisprudencial na matéria, cujas principais decisões convém destacar, incluindo-se também, pela sua relevância, jurisprudência francesa[44].

Jurisprudência Francesa

- **Affaire "Mère Supérieure des Sœurs de la Providence" (1855) –** O *tribunal civil de La Seine* proibiu a exibição pública de um quadro com a representação da Madre Superior das Irmãs da Providência. A decisão fundou-

[42] VON SAVIGNY, Friedrich C. – **System des heutigen Römischen Rechts**, vol. I, Berlim, 1840, p. 338, *apud* PINHEIRO, Alexandre, op.cit. 434.
[43] PINHEIRO, Alexandre, op.cit. 434.
[44] Os percursores da *privacy* nos Estados Unidos, Warren e Brandeis referem o vanguardismo francês no seu artigo, fazendo referência à "*Loi Relative à la Presse*" e ao direito de privacidade que esta previa, de 11 de maio de 1868. WARREN, Samuel e BRANDEIS, Louis. op. cit., p. 214.

se na necessidade de proteção da vida privada (*vie privée*) daquela Madre Superior[45].

- **Affaire "Rachel" (1858) –** O *tribunal civil de La Seine* ordenou a cessação de publicações de imagens representativas (desenhos e pinturas) da atriz Rachel Félix no seu leito de morte. O processo foi despoletado pela irmã da atriz, sendo que o tribunal decretou o fim das publicações com fundamento na proteção e respeito pelo desgosto e pela dor da família[46]. Segundo Sousa Pinheiro, defende-se que este processo contém a primeira referência jurisprudencial ao "*droit à la vie privée"*[47].

Jurisprudência Alemã

- **Decisão "Graf Zeppelin" (1910) –** o *Reichsgerichts*, condenou uma empresa pela utilização da imagem de Graf Zeppelin a abdicar da marca. O facto de Zeppelin ter previamente autorizado a utilização da marca por outra empresa foi crucial para a fundamentação da decisão. A decisão não abordou a questão da indemnização a aplicar.
- **A decisão "Herrenreiter" (1958)[48] –** neste processo, o tribunal condenou o produtor de um fármaco considerado estimulante sexual que havia utilizado, sem autorização, a imagem de um cavaleiro, no exercício de atividade equestre, para promover o seu produto. O tribunal fundou a sua decisão na violação do direito pessoal à imagem, conjugado com uma situação de enriquecimento injusto, previso no § 812.° do BGB.

A discussão mais aprofundada deu-se em relação à admissibilidade de atribuição de uma indemnização pecuniária por uso não autorizado da imagem do cavaleiro. Para o BGHZ, a indemnização só poderia ser atribuída se à imagem correspondesse algum valor de mercado, pois deveria existir uma correspondência entre a indemnização e um hipotético consentimento para a

[45] BERTRAND, André — **Droit à la vie privée et droit à l'image**, Paris : Litec. 1999, p. 2, *apud* PINHEIRO, Alexandre, op.cit. 436.
[46] LINDON, op. cit., p. 11, *apud* PINHEIRO, Alexandre, op. cit. 436.
[47] BERTRAND, André, op. cit. p.2, *apud* PINHEIRO, Alexandre, op.cit. 436.
[48] Esta decisão foi preferida pelo BGHZ (26, 349) e está disponível e pode ser consultada em http://www.servat.unibe.ch/dfr/bz026349.html.

utilização da imagem. A indemnização apenas poderia ser atribuída se fosse possível ficcionar o consentimento da pessoa visada. Caso não fosse possível criar um cenário hipotético em que a pessoa teria consentido na utilização da imagem, não há lugar à indemnização.

- **A decisão Lafontaine (2006)**[49] **–** neste processo, cujos factos eram relativos à utilização da imagem de um conhecido político num anúncio publicitário de uma empresa do ramo automóvel, o BGH decidiu que a utilização da imagem de uma pessoa com uma posição socialmente relevante encontrava-se abrangida pela liberdade de expressão prevista no artigo 5.º do GG. Este Tribunal entendeu também que o "entretenimento" devia prevalecer sobre o direito da personalidade.

Esta jurisprudência Lafontaine diverge relativamente à jurisprudência Herrenreíter na medida em que elimina a ficção do consentimento do titular da imagem.

- **A Decisão Lesebrief (1954)**[50] **–** O BGH, no âmbito desta ação, que versava sobre a publicação parcial de uma carta que um advogado havia enviado a um jornal, vem aceitar um direito geral da personalidade, que resultaria da interpretação do § 823, n.º 1.º do BGB[51]. O BGH assume uma posição na qual sustenta que notas pessoais, segundo a regra geral, não podem ser publicadas sem o consentimento do autor vivo, e apenas na sua forma permitida.

Para esta decisão relevou o facto de a GG adotar uma construção dogmática que permitia a fundamentação do "direito geral da personalidade". Ainda assim, um sector importante da doutrina entendia que "direito geral da personalidade" não era isento de equívocos no que dizia respeito ao seu âmbito de aplicação. Nesse sentido, defendia-se que apenas o Estado estaria vinculado a uma "função de dever de proteção", devendo conformar «*o "direito geral da personalidade"*

---

[49] Esta decisão foi preferida pelo BGHZ (169, 340) e está disponível e pode ser consultada em http://lorenz.userweb.mwn.de/urteile/izr182_04.htm (17.03.2018).

[50] A decisão está disponível para consulta em http://www.servat.unibe.ch/dfr/bz013334.html (17.03.2018).

[51] Não se encontra qualquer menção expressa a esta disposição do BGB, mas o acórdão assenta na doutrina lá espelhada, pois faz referência ao "direito geral da personalidade" (número 1 do artigo 2.º do GG) e ao "princípio da dignidade da pessoa humana" (número 1 do artigo 1.º do GG). Assim, o Direito Civil seria a base para a fundamentação do novo "direito geral da personalidade". PINHEIRO, Alexandre Sousa, op. cit., p. 438.

nas relações entre privados, não se verificando um fenómeno de eficácia externa»[52]

No seguimento desta decisão, a jurisprudência dos altos Tribunais alemães estabilizou no sentido acima defendido. Desta fase de construção argumentativa, cabe realçar, a Decisão Investitionshilfe de 1954[53] e a decisão "Persõnlíchkeítsrecht" de 1957[54]. A partir deste quadro jurisprudêncial sobre os direitos da personalidade, a jurisprudência irá, posteriormente, desenvolver-se no sentido da autodeterminação informacional com a decisão dos censos de 1983.

- **A decisão Mephisto (197l)[55] –** no âmbito deste processo, referente à sátira do percurso profissional do ator falecido Gustaf Grúndgens[56], O Tribunal ponderou a relação entre a liberdade de criação e expressão artística (previsto no artigo 5.º) e a limitação aos direitos fundamentais decorrente do número 2 do artigo 2., que seria levada a cabo por critérios estabelecidos pela ordem constitucional, pela moral e pelos direitos dos outros. O Tribunal conclui pela não aplicação deste último.

Note-se, contudo, que, de acordo com a posição aprovada, não foi necessário ponderar o "livre desenvolvimento da personalidade" visto que este não se poderia aplicar a um falecido, como era o caso de Gustaf Grúndgens.

---

[52] PINHEIRO, Alexandre Sousa, op. cit., p. 439.

[53]Esta decisão versou sobre incentivos ao investimento e o Tribunal decidiu no sentido de que a liberdade geral de atuação é um pressuposto essencial sem o qual o ser humano não pode ser entendido ou julgado como "pessoa ética e moral". Em conformidade, o Tribunal decidiu que deve-se avaliar o ser humano como um "ser social", pelo que, em caso de tensão entre o ser individual e a comunidade, deveria prevalecer os interesses desta última. Contudo, no âmbito da Lei Fundamental, era necessário restringir a liberdade de atuação, sem infringir o disposto relativo ao princípio da dignidade da pessoa humana.

[54]Os factos subjacentes ao caso respeitavam ao segredo médico. O Tribunal entendia que a previsão constitucional de um direito ao desenvolvimento da personalidade conjugado com o princípio da dignidade da pessoa humana impunha o direito geral da personalidade como posição jurídica oponível quer a entidades públicas como a entidades privadas. O Tribunal entendeu também que não podia ser negada a conclusão segundo a qual o conceito de "personalidade geral" devia ser considerado um "outro direito" para os efeitos do art.º 823.º.
A decisão está disponível para consulta em http://www.servat.unibe.ch/dfr/bz024072.html (17.03.2018).

[55] A decisão está disponível para consulta em http://www.servat.unibe.ch/dfr/bv030173.html (17.03.2018).

[56] A discussão era sobre a publicação de um livro de Klaus Mann, no qual este utilizou um personagem para satirizar o percurso profissional do ator Gustaf Grúndgens, ainda que sob outro nome. A crítica era feita através de insinuações e comentários sobre a ligação do ator ao regime nazi.

O aspeto decisório fulcral nesta decisão estaria na conformidade, apreciada no caso concreto, entre as liberdades de expressão e a criação artística com o princípio da dignidade da pessoa humana. Sobre isto, o Tribunal considerou que "*a obra de arte não tem apenas um efeito com valor estético, mas, também, um dever-ser social*", pelo que a obra foi retirada do mercado.

- **A decisão Elfes (1957)**[57]- nesta decisão o Tribunal reiterou a linha decisória do processo Investitionshilfe de 1954, segundo a qual o indivíduo não pode ser considerado um ser "extrassocial", pelo que o direito fundamental geral de atuação e o direito ao livre desenvolvimento da personalidade podem ser limitados. Nos termos da lei que regulava a renovação de passaportes, existia uma cláusula residual que permitia à Administração não deferir o pedido dos particulares quando estivessem em causa "outros interesses vitais". Foi com fundamento nesta cláusula restritiva que o Tribunal decidiu a favor da Administração Pública, entendendo que a restrição havia sido corretamente realizada.

Esta decisão releva a nível dogmático no medida em que resulta essencialmente da interpretação do Tribunal, no sentido de a GG proteger "toda" a "personalidade" com recurso ao direito fundamental ao livre desenvolvimento da personalidade, e não apenas proteger o conteúdo nuclear da personalidade.

- **A decisão Eppler (1980)**[58] – mais uma vez, no âmbito deste processo discutiu-se a interpretação do art.º 2.º como fundamento para a restrição de direitos. Depois de ter qualificado o direito sediado no artigo 2.° como um "direito de liberdade inominado", o Tribunal reiterou a doutrina de que a articulação entre o número 1 do artigo 2.° com o número 1 do artigo 1.º complementa os direitos constitucionais especialmente previstos. Uma das

[57] A matéria de facto subjacente à decisão dizia respeito à recusa apresentada pela Administração Pública a um político, para proceder à renovação do passaporte, com o fundamento substancial de que o indivíduo em reuniões e outras iniciativas internacionais criticava arduamente a política de defesa alemã, bem como a reunificação do Estado. O referido processo punha em causa tanto a liberdade geral de atuação, como a liberdade de circulação. Esta decisão pode ser consultada em http://www.servat.unibe.ch/dfr/bv006032.html (17.03.2018).

[58] A matéria de facto consistia no facto de um político da CDU ter atribuído publicamente um discurso público favorável à nacionalização dos bancos e da indústria a um político do SPD. Este último intentou uma ação judicial por ter sido lesado devido ao facto de tais palavras não terem correspondência com aquilo que ele fez ou disse.
Esta decisão pode ser consultada em http://www.servat.unibe.ch/dfr/bv054148.html (17.03.2018).

funções desta conjugação é a proteção constitucional dos direitos e liberdades não expressamente previstos na GG. O Tribunal decidiu que estava em causa um "prejuízo político", mas não um "atentado à dignidade pessoal", sendo que para tal conclusão, o Tribunal fundamentou que a imputação de observações a um indivíduo não afeta o direito geral da personalidade na medida em que tem na sua base a "ação de outro" indivíduo e não do autor da ação.

- **A decisão Soraya (1973)**[59] – o Tribunal, no âmbito de um recurso proposto pela revista, foi chamado a abordar a existência de uma ordem objetiva de valores constitucionais, que também influenciam o Direito Privado, através de um "efeito de irradiação". O sistema de valores existente assentaria na personalidade humana, relativamente à qual é reconhecido o direito do livre desenvolvimento na comunidade social, e que tem como elemento transversal o princípio da dignidade da pessoa humana". «*Além de uma função enquadradora de carácter objetivo, a articulação entre os artigos 2.° e 1.°, n.º 1 apresenta a função normativa de "preencher lacunas na proteção da personalidade"*»[60]. Ao ponderar os valores em causa, o Tribunal considerou que no caso de uma entrevista fictícia, não existia interesse geral do público à informação, pelo que devia prevalecer o direito geral da personalidade.

No seguimento desta decisão, "*a doutrina refere uma Lex Soraya que assenta na atribuição de uma indemnização à lesada*"[61], que irá consubstanciar responsabilização civil por danos não patrimoniais.

- **A decisão Tonband (l973)**[62] – no âmbito deste processo, o Tribunal pronunciou-se no sentido de que o direito fundamental previsto no disposto no

---

[59] Dos factos alegados no processo pode ler-se que um periódico empregou esforços no sentido de conseguir entrevistar a princesa Soraya do Irão, aquando de uma visita sua à Alemanha, mas não conseguiu obter a desejada entrevista. Não tendo conseguido o seu objetivo, a revista publicou uma "entrevista inventada" com a princesa Soraya, e fê-lo de forma a criar a ilusão de urna verdadeira entrevista.
Esta decisão pode ser consultada em http://www.servat.unibe.ch/dfr/bv034269.html (17.03.2018).

[60] PINHEIRO, Alexandre Sousa, op. cit., p. 443.

[61] *Ibidem.*

[62] A matéria de facto constante do processo relaciona-se com a uma gravação efetuada aquando da realização de um contrato de compra e venda com simulação de preço, e a realização, no âmbito do mesmo negócio, de um contrato de mútuo em fraude à lei. Os vendedores gravaram as negociações dos contratos sem o conhecimento ou consentimento por parte do comprador. O problema jurídico colocou-se quando da apresentação e consequente aceitação, em juízo, da referida gravação corno prova.
Esta decisão pode ser consultada em http://www.servat.unibe.ch/dfr/bv034238.html (17.03.2018).

numero 1 do artigo 2.º ao proteger o livre desenvolvimento da personalidade, abrange também o direito à própria imagem e o direito à palavra falada. Em conformidade, o Tribunal reafirmou a doutrina da "área cerne de proteção da personalidade", que foi violado pelas gravações levadas a cano pelos vendedores. O direito da personalidade também protege negociações comerciais, garantindo o seu registo gravado apenas com o consentimento das partes, assim se cumprindo as exigências do princípio da proporcionalidade.

No entendimento do Tribunal, como não se tratava de uma intervenção autorizada pelos tribunais competentes ou de uma intervenção numa investigação levada a cabo por um poder público, as gravações não poderiam ser aceites como meio de prova por terem sido obtidas em contradição com a GG e a lei. Adicionalmente, a Tribunal entendeu que não existia um correlativo interesse social especialmente protegido que permitisse limitar o direito de personalidade.

- **A decisão Lebach (1973)**[63] – esta decisão resultou da ponderação de valores realizada pelo Tribunal Constitucional Federal da República Federal da Alemanha entre a liberdade de expressão (prevista pelo artigo 5.º do GG) e o "direito ao esquecimento", que permitiria ao indivíduo condenado pela prática de um crime, a possibilidade de ressocialização posterior.

No entendimento deste tribunal, era necessário recorrer ao princípio da proporcionalidade para delimitar a fronteira da área intocável da vida interna, impedindo a transmissão de uma mensagem informativa mais completa no momento da libertação. Para o tribunal, a captação e divulgação de representações do indivíduo condenado iria colidiria com o seu direito ao livre desenvolvimento da personalidade, conjugado com o princípio da dignidade da pessoa humana (nos termos do disposto no número 1 dos artigos 2.° e 1.º da GG), causando ofensas a uma área do sujeito na relação consigo mesmo e com a comunidade onde procurará integrar-se aquando da sua libertação pois a exposição dos factos, iria resultar num efeito estigmatizador do indivíduo.

[63] A ação dizia respeito à captação de imagens sobre o nome e a fisionomia de um indivíduo condenado pela prática de um crime.
Esta decisão pode ser consultada em http://www.servat.unibe.ch/dfr/bv035202.html (17.03.2018).

Em resultado desta vasta jurisprudência, foi formado um "*corpus homogéneo de decisões sobre a autodeterminação informacional*"[64], ainda que a jurisprudência posterior proceda de seguida à distinção entre os direitos de personalidade e a proteção de dados, conforme se analisará de seguida.

As influências doutrinárias

Importa salientar, não apenas a jurisprudência mas também, as influências doutrinárias que contribuíram para a formação e desenvolvimento *Datenschutz*, dentre as quais destacam-se Heinrich Hubmann, Hans -Ulrich Evers e Niklas Luhmann.

Heinrich Hubmann é considerado um dos criadores de uma das principais construções doutrinárias clássica relativas aos direitos de personalidade, a chamada "*teoria das esferas*"[65], que assenta na ideia de que a sociabilidade de um indivíduo deve e serve como limitação à sua liberdade individual, devendo a intensidade da tutela jurídica da personalidade ser inversamente proporcional à sociabilidade do seu comportamento. Assim sendo, a doutrina alemã perpetrada por Heinrich Hubmann na sua obra *Das Persönlichkeitsrecht*, caracteriza-se por reconhecer na personalidade humana três esferas concêntricas, dentro das quais a personalidade da pessoa se desenvolve[66]. A primeira e mais restrita dessas esferas é a esfera secreta (*Geheimnisphäre*), a qual englobaria situações restritas à própria pessoa e exclusivamente a ela acessível (ou a um círculo limitadíssimo de pessoas próximas tais como familiares e amigos próximos). A segunda esfera é a esfera privada (*Privatsphäre*), que seria mais ampla que a anterior e já engloba algumas integrações com o espaço público e com terceiros. A última e mais ampla esfera na qual se desenvolve a personalidade da pessoa seria a esfera individual, que

[64] PINHEIRO, Alexandre, op.cit. 445.
[65] A teoria das esferas foi estudada e desenvolvida por diversos autores, sendo que os autores divergem quanto à denominação e à quantidade das referidas esferas. Na Alemanha, Heinrich Henkel também se debruçou sobre a teoria das esferas. *Apud* CORDEIRO, António Menezes – **Tratado de Direito Civil Português: Parte Geral – Pessoas. Vol. 1, tomo III**. Lisboa: Almedina, 2004. p. 200.
[66] *Apud* CORDEIRO, António Menezes. op. cit., p. 200.

abarcaria o "*ser individual integrado no mundo e ao seu valor singular na área pública*"[67].

Por seu turno, Hans-Ulrich Evers defendia que «*o direito à manutenção da esfera privada faz parte da "liberdade geral de ação" prevista no art.º 2, n.º 1 GG. Esta envolve a necessidade do indivíduo preservar assuntos pessoais e, no limite, de se "fechar" relativamente à comunidade*»[68]. Segundo Hans-Ulrich Evers, o disposto no número 1 do artigo 2.º da Lei Fundamental da República Federal da Alemanha confere um "direito à autoconformação" pois abrange o ser que atua e, na medida que o faz, revela a sua personalidade. Este direito de autoconformação inclui também o direito de conformar a extensão de abertura com o meio social, pelo que relevam também os limites estabelecidos pelo indivíduo[69].

Em conformidade, o limite da esfera privada será o limite a partir do qual os factos pessoais podem ser do conhecimento de público ilimitado. Mesmo ao Estado, só lhe é permitida a penetração na esfera privada quando estiverem preenchidos os pressupostos estabelecidos por lei para o efeito[70].

Por último, Niklas Luhmann debruçou-se sobre a autoapresentação do indivíduo. Para o autor, cada indivíduo tem o "poder funcional de autoapresentação prévio", na medida em que a integração social do indivíduo é da sua própria responsabilidade, podendo este "personificar" as suas interações no contexto de uma sociedade que oferece "sistemas comunicacionais diferenciados"[71].

Apesar de termos referenciado estes três autores, importa esclarecer que o seu grande contributo resultou tanto das críticas que foram sendo feitas a cada uma das construções como dos esforços que foram feitos no sentido de colmatar as falhas identificadas[72]. A partir destas doutrinas e das que se seguiram em consequência destas, a jurisprudência também foi tomando o seu rumo no sentido do desenvolvimento da *Datenschutz*.

---

[67] Pinheiro, Alexandre Sousa, op. cit. p. 447.
[68] EVERS, Hans-Ulrich - **Privatsphäre und Ämter für Verfassungsschutz**. Berlim: Walter de Gruyter & Co., 1960, p. 38, *apud* Pinheiro, Alexandre Sousa, op. cit. p. 457.
[69] Ibidem.
[70] EVERS, Hans-Ulrich, op. cit. p. 44, *apud* Pinheiro, Alexandre Sousa, op. cit. p. 458.
[71] LUHMANN, Niklas - **Grundrechte als Institution. Ein Beitrag zur politischen Soziologie**. Berlim: Duncker & Humbolt, 1999, *apud* Pinheiro, Alexandre Sousa, op. cit. p. 460.
[72] Pinheiro, Alexandre Sousa, op. cit. p. 446.

Assume especial relevância o "parecer de carácter dogmático pedido pelo Ministério do Interior a um importante grupo de peritos"[73]. Este parecer surge no contexto de uma Alemanha pós segunda guerra mundial, que por um lado estava traumatizada pela utilização de registos públicos que fora feita pelo poder nazi, mas que não podia impedir a automatização de processos para tratamento de informação pessoal, incluindo o recurso a computadores. Este estudo antecipou a doutrina da Decisão dos Censos, que iremos abordar de seguida, e assentou nos seguintes aspetos:

- Não existia qualquer disciplina jurídica que regulasse a "relação comunicacional indivíduo-Estado" e essa regulação era necessária de forma a estabelecer regras que garantissem o equilíbrio naquela relação, "de modo a não transformar as pessoas em "objetos informacionais"[74].
- O uso da informática, que permite simultaneamente a exclusão parcial do fator territorial e o tratamento de mais informação de forma mais célere, exige também que existam soluções padronizadas para os potenciais problemas.
- A pessoa perdia o direito de "autodeterminação, na medida em que já não pode delimitar as fronteiras entre o estatal/público e o privado"[75].
- «*A proteção de dados assume-se claramente corno problema político, não como figura "técnico-instrumental*"»[76].
- Os "dados pessoais" são informação tratada, que recaem tanto sobre pessoas como sobre objetos[77].
- As regras a aplicar deviam ser diferentes consoante se tratasse de entidades públicas ou entidades privadas a proceder ao tratamento dos dados[78].
- Os autores defendem "a necessidade de respeito pelas liberdades de expressão e opinião, religiosa e de informar", no que toca à relação entre a

[73] STEINMÜLLER et alli – "Grundfragen des Datenchutzes. Gutachten im Auftrag des Bundesministeriums des Innern", **Bunderstagdrucksache**, Bona, VI/3826, 1972 *apud* Pinheiro, Alexandre Sousa, op. cit. p. 463.
[74] Idem, p. 36-37.
[75] Ibidem.
[76] STEINMÜLLER et alli, op. cit. p.41 *apud* Pinheiro, Alexandre Sousa, op. cit. p. 466.
[7777] STEINMÜLLER et alli, op. cit.p.55 *apud* Pinheiro, Alexandre Sousa, op. cit. p. 466.Pinheiro, Alexandre Sousa, op. cit. p. 466.
[78] STEINMÜLLER et alli, op. cit.p.59 *apud* Pinheiro, Alexandre Sousa, op. cit. p. 467.

informatização e os direitos fundamentais. O direito à "autodeterminação informacional" não pode impedir o desenvolvimento da opinião pública[79].

- É através do n.º 1 do artigo 2 da Lei Fundamental da República Federal Alemã que os autores fundamentam a constitucionalidade do novo direito à "autodeterminação informacional"[80].
- À partida, a utilização dos dados para outra finalidade que não aquela para a qual foram recolhidos os dados é proibida e só é admissível nos casos em que as circunstâncias respeitem o princípio da proporcionalidade e estejam especialmente previstas por lei[81]. Ao abrigo desta limitação, ficam condicionadas as trocas de informação no âmbito da Administração Pública.
- O parecer alerta para a necessidade de "direitos secundários" que permitam ao indivíduo alterar, corrigir e eliminar os dados que lhe dizem respeito[82].

<u>As referências jurisprudenciais</u>

Antes de entrar na Decisão dos Censos, importa mencionar brevemente as decisões *Mikrozensus* e *Ehescheidungsakaten*, nas quais releva especialmente releva especialmente: *«(i) a criação de uma área pessoal imune à intervenção dos poderes públicos ou privados, (ii) o reconhecimento (ainda que tímido) da adequação da informação recolhida a uma finalidade determinada, (iii) o reconhecimento do principio "proporcionalidade" na área informacional, (iv) a fundação da protecção de informação individual no principio da dignidade da pessoa humana*.»[83]

- **A decisão Mikrozensus (1969)[84]**– o Tribunal foi chamado a pronunciar-se sobre a compatibilidade com a Constituição de normas relativas à população e à vida profissional, através das quais se recolhia informação sobre "viagens de férias e de recreio". O Tribunal defendeu que estas informações não punham em causa a interpretação integrada dos artigos 1 .°. n.° 1 e 2.°, n.° 1 da GG.

---

[79] STEINMÜLLER et alli, op. cit.p.83 *apud* Pinheiro, Alexandre Sousa, op. cit. p. 469.
[80] STEINMÜLLER et alli, op. cit.p.84 *apud* Pinheiro, Alexandre Sousa, op. cit. p. 46.
[81] STEINMÜLLER et alli, op. cit.p.109 *apud* Pinheiro, Alexandre Sousa, op. cit. p. 471.
[82] STEINMÜLLER et alli, op. cit.p.126 *apud* Pinheiro, Alexandre Sousa, op. cit. p. 473.
[83] Pinheiro, Alexandre Sousa, op. cit. p. 475.
[84] Esta decisão está disponível para consulta em http://www.servat.unibe.ch/dfr/bv027001.html (17.03.2018)

No entendimento do Tribunal, apesar de existir a necessidade de respeitar o "espaço interno do indivíduo", o "direito à autodeterminação na área interna da vida", o "direito a ser deixado em paz" pelo Estado, o "direito à solidão" e à "área intangível da vida individual" livre de intervenções do poder público, não se pode concluir que tenha havido violação da esfera íntima da pessoa pois o tratamento desta informação era de carácter aleatório e não seletivo. Assim, a recolha desta informação não punha em causa os princípios do Estado de Direito, pois o Tribunal procedia à distinção entre "dados constitucionalmente protegidos" e "dados ordinariamente protegidos".

- **A decisão Ehescheidungsakaten (1970)**[85] – Na sua decisão deste processo, o Tribunal decidiu que a transferência em causa não era, em princípio, lícita, exceto nos casos em que houvesse consentimento dos cônjuges ou ex-cônjuges, ou quando estivesse em causa um interesse geral preponderante, e na medida em que fosse respeitado o princípio da proporcionalidade. A perspetiva social do indivíduo pode justificar a interferência do poder público na esfera privada do mesmo, mas desde que seja respeitado o princípio da proporcionalidade. No cas concreto, tendo em conta que o pedido dos dados do divórcio não foi acompanhado por qualquer fundamentação, o tribunal não tinha possibilidade de proceder a um juízo com base no princípio da proporcionalidade, pelo que não se podia concluir pela proporcionalidade desta interferência.

O Tribunal voltou a defender a existência de uma "área intangível da vida individual", livre de intervenções do poder público, que visa garantir o "livre desenvolvimento da personalidade", como manifestação da dignidade da pessoa humana.

Na sequência desta jurisprudência, em 1977 foi aprovada a primeira Lei Federal De Proteção de Dados Da República da Federal da Alemanha, a Bundesdateschutzgesetz (BDSG). Este diploma previa que qualquer "*tratamento informatizado de dados pessoais carecia de uma condição de legitimidade baseada ou na lei, ou no consentimento individual*", ainda que a lei também se

[85] Esta decisão recaia sobre a transferência de dossiês de um processo de divórcio para utilização em processo disciplinar. Está disponível para consulta em http://www.servat.unibe.ch/dfr/bv027344.html (17.03.2018)

aplicasse a "dados manuais". O BDSG estabeleceu regras distintas para o tratamento por entidades públicas e entidades privadas, garantindo também ao indivíduo os direitos secundários de "informação, de correção e de apagamento de dados pessoais incorretamente registados". Através desta lei foi também criado um Comissário Federal de proteção de dados[86].

A decisão dos Censos (*Volkszählung*)[87]

A Decisão dos Censos é um dos casos mais relevantes, no contexto alemão e internacional, no domínio da proteção de dados pessoais.

Ao abrigo desta decisão, o Tribunal afirmou que o direito geral da personalidade, tal como previsto no número 1 do artigo 2.° da GG, conjugado com o número 1 do artigo 1.º da GG, garante ao indivíduo proteção contra a recolha, armazenamento, uso e transmissão ilimitados de dados pessoais. Este direito está, logicamente, sujeito a limitações com fundamento no interesse geral da comunidade, que devem estar necessariamente fundamentadas na Constituição e na lei. Deste modo, o legislador, ao prever as situações que consubstanciem limites a este direito, deve observar o princípio da proporcionalidade e assegurar as garantias a nível da organização e procedimentos que possam significar perigos de violação do direito à autodeterminação informacional.

No que diz respeito à matéria estatística, o Tribunal considera que devem ser distinguidos os dados pessoais dos dados anónimos, pois, no âmbito da atividade estatística, o Tribunal reconhece que não pode verificar uma completa observância do princípio da finalidade, dado que a informação recolhida pode ser usada para diversas finalidades públicas. Ainda assim, a estatística ou outra forma pública de tratamento de dados não pode fornecer resultados quanto ao "perfil completo do indivíduo" ou a "catalogação da personalidade".

[86] Pinheiro, Alexandre Sousa, op. cit. p. 517.
[87] BVerfGE, 65, 1; disponível em <http://www.servat.unibe.ch/dfr/bv065001.html> (6.11.2011).

O Tribunal entende que o centro do ordenamento se encontra o "valor" da "dignidade" da pessoa como membro de uma sociedade livre. Deste modo, o direito geral da personalidade pode adquirir um significado especial, tendo em conta os novos perigos decorrentes da evolução tecnológica, que possibilitava que sistemas informáticos permitissem o armazenamento e a consulta de informação pessoal, ficando ultrapassados os dossiês e ficheiros manuais. Nesse sentido, o "tratamento de dados pessoais" (*Datenverarbeitung*) com recurso à informática carece de medidas especiais de proteção, nomeadamente no que respeita à segurança dos sistemas e às garantias de organização e de procedimentos que devem ser asseguradas.

Através de bases de dados integradas, passou a ser possível unificar informação individual dispersa por vários ficheiros, sem que o titular de dados pessoais possa exerça qualquer controlo sobre a veracidade destes dados ou possa sequer conhecer a sua utilização. Assim sendo, aumentaram as possibilidades de obter informação sobre os indivíduos, principalmente enquanto membros de uma comunidade política, pelo que são justificados os receios de que nasçam formas de "pressão psíquica" que limitem o comportamento dos indivíduos. O Tribunal entendeu que não era compatível com a autodeterminação informativa um modelo de funcionamento social que sistemas informatizados criassem casos em que os indivíduos não saibam quem detém informação a seu respeito e qual o conteúdo daquela informação. Nesse sentido, o Tribunal enfatizou o direito ao "livre desenvolvimento da personalidade" associado ao bem comum como condição necessária para o funcionamento de uma sociedade democrática.

Claro está que o Tribunal também reconheceu que o direito à autodeterminação informacional não é ilimitado e está sujeito às limitações próprias ditadas pela inserção do indivíduo num contexto social, do qual faz parte integrante. Os limites ao direito à autodeterminação informacional devem ser previstos em base legal e devem respeitar o princípio da proporcionalidade, que deve funcionar como medida de graduação da limitação dos direitos fundamentais.

Numa dos excertos, a decisão Censos considera que, com as "possibilidades de tratamento" e dá "conexão" próprias da evolução da técnica, não existem "dados

inofensivos", pelo que a definição adequada do princípio da finalidade é estritamente decisiva, no sentido de que os tratamentos devem obedecer ao critério de "vinculação à finalidade". Deste modo, o Tribunal concluiu que a informação sensível para o titular dos dados não provém unicamente da natureza íntima de tal informação, mas do "contexto de uso" que será dado à respetiva informação. Para o Tribunal, a natureza "íntima" da informação pessoal deve deixar de ser critério valorativo relativamente à sensibilidade dos dados, devendo ter-se em conta a finalidade dos tratamentos concretos[88].

O tribunal considerou que os casos de recolha coerciva de dados não poderiam ser ilimitados, nomeadamente nos casos de tratamentos realizados no âmbito da atividade administrativa. De tal modo, para além do respeito pelo princípio da proporcionalidade, o legislador deve identificar os tipos, natureza e forma de utilização dos dados, estabelecendo um regime que impeça os perigos do abuso dos dados recolhidos. Em regra, apresentam pertinência os dados com repercussão social, e não informações da esfera íntima ou que possam contribuir para a autoincriminação do titular. A natureza coerciva da recolha torna decisiva a definição do princípio da tonalidade e da limitação da informação ao "mínimo necessário" para a prossecução dos objetivos públicos.

Esta decisão foi fundamentada na autodeterminação informacional reconhecida com base na conjugação do disposto no número 1 do artigo 2.º da GG e no número 1 do artigo 1.º da Lei Fundamental de Bona[89].

A jurisprudência continuou a evoluir e o primeiro BDSG foi alterado na sequência da Decisão de Censos[90]. A futura Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 também irá provocar alterações ao BDSG, mas esta matéria será abordada nos capítulos seguintes.

---

[88] O Tribunal não rejeita expressamente a "teoria das esferas", mas aponta no sentido de se dever qualificar os tratamentos como sensíveis ou não sensíveis, e não os dados em função da sua natureza secreta, íntima ou privada.
[89] Pinheiro, Alexandre Sousa, op. cit. p. 486.
[90] Apesar de Decisão dos Censos ser de 1983, o BDSG só foi alterado em 1990.

A EVOLUÇÃO DA PROTEÇÃO DE DADOS NO DIREITO INTERNACIONAL

Apesar da importância destas duas evoluções para o entendimento das opções adotadas pelas diversas leis no âmbito da proteção de dados, não nos alongaremos mais sobre estes dois paradigmas pois, antes de entrar no capítulo específico da legislação portuguesa, importa dar uma breve explicação sobre o desenvolvimento da proteção de dados no contexto internacional, nomeadamente nos textos da ONU, do Conselho da Europa. No âmbito do direito da União Europeia, importa também analisar os instrumentos que irão posteriormente influenciar a legislação nacional.

ONU

> "*Ninguém sofrerá intromissões arbitrária 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.*"[91]

> "*Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra ou à sua reputação.*"[92]

A DUDH reconhece o direito à privacidade e o direito à reserva da intimidade da vida privada, fundado na dignidade humana, que reconhece "ser inerente a todos os membros da família humana", sendo que os próprios povos das Nações Unidades "reafirmaram, na Carta da ONU, sua fé nos direitos humanos fundamentais, na dignidade e no valor do ser humano"[93].

---

[91] Esta transcrição corresponde ao disposto no artigo 12.º da Declaração Universal dos Direitos do Homem, aprovado em 1948. A declaração está disponível e pode ser consultada através do link http://www.un.org/en/universal-declaration-human-rights/index.html (17.03.2018).

[92] Esta transcrição corresponde ao disposto no artigo 17.º do Pacto Internacional dos Direitos Civis e Políticos, de 1966. O diploma está disponível para consulta em http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhuniversais/cidh-dudh-direitoscivis.html.

[93] Primeiro e Quinto Considerandos da Declaração Universal dos Direitos do Homem.

Estes direitos, à privacidade e à reserva da vida privada, foram posteriormente densificados pela proclamação de Teerão[94] e Resolução n.º 2450, de 19 de Dezembro de 1968[95], que foi aprovada na sequência daquela proclamação. Esta Resolução convida o Secretário-Geral, com a ajuda do comité relevante, a levar a cabo um estudo sobre os problemas relacionados aos direitos humanos que possam advir da evolução da ciência e da tecnologia, requerendo também um relatório com os estudos já realizados ou em curso sobre as mesmas matérias.

CONSELHO DA EUROPA

> *"1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 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 a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros."*

Em 1950, o Conselho da Europa adotou a Convenção Europeia dos Direitos do Homem – CEDH, que viria a entrar em vigor em 1953. O objetivo da CEDH é o de promover o Estado de Direito, a democracia, os direitos humanos e o desenvolvimento social.[96]

Todos os Estados membros do Conselho da Europa estão obrigados ao cumprimento da CEDH e muitos incorporaram ou deram cumprimento à CEDH no

---

[94] Esta proclamação foi aprovada na Conferência de Teerão de 1968, na qual foi analisada a evolução tecnológica e as vantagens e desvantagens dela resultantes. A proclamação está disponível e pode ser consultada em http://www.direitoshumanos.usp.br/index.php/Confer%C3%AAncias-de-C%C3%BApula-das-Na%C3%A7%C3%B5es-Unidas-sobre-Direitos-Humanos/proclamacao-de-teera.html (17.03.2018)

[95] A Resolução n.º 2450, de 19 de Dezembro de 1968 pode ser consultada em https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/244/10/IMG/NR024410.pdf?OpenElement (17.03.2018).

[96] Conselho da Europa - **Manual da legislação Europeia sobre protecção de dados**, pp. 14 e 15. Disponível em https://www.cnpd.pt/bin/legis/internacional/fra-2014-handbook-data-protection-pt.pdf

seu direito nacional. Ainda assim, de forma a garantir que as partes contratantes cumprissem as obrigações assumidas ao abrigo do CEDH, foi criado, em 1959, o Tribunal Europeu dos Direitos do Homem - TEDH, O TEDH assegura o cumprimento das obrigações assumidas pelos Estados ao abrigo da Convenção através da apreciação de queixas apresentadas por cidadãos, grupos de cidadãos, ONG ou pessoas coletivas que aleguem violação da Convenção.

Na sua jurisprudência, o TEDH já se pronunciou sobre diversas situações em que foi suscitada a questão da proteção de dados, entre as quais importa destacar questões relacionadas com a interceção de comunicações[97], as várias formas de vigilância[98] e proteção contra o armazenamento de dados pessoais pelas autoridades públicas[99].

Na sequência do surgimento da tecnologia da informação e de novos meios de comunicação e informatização, o Conselho da Europa sentiu a necessidade de "*adotar regras mais pormenorizadas para salvaguardar as pessoas através da proteção dos seus dados pessoais*"[100]. Nesse sentido, o Comité de Ministros do Conselho da Europa adotou, em meados da década de 70, duas resoluções sobre a proteção de dados pessoais que faziam referência ao artigo 8.º da CEDH: A Resolução (73)22 relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor privado, de

---

[97] Ver, a título de exemplo, os seguintes acórdãos:
TEDH, acórdão Malone c. Reino Unido de 2 de agosto de 1984, petição n.º 8691/79, disponível para consulta em https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57533%22]} (17.03.2018);
TEDH, acórdão Copland c. Reino Unido de 3 de abril de 2007, petição n.º 62617/00, disponível para consulta em https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-79996%22]} (17.03.2018).

[98] Ver, a título de exemplo, os seguintes acórdãos:
TEDH, acórdão Klass e o. c. Alemanha de 6 de setembro de 1978, petição n.º 5029/71, disponível para consulta em https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]} (17.03.2018);
TEDH, acórdão Uzun c. Alemanha de 2 de Setembro de 2010, petição n.º 35623/05, disponível para consulta em https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-100293%22]} (17.03.2018).

[99] Ver, a título de exemplo, os seguintes acórdãos:
TEDH, acórdão Leander c. Suécia de 26 de março de 1987, petição n.º 9248/81, disponível para consulta em https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]} (17.03.2018);
TEDH, acórdão S. and Marper c. Reino Unido de 4 de dezembro de 2008, petições n.ºs 30562/04 e 30566/04, disponível para consulta em https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]} (17.03.2018).

[100] Conselho da Europa, op.cit. p. 15 e 16.

26 de setembro de 1973[101]; e a Resolução (74) 29 relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor público, 20 de Setembro de 1974[102].

Convenção n.º 108

No entanto, o maior foco recai sobre a Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal (Convenção 108)[103][104].

A Convenção 108 aplica-se a todos os tratamentos de dados pessoais realizados tanto pelo setor privado como pelo setor público, incluindo os tratamentos de dados efetuados pelas autoridades policiais e judiciárias. Conforme consta do disposto no artigo 1.º, a Convenção visa garantir o respeito pelos direitos e liberdades fundamentais de cada indivíduo, em particular, o seu direito à privacidade em relação a "tratamentos automatizados[105] dos dados pessoais[106] que

---

[101] A Resolução pode ser consultada em https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=590512&SecMode=1&DocId=649498&Usage=2 (17.03.2018).

[102] A Resolução pode ser consultada em https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2 (17.03.2018).

[103] Esta convenção foi aprovado e aberta para assinatura em 1981 e pode ser consultada em https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 (17.03.2018).

[104] No âmbito da União Europeia, através da Recomendação da Comissão n.º 81/679/CEE, de 29 de Julho, relativa à Convenção do Conselho da Europa sobre o tratamento automatizados de dados, a Comissão recomendou que os Estados-membros assinassem e ratificassem a Convenção. Esta recomendação está disponível para consulta em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31981H0679.

O que se verificou é que, apesar da Recomendação, apenas 7 países procederam à assinatura e ratificação da Convenção do Conselho da Europa, pelo que o Parlamento Europeu aprovou a Resolução do Parlamento Europeu de 9 de Março de 1982, na qual considerou necessário aprovar legislação comunitária sobre a matéria da proteção de dados.

[105] Apesar desta disposição, a Convenção admite que os Estados apliquem as normas da Convenção ao tratamento manual de dados, por força do disposto na alínea c) do número 2 do artigo 3.º. Caso os Estados assim optassem, estariam a conferir maior proteção do que a prevista na Convenção, possibilidade reconhecida no artigo 11.º da própria Convenção. Neste sentido, RAPOSO, Amável – **A Convenção de Proteção de Dados do Conselho da Europa na Expectativa da Ratificação Portuguesa,** in Gabinente De Documentação E Direito Comparado – Colóquio Informática e Tribunais, Lisboa 1992, p. 449, *apud* PINHEIRO, Alexandre Sousa, op. cit. p. 539.

Na verdade, nos termos do disposto no artigo 3.º da Convenção, o âmbito dos ficheiros de dados aos quais a Convenção será aplicada deve ser determinado pelos Estados aquando da assinatura da Convenção, no momento do depósito do instrumento de ratificação, aceitação, aprovação ou

lhe digam respeito. O tratamento de dados deve respeitar finalidades legítimas e determinadas[107].

Outros dois aspetos importantes da Convenção 108 são o facto desta proceder à criação da figura do "responsável pelo tratamento"[108] e consagrar igualmente os direito do indivíduo de ser informado sobre a existência de ficheiros automatizados a seu respeito, de aceder à informação, de retificar e de suprimir dados pessoais que lhe digam respeito e que constem de ficheiros automatizados.

Por último, a Convenção proíbe, na ausência de garantias jurídicas adequadas, o tratamento de dados «sensíveis», tais como dados sobre a raça, a opinião política, a saúde, as convicções religiosas, a vida sexual ou o registo criminal de uma pessoa.

A proteção de dados na jurisprudência do TEDH

Conforme acima demonstrado, a CEDH não prevê, expressa e isoladamente, a figura da proteção de dados. Nesse sentido, a abordagem do TEDH assentou na escolha de um "direito de referência" para permitir a penetração da figura da proteção de dados e da Convenção n.º 108.

---

adesão, ou em momento posterior. Naquela disposição pode ler-se :"*Qualquer Estado pode, (…)para notificar por declaração dirigida ao Secretário-Geral do Conselho da Europa:*
a) que não aplicará a presente Convenção a certas categorias de ficheiros de dados pessoais automatizados, cuja lista será depositada. Nesta lista não deve incluir, no entanto, as categorias de ficheiros de dados automatizados sujeitos, ao abrigo da sua lei interna, a provisões de proteção de dados. Por conseguinte, deve alterar a lista com uma nova declaração sempre que categorias adicionais de ficheiros de dados pessoais automatizados forem sujeitas a provisões de proteção de dados, ao abrigo da sua legislação interna;
b) que também aplicará a presente Convenção a informações relativas a grupos de pessoas, associações, fundações, empresas, corporações e quaisquer outros órgãos que constituam, de forma direta ou indireta, indivíduos, independentemente de esses órgãos possuírem personalidade jurídica ou não".

[106] O disposto na alínea a) do artigo 2.º da Convenção estabelece que são dados pessoais as "informações relativas a uma pessoa identificada ou identificável". Considerando que a Convenção não concretiza o conceito de pessoa identificável, o Relatório Explicativo da Convenção do Conselho da Europa vem dizer, no seu artigo 28.º, que por pessoa identificável deve entender-se uma "pessoa facilmente identificável", cujo processo de identificação não acarrete custos excessivos nem seja altamente complexo. Neste sentido, ver também GONÇALVES, Maria Eduarda – **Direito da Informação**, Coimbra: Almedina, 2003, p. 89.
O Relatório Explicativo da Convenção do Conselho da Europa está disponível para consulta em https://rm.coe.int/16800ca434.

[107] PINHEIRO, Alexandre Sousa, op. cit. p. 538.

[108] A Convenção cria a figura do "controller of the file" mas não procede à concretização de quais deviam ser as regras de funcionamento desta entidade.

Ao contrário da solução germânica, acima descrita, a jurisprudência do TEDH, na sua construção do direito à proteção de dados, não procurou expandir um principio – no caso, a dignidade humana –, mas partiu do direito ao respeito pela vida privada, pela vida familiar, pelo domiciliou e pela correspondência – formando o núcleo da "esfera privada"[109] – previsto no artigo 8.° da CEDH.

UNIÃO EUROPEIA

No início da década de 70, começou a ser discutida a necessidade de aprovar um instrumento europeu de proteção de dados, sendo que o Parlamento Europeu, em 1975, apresentou um estudo "*em que se apontava para a conveniência de elaborar rapidamente legislação comunitária que contribuísse para a uniformização das legislações nacionais de proteção dos cidadãos relativamente a erros ou abusos cometidos por via informática*"[110]. É na sequência deste estudo que é aprovada a Resolução do Parlamento Europeu de 8 de Maio 1979, contendo 14 referências introdutórias e 17 recomendações, estas últimas divididas em três capítulos "*relativos a princípios, direitos e à criação de u órgão de proteção de dados nacional."*[111]

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995

Em 1995, o Parlamento Europeu e o Conselho aprovara aquele que viria a ser, até 2016, o principal instrumento jurídico da UE sobre proteção de dados: a 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

[109] RAMIRO, Mónica Arenas – **El Derecho Fundamental a la Protección de Datos Personales en Europa**. Valência: Tirant lo Blanch, 2006, p. 56.
[110] PINHEIRO, Alexandre Sousa, op. cit. p. 573.
[111] PINHEIRO, Alexandre Sousa, op. cit. p. 574.

dados pessoais e à livre circulação desses dados (Diretiva de Proteção de Dados)[112] [113].

A Diretiva foi aprovada ao abrigo da norma habilitante constante do artigo 100.º- A do TUE[114]. A livre circulação de mercadorias, serviços e pessoas no mercado interno exigia o livre fluxo de dados, que só seria possível se os Estados-Membros pudessem confiar na existência de um nível uniformemente elevado de proteção de dados. Uma vez que o objetivo da aprovação da Diretiva de Proteção de Dados era a harmonização da legislação sobre proteção de dados a nível nacional[115], esta prevê um grau de especificidade comparável ao da legislação nacional sobre proteção de dados (então) em vigor. Segundo a jurisprudência do TJUE, "*a Diretiva 95/46 visa [...] tornar equivalente em todos os Estados-Membros o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais [...] A aproximação das legislações nacionais aplicáveis na matéria não deve fazer diminuir a proteção que asseguram, devendo, pelo contrário, ter por objetivo garantir um elevado nível de proteção na União Assim, [...] a harmonização das referidas legislações nacionais não se limita a uma harmonização mínima, mas conduz a uma harmonização que é, em princípio, completa.*"[116]. Consequentemente, os Estados-Membros dispunham apenas de uma pequena margem de manobra na transposição da Diretiva. Nesse sentido, apesar de a Diretiva incluir dois

---

[112]A Diretiva de Proteção de Dados está disponível para consulta em http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31995L0046.

[113] O processo de aprovação da Diretiva de Proteção de Dados foi longo e complexo, sendo que a primeira proposta foi apresentada em 1990 e a Diretiva só foi aprovada 5 anos depois, após duas alterações significativas (em 1992 e em 1993, apesar desta última ser uma "espécie de contraproposta"). HIGUERAS, Manuel Herdero – **La Directiva Comunitaria de la Protección de Datos de Carácter Personal**. Pamplona, 1997, p. 41 *apud* PINHEIRO, Alexandre Sousa, op. cit. p. 612

[114] O Tribunal de Justiça da União Europeia comentou este aspeto: "Directive 95/46, adopted on the basis of Article 100ª of the Treaty, is intended to ensure the free movement of personal data between Member States through the harmonization of national provisions on the protection of individuals with regard to the processing of such data". Decisões C-465/00, C-138/01 e C-139/01, disponíveis para consulta em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62000CJ0465.

[115] Ver os Considerandos 1, 4, 7 e 8 da Diretiva de Proteção de Dados.

[116] TJUE, acórdão de 24 de novembro de 2011, nos processos apensos C-468/10 e C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estad, n.ºs 28 e 29. Acórdão disponível para consulta em http://curia.europa.eu/juris/celex.jsf?celex=62010CJ0468&lang1=en&type=NOT&ancre=.

propósitos no seu artigo 1.º[117], é "*comummente aceite que o texto europeu visa, essencialmente, garantir a liberdade de circulação de dados pessoais*"[118].

Nos termos do disposto no número 1 do artigo 3.º da Diretiva, esta é aplicável ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro automatizado ou destinados a ficheiros automatizados. Note-se que estão excluídos do âmbito de aplicação da Diretiva os tratamentos de dados pessoais que, por um lado, sejam efetuados "*no exercício de atividades não sujeitas à aplicação do direito comunitário*[119]*, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objeto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as atividades do Estado no domínio do direito penal*"[120] [121].

---

[117] O artigo 1.º da Diretiva dispõe que: "*1. Os Estados-membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.*
2. Os Estados-membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-membros por razões relativas à proteção assegurada por força do nº 1."

[118] HIGUERAS, Manuel Herdero, op. cit., p. 70 *apud* PINHEIRO, Alexandre Sousa Pinheiro, op. cit., p, 616.

[119] A fórmula não taxativa adotada visava "*permitir abranger atividades prosseguidas quer a nível nacional, quer objeto de regulação comunitária*". HIGUERAS, Manuel Herdero, op. cit., p. 88 *apud* PINHEIRO, Alexandre Sousa Pinheiro, op. cit., p, 618.

[120] Ver o disposto no primeiro travessão do número 2 do artigo 3.º da Diretiva.

[121] A proteção de dados nestas matérias baseia-se em instrumentos jurídicos diferentes. A proteção de dados no setor policial e da justiça penal só está regulada no contexto da cooperação transfronteiriça entre as autoridades policiais e judiciárias.
A Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais no âmbito da cooperação policial e judiciária em matéria penal visa assegurar a proteção dos dados pessoais das pessoas singulares quando estes são tratados para efeitos de prevenção, investigação ou repressão de infrações penais ou de execução de sanções penais. Os Estados-Membros e a UE são representados por autoridades competentes que trabalham no setor policial ou da justiça penal. A aplicabilidade da Decisão-Quadro está limitada à garantia da proteção dos dados no âmbito da cooperação transfronteiriça entre estas autoridades e não abrange a segurança nacional. A Decisão-Quadro pode ser consultada em http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008F0977.
Note-se que em 2016 foi aprovada a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Esta diretiva está disponível para consulta em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016L0680.
Para além da Decisão-Quadro relativa à proteção de dados, existem outros instrumentos jurídicos que regulam o intercâmbio de informações detidas pelos Estados-Membros netas áreas específicas, tais como a Decisão-Quadro 2009/315/JAI do Conselho relativa à organização e ao conteúdo do intercâmbio de informações extraídas do registo criminal entre os Estados-Membros e a Decisão do

Outra exceção ao âmbito de aplicação da Diretiva é a chamada "exceção doméstica", que diz respeito ao tratamento de dados pessoais por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas. [122]Este tratamento é geralmente considerado parte das liberdades pessoais.

O âmbito de aplicação territorial da Diretiva de Proteção de Dados não se limita aos 28 Estados-Membros da UE, incluindo também os Estados que não são membros da UE mas que fazem parte do EEE[123]. Na verdade, a questão do âmbito de aplicação territorial da Diretiva levantava diversas questões. No artigo 4.º da Diretiva pode ler-se que "*1. Cada Estado-membro aplicará as suas disposições nacionais adotadas por força da presente diretiva ao tratamento de dados pessoais quando:*

a) O tratamento for efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento[124] situado no território desse Estado-membro; se o mesmo responsável pelo tratamento estiver estabelecido no território de vários Estados-membros, deverá tomar as medidas necessárias para garantir que cada um desses estabelecimentos cumpra as obrigações estabelecidas no direito nacional que lhe for aplicável;

b) O responsável pelo tratamento não estiver estabelecido no território do Estado-membro, mas num local onde a sua legislação nacional seja aplicável por força do direito internacional público;

c) O responsável pelo tratamento não estiver estabelecido no território da Comunidade e recorrer, para tratamento de dados pessoais, a meios, automatizados

---

Conselho relativa a disposições de cooperação entre as unidades de informação financeira dos Estados-Membros em matéria de troca de informações.

[122] Ver o disposto no segundo travessão do número 2 do artigo 3.º da Diretiva.

[123] De acordo com a Decisão do Conselho e da Comissão de 13 de dezembro de 1993 relativa à celebração do Acordo sobre o Espaço Económico Europeu entre as Comunidades Europeias, os seus Estados-membros e a República da Áustria, a República da Finlândia, a República da Islândia, o Principado do Liechtenstein, o Reino da Noruega, o Reino da Suécia e a Confederação Suíça, disponível para consulta em http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L .1994.001.01.0003.01.ENG (17.03.2018).

[124] O Considerando 19.º estabelece que "*o estabelecimento no território de um Estado-membro pressupõe o exercício efetivo e real de uma atividade mediante uma instalação estável; que, para o efeito, a forma jurídica de tal estabelecimento, quer se trate de uma simples sucursal ou de uma filial com personalidade jurídica, não é determinante; que, quando no território de vários Estados-membros estiver estabelecido um único responsável pelo tratamento, em especial através de uma filial, deverá assegurar, nomeadamente para evitar que a legislação seja contornada, que cada um dos estabelecimentos cumpra as obrigações impostas pela legislação nacional aplicável às respetivas atividades*".

ou não, situados no território desse Estado-membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade."

Ora, da disposição acima transcrita resulta que «*(i) é pretendida a aplicação de legislação de um Estado-membro aos tratamento efetuados no âmbito da União; (ii) a fixidez da regra do país do estabelecimento não pode ser invocada para "iludir" as obrigações provenientes para particulares e entidades privadas decorrentes de outras disposições da diretiva*»[125]. Estas conclusões levantavam dificuldades nos casos em que o tratamento não se processasse apenas em um Estado-membro pois, nos casos de tratamentos plurilocalizados, haveria a obrigatoriedade de cumprimento de todas disposições de proteção de dados que estivessem em vigor nos Estados-Membros em questão[126].

A Diretiva 95/46/CE assumiu um modelo de controlo administrativo prévio em relação aos tratamentos de dados que apresentam maiores riscos para o direito à proteção de dados pessoais. Este foi o modelo "*consagrado na generalidade dos diplomas legais que procederam à sua transposição para a ordem jurídica dos Estados membros da União Europeia – veja-se o artigo 20.º da Diretiva. Nos restantes tratamentos de dados pessoais, dotados portanto de menor risco para os direitos e liberdades, a Diretiva traça o caminho preferencial do controlo a posteriori pela autoridade administrativa dos tratamentos de dados (v. considerando 52), apenas admitindo como regra a notificação prévia dos mesmos à autoridade administrativa de controlo, com o objetivo, assumido no considerando 48, de assegurar a publicidade das finalidades e principais características do tratamento*"[127].

Considerando que a Diretiva 95/46/CE foi revogada pelo RGPD, não nos iremos alongar sobre aquele diploma, que será analisado por referência aquando da análise do RGPD. Nesse sentido, deixamos de seguida apenas algumas considerações específicas a ter em conta.

---

[125] PINHEIRO, Alexandre Sousa, op. cit., p. 620.

[126] No "Primeiro relatório sobre a implementação da Diretiva relativa à proteção de dados" pode ler-se que "*a implementação desta disposição é deficiente em diversos casos, permitindo a manifestação do tipo de conflitos que o artigo mencionado pretende evitar*." O relatório está disponível para consulta em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14012 (17.03.2018).

[127] CALVÃO, Filipa - **O modelo de supervisão de tratamentos de dados pessoais na União Europeia: da atual diretiva ao futuro regulamento**, in *Forum de Proteção de Dados*, n.º 1, julho. 2015, pp. 37.

Quando uma pessoa - singular ou coletiva- pretendesse levar a cabo uma atividade que envolvesse tratamento de dados pessoais, aplicar-se-ia um sistema de notificação para efeito de registo ("comunicação prévia sem prazo") no que se refere a tratamentos de dados que acarretassem menor risco, "*e em casos de maior risco, por incidir sobre dados pessoais sensíveis ou pelo contexto ou dimensão do tratamento, um sistema de controlo administrativo prévio, a realizar pela autoridade de controlo nacional*"[128].

Em relação às situações de maior risco para a privacidade – nomeadamente as que se referem a dados sensíveis, parte-se da proibição do tratamento dos mesmos, mas admitindo a lei que a proibição possa ser afastada mediante autorização ("proibição com reserva de autorização"[129]).

A Diretiva de Proteção de Dados deu corpo aos princípios do direito à privacidade já consagrados na Convenção 108 do Conselho da Europa e, como esta Convenção também o fizera, previu um conjunto de direitos inerentes à proteção de dados, tais como o direito de informação, o direito de acesso e direito de oposição.

Os artigos 10.º e 11.º elencam a informação que deve ser prestada ao titular dos dados aquando da recolha dos dados, sendo que esta informação varia consoante os dados sejam recolhidos diretamente do titular ou indiretamente. O rol de informação a ser prestada inclui a identidade do responsável pelo tratamento e do seu representante, conforme aplicável; as finalidades do tratamento a que os dados se destinam; e outra informação, tais como os destinatários ou categorias de destinatários dos dados, o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder, a existência do direito de acesso aos dados que lhe digam respeito e do direito de os retificar.

O direito de acesso vem previsto no artigo 12.º da Diretiva e garante ao titular dos dados o direito de aceder aos dados que lhe digam respeito, podendo obter "*a confirmação de terem ou não sido tratados dados que lhes digam respeito, e*

[128] CALVÃO, Filipa, «O modelo de supervisão de tratamentos de dados pessoais na União Europeia: da atual diretiva ao futuro regulamento», in *Forum de Proteção de Dados*, n.º 1, julho. 2015, pp. 38.
[129] Sobre a proibição com reserva de autorização, ver Pedro Costa Gonçalves, Reflexões sobre o Estado Regulador e o Estado Contratante, Direito Público e Regulação 8, Cedipre, Coimbra Editora, Coimbra 2013, pp. 146—148.

informações pelo menos sobre os fins a que se destina esse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados, a comunicação, sob forma inteligível, dos dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem dos dados, o conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito, pelo menos no que se refere às decisões automatizadas referidas no nº 1 do artigo 15º".

Nos termos do artigo 14º, a Diretiva obrigava os Estados-membros a reconhecer à pessoa em causa o direito de:

a. Pelo menos nos casos de tratamentos necessários para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados e tratamentos necessários para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, se opor em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objeto de tratamento, salvo disposição em contrário do direito nacional. Em caso de oposição justificada, o tratamento efetuado pelo responsável deixa de poder incidir sobre esses dados;
b. Se opor, a seu pedido e gratuitamente, ao tratamento dos dados pessoais que lhe digam respeito previsto pelo responsável pelo tratamento para efeitos de mala direta; ou ser informada antes de os dados pessoais serem comunicados pela primeira vez a terceiros para fins de mala direta ou utilizados por conta de terceiros, e de lhe ser expressamente facultado o direito de se opor, sem despesas, a tais comunicações ou utilizações. [130]

Em relação aos fluxos transfronteiriços de dados[131], o número 1 do artigo 25.º, n.º 1, da Diretiva de Proteção de Dados regulava a "*transferência para um país terceiro*

[130] Este direito funciona como uma "*limitação às consequências não consentidas expressamente na recolha de dados pessoais*". GONÇALVES, Maria Eduarda – "A Proteção de Dados Pessoais em Direito Internacional e em Direito Interno", **Revista do Ministério Público**, ano 10, n.º 40, 1989, p. 101 *apud* PINHEIRO, Alexandre Sousa, op. cit.,p. 660.
[131] O TJUE tem feito uma interpretação restritiva do conceito de fluxos transfronteiriços, considerando que a mera publicação on-line de dados pessoais não deve ser considerada um fluxo

de dados pessoais objeto de tratamento, ou que se destinem a ser objeto de tratamento após a sua transferência [...]", prevendo o livre fluxo de dados entre os Estados-Membros, pois os "níveis de proteção adequados" ficam assegurados com a transposição da própria Diretiva para a legislação nacional[132].

Em conformidade, a transferência de dados pessoais para países terceiros não estava proibida e nem sujeita a restrições nos termos da legislação nacional sobre proteção de dados se tivesse sido apurado que o destinatário possuía um nível adequado de proteção de dados[133] ou se transferência fosse necessária tendo em conta os interesses específicos da pessoa em causa ou os interesses superiores legítimos de terceiros, especialmente interesses públicos relevantes.

A opção por um critério de exigência de adequação, e não de equivalência, permitiu o reconhecimento de vários sistemas de proteção dos dados. Segundo o disposto no número 6 do artigo 25.º da Diretiva, a Comissão Europeia era competente para

---

transfronteiriço de dados. O TJUE aplica o mesmo critério aos registos públicos e aos meios de comunicação social online, tais como os jornais eletrónicos e a televisão. Apenas a comunicação dirigida a destinatários específicos está abrangida pelo conceito de «fluxo transfronteiriço de dados».
Sobre isto, ver o Acórdão Bodil Lindqvist, no TJUE considerou que «a referência, feita numa página da Internet, a várias pessoas e a sua identificação pelo nome ou por outros meios, por exemplo, o número de telefone ou informações relativas às suas condições de trabalho e aos seus passatempos constitui um "tratamento de dados pessoais por meios total ou parcialmente automatizados" na aceção do artigo 3.º, n.º 1, da Diretiva 95/46.». Contudo, o TJUE defende, tendo em conta, por um lado, o estado de evolução da Internet à data da elaboração da diretiva e, por outro, a ausência, na Diretiva, de critérios aplicáveis à utilização da Internet, «*não se pode presumir que o legislador comunitário tinha a intenção de incluir prospectivamente no conceito de "transferência para um país terceiro de dados" a inserção [...] de dados numa página Internet, mesmo que estes se tornem deste modo acessíveis às pessoas de países terceiros que possuam os meios técnicos para acederem a esses dados.*» Caso assim não fosse, ou seja, se a Diretiva fosse «*interpretada no sentido de que existe uma "transferência para um país terceiro de dados" cada vez que são carregados dados de caráter pessoal numa página Internet, essa transferência seria necessariamente uma transferência para todos os países terceiros onde existem os meios técnicos necessários para aceder à Internet. O regime especial previsto [na Diretiva] tornar-se-ia, necessariamente, no que respeita às operações na Internet, um regime de aplicação geral. Com efeito, desde que a Comissão verificasse [...] que um país terceiro não assegura um nível de proteção adequado, os Estados-Membros seriam obrigados a impedir qualquer colocação na Internet de dados de caráter pessoal.*» Este acórdão pode ser consultado em http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=9409 (17.03.2018).

[132] PINHEIRO, Alexandre Sousa, op. cit., p. 627.

[133] Para a avaliação da adequação do sistema de proteção de dados de um determinado país, o número 2 do artigo 25.º da Diretiva dispõe que serão utlizadas como critério *"todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projetados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país*". Em conformidade, a análise não deve ser abstrata. PINHEIRO, Alexandre Sousa, op. cit., p. 628.

apreciar o nível de proteção de dados em países estrangeiros[134] [135] e, para este efeito, consultava o Grupo de Trabalho do artigo 29.º[136], que deu um contributo substancial para a interpretação dos artigos 25.º e 26.º[137].

Importa notar que a Diretiva estabelecia uma obrigatoriedade segundo a qual "*Cada Estado-membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adotadas pelos Estados-membros nos termos da presente diretiva. Essas autoridades exercerão com total independência as funções que lhes forem atribuídas*." O estabelecimento destas autoridades de controlo independentes funcionou como meio de melhorar o cumprimento das regras sobre proteção de dados e revelou-se um importante contributo para a aplicação eficaz da legislação europeia sobre proteção de dados[138].

---

[134] A constatação de um nível adequado de proteção pela Comissão Europeia tinha efeito vinculativo. Se a Comissão Europeia publicasse uma constatação de um nível adequado de proteção relativamente a um determinado país no Jornal Oficial da União Europeia, todos os países membros do EEE e os respetivos órgãos estavam vinculados por essa decisão, o que significa que o fluxo de dados para esse país não estaria sujeito a procedimentos de controlo ou autorização perante as autoridades nacionais.

[135] Para uma lista continuamente atualizada de países que foram objeto de uma constatação de um nível de proteção adequado, consultar a página inicial da Comissão Europeia, Direção Geral da Justiça, disponível em: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[136] O grupo de trabalho foi instituído pelo artigo 29.º da Diretiva 95/46/CE e é um órgão europeu independente, com carácter consultivo em matéria de proteção de dados e privacidade. As suas atribuições são definidas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE. A partir de maio de 2018 e com a entrada em vigor do RGPD, o Grupo de Trabalho do artigo 29.º da Diretiva 95/46/CE foi substituído pelo Comité Europeu para a Proteção de Dados. O Comité deverá ser um órgão independente da União, dotado de personalidade jurídica (cf. artigos 68.º e ss do RGPD).

[137] Sobre esta matéria, ver:

- Grupo de Trabalho do artigo 29.º (2003) - **Documento de trabalho sobre as transferências de dados pessoais para países terceiros: a aplicação do artigo 26.º, n.º 2, da Diretiva Proteção de Dados da UE a regras vinculativas para as empresas em matéria de transferências internacionais de dados**, WP 74, Bruxelas, 3 de junho de 2003;
- Grupo de Trabalho do artigo 29.º (2005) - **Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995**, WP 114, Bruxelas, 25 de novembro de 2005.

[138] De igual modo, o Conselho da Europa também introduziu este elemento na Convenção 108, através do Protocolo Adicional à Convenção 108, que determina que "*cada Parte deverá designar uma ou mais autoridades responsáveis por assegurar o cumprimento das medidas que aplicam, no seu direito interno, os princípios enunciados nos capítulos II e III da Convenção e no presente Protocolo*". Este protocolo está disponível para consulta em http://direitoshumanos.gddc.pt/3_18/IIIPAG3_18_3.htm (17.03.2018).

Outros instrumentos

No seguimento e na sequência da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e nos seus termos, a Comissão aprovou a Decisão 2000/520/CE, de 26 de Julho, relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas "questões mais frequentes" (FAQ) emitidos pelo *Department of Commerce dos Estados Unidos da América.*[139]. Este acordo visava compatibilizar a legislação sectorial e a autorregulação norte-americanas com a legislação europeia em matéria de proteção de dados.

Uma vez que a Diretiva de Proteção de Dados só podia ter por destinatários os Estados Membros da UE, era necessário aprovar outro instrumento jurídico que assegurasse a proteção de dados nos casos de tratamento de dados pessoais pelas instituições e órgãos da UE. O Regulamento do Parlamento Europeu e da Comissão Europeia n.º 45/2001 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados desempenha esta função[140]. Além disso, mesmo em áreas abrangidas pela Diretiva de Proteção de Dados, surge muitas vezes a necessidade de estabelecer disposições mais detalhadas em matéria de proteção de dados para assegurar a necessária clareza na conciliação com outros interesses legítimos. É neste contexto que foram aprovadas a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas[141] e a Diretiva 2006/24/CE relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes

[139] Esta Decisão foi aprovada em 2000 e ficou conhecida vulgarmente conhecida como *Acordo de Safe Harbor.* Ao abrigo deste acordo, as entidades com sede nos EUA declararam cumprir as regras relativa à proteção dos dados pessoais estabelecidas através da legislação comunitária, ficando então fundamentadas as operações de transferência de dados de entidades que operam nas duas jurisdições. Note-se que esta Decisão foi considerada inválida pelo TJUE em Outubro de 2015, com fundamento, por um lado, na violação de direitos fundamentais no tratamento de dados pessoais realizado pelos EUA e, por outro lado, no esvaziamento dos poderes das entidades de controlo nacionais que a decisão promove, inibindo-as de investigar as demais queixas com independência. TJUE, Caso Schrems, processo C-362/14, disponível para ser consultado em http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=28904 (17.03.2018).

[140] Este regulamento está disponível para consulta em http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001R0045 (17.03.2018)

[141] Este regulamento está disponível para consulta http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058 (17.03.2018)

públicas de comunicações (Diretiva da Conservação de Dados, invalidada em 8 de abril de 2014)[142], e que altera a Diretiva 2002/58/ CE.

A Carta dos Direitos Fundamentais da União Europeia e o Tratado de Lisboa

Os tratados originais das Comunidades Europeias não continham qualquer referência ao direito à privacidade ou à proteção de dados. Na verdade, a única referência menção à proteção de dados era feita por referência à Autoridade de Supervisão na área da proteção de dados[143]. Foi, contudo, em consequência da jurisprudência do então Tribunal de Justiça das Comunidades Europeias (TJCE), no âmbito de processos instaurados com fundamento em alegadas violações dos direitos humanos no âmbito da legislação da UE, que se desenvolveu uma nova abordagem relativa à proteção de dados: evolui-se no "sentido da distinção entre a "vida privada" e a "proteção de dados", permitindo a aplicação da Convenção 108" e das suas disposições[144].

Reconhecendo a necessidade de garantir níveis semelhantes da proteção dos direitos humanos e num esforço para aproximar os cidadãos da União, a União Europeia proclamou, em 2000, a Carta dos Direitos Fundamentais da União

[142] O Tribunal de Justiça da União Europeia declarou inválida a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, ao considerar que a Diretiva 2006/24/CE implicava uma invasão desproporcional na vida privada dos cidadãos utilizadores de meios de comunicação eletrónica, violando direitos fundamentais ao respeito pela vida privada e à proteção de dados pessoais. Esta conclusão teve como fundamento o facto de a Diretiva ser aplicável a todos os indivíduos, todos os meios de comunicação eletrónica e todos os dados de tráfego, sem qualquer diferenciação; não conter critérios objetivos de acesso aos dados pelas autoridades nacionais competentes e para a estipulação dos prazos máximo e mínimo de conservação dos dados. Adicionalmente, a Diretiva não oferecia salvaguardas suficientes contra eventuais abusos, não assegurava a destruição irreversível dos dados, findo o prazo de conservação e não impunha que os dados sejam conservados no território da União.
Esta diretiva está disponível para consulta em http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32006L0024 (17.03.2018).
[143] No artigo 286.º do Tratado da Comunidade Europeia pode ler-se que "*A partir de 1 de Janeiro de 1999, os atos comunitários relativos à proteção das pessoas singulares em matéria de tratamento de dados de carácter pessoal e de livre circulação desses dados são aplicáveis às instituições e órgãos instituídos pelo presente Tratado, ou com base nele. 2. Antes da data prevista no n.º 1, o Conselho, deliberando nos termos do artigo 251.º, deve criar um órgão independente de supervisão, incumbido de fiscalizar a aplicação dos citados atos comunitários às instituições e órgãos da Comunidade e adotar as demais disposições que se afigurem adequada*."
[144] PINHEIRO, Alexandre Sousa, op. cit., p. 662.

Europeia[145]. Esta Carta incorpora direitos civis, políticos, económicos e sociais dos cidadãos europeus, sintetizando as tradições constitucionais e as obrigações internacionais comuns aos Estados-Membros. Os direitos fundamentais reconhecidos na Carta estão divididos em seis secções: dignidade, liberdades, igualdade, solidariedade, cidadania e justiça.

É no artigo 8.º que encontramos o direito à proteção de dados, no qual pode ler-se que "*1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.*

2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."

As instituições da UE e os Estados-Membros têm o dever de observar e garantir este direito à proteção de dados, que também é aplicável aos Estados-Membros quando aplicam o direito da União[146]. Note-se que, tendo sido formulado cinco anos após a adoção da Diretiva de Proteção de Dados, o artigo 8.º da Carta deve ser interpretado no sentido de incorporar a legislação da UE sobre proteção de dados preexistente. Por conseguinte, a Carta não apenas menciona expressamente o direito à proteção de dados no número 1 do artigo 8.º, n.º 1, como também faz referência a princípios fundamentais da proteção de dados no número 2 do mesmo artigo 8.º.

---

[145] Embora originalmente a Carta não fosse mais do que um documento meramente político, a Carta passou a ser juridicamente vinculativa como direito primário da UE com a entrada em vigor do Tratado de Lisboa em 1 de dezembro de 2009. Nos termos do disposto no número 1 do artigo 6.º do TUE, "*A União reconhece os direitos, as liberdades e os princípios enunciados na Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, com as adaptações que lhe foram introduzidas em 12 de dezembro de 2007, em Estrasburgo, e que tem o mesmo valor jurídico que os Tratados.*"
A Carta pode ser consultada em http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[146] Nos termos do disposto no número 1 do artigo 51.º da Carta, "As disposições da presente Carta têm por destinatários as instituições, órgãos e organismos da União, na observância do princípio da subsidiariedade, bem como os Estados-Membros, apenas quando apliquem o direito da União. Assim sendo, devem respeitar os direitos, observar os princípios e promover a sua aplicação, de acordo com as respetivas competências e observando os limites das competências conferidas à União pelos Tratados."

Por fim, o direito primário da UE passou também a reconhecer o direito à proteção de dados e atribuiu à UE competência genérica para legislar sobre matérias relacionadas com a proteção de dados. No seu artigo 16.º, o Tratado sobre o Funcionamento da União Europeia estabelece que "*todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito*" e a competência para aprovar as regras relativas à proteção de dados das pessoas singulares no que diz respeito ao tratamento de dados pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados recai sobre "*Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário".*[147]

Note-se que ao abrigo do número 2 do artigo 16.º, as normas que forem adotas pelo Parlamento e pelo Conselho não prejudicam as normas específicas previstas no artigo 39.º do Tratado da União Europeia.

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

Conceitos e âmbito de aplicação

O 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) foi publicado no Jornal Oficial da União Europeia em 4 de maio de 2016. A sua entrada em vigor ocorreu no vigésimo dia seguinte ao da sua publicação (24 de maio de 2016).

O RGPD é obrigatório em todos os seus elementos e é diretamente aplicável em todos os Estados-Membros da União Europeia desde 25 de maio de 2018, sem

[147] Sobre o impacto do Tratado de Lisboa na proteção de dados, ver HUSTINX, Peter – **Data protection in the Light of the Lisbon Treaty and the Consequences for Present Regulations**, disponível em http://www.law.uni-sofia.bg/Kat/T/IP/T/ZLD/DocLib/2009%20-%20Data%20protection%20in%20the%20light%20of%20the%20Lisbon%20Treaty%20and%20the%20consequences%20for%20present%20regulations.pdf (17.03.2018)

necessidade de qualquer ato interno de transposição ou receção, com exceção de algumas áreas que expressamente identifica (designadamente a possibilidade de os Estados-Membros limitarem o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º do RGPD, e no que diz respeito ao regime sancionatório previsto nos artigos 85.º a 91.º).

O objetivo principal do RGPD é o de conferir eficácia à proteção de dados em todo o espaço da União Europeia, procurando harmonizar as diversas legislações nacionais e favorecer a concorrência, pretendendo, ao mesmo tempo, atualizar as regras comunitárias que estavam em vigor desde 1995 e já se encontravam obsoletas e desadequadas a muitos dos desafios que a proteção de dados agora enfrenta, com a utilização das redes sociais, da computação em nuvem, nos serviços baseados em localização e cartões inteligentes. Por outro lado, apesar da Diretiva Proteção de Dados garantir "*uma proteção efetiva do direito fundamental à proteção de dados (...) as diferenças na forma como cada Estado-Membro implementa a lei levaram a inconsistências, que criam complexidade, incerteza jurídica e custos administrativos. Isso afeta a confiança dos indivíduos e a competitividade da economia da UE.*"[148]

O RGPD constitui o elemento fundamental do pacote legislativo apresentado pela Comissão, que incluiu também a Diretiva (EU) 2016/680 do Parlamento e do Conselho, também de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho).

Sem prejuízo de legislação específica, o Regulamento Geral sobre a Proteção de Dados aplica-se transversalmente a todos os sectores de atividade, sem prejuízo da existência de legislação específica.

O âmbito de aplicação material do Regulamento vem definido no seu artigo 2.º, o

[148] Comissão Europeia – **Comunicado de imprensa da Comissão Europeia**, de 21 Dezembro de 2015, disponível para consulta em http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (17.03.2018)

qual determina, no seu n.º 1, que o Regulamento é aplicável ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como aos tratamentos por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

O RGPD estabelece também a lista de definições aplicáveis, da qual resulta que o conceito de dados pessoais respeita apenas a informações relativas pessoas singulares identificadas ou identificáveis, ou seja, que possam ser identificadas, direta ou indiretamente, em especial por referência a um identificador tal como o nome, número de identificação, dados de localização ou outros elementos (cf. número 1 do artigo 4.º). De igual modo, o RGPD estabelece que o conceito de tratamento abrange uma diversidade de operações (ou conjunto de operações) envolvendo dados pessoais (ou sobre conjuntos de dados pessoais), tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição, quer sejam efetuadas por meios automatizados ou não automatizados (cf. número 2 do artigo 4.º).
Do âmbito de aplicação do RGPD continua a estar excluído, tal como estava na Diretiva 95/46/CE, [149], o tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas (i.e. sem qualquer ligação com uma atividade profissional ou comercial), embora se deva entender que as normas sejam aplicáveis aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas. Outras exclusões do âmbito de aplicação material do RGPD são as exclusões de tratamento de dados pessoais:

a. Efetuado no exercício de atividades não sujeitas à aplicação do direito da União:
b. Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2 do TUE (nomeadamente atividades relativas à política externa e de segurança comum);
c. Efetuado pelas autoridades competentes para efeitos de prevenção,

[149] Esta exclusão vinha prevista no número 2 do artigo 3.º da Diretiva.

investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, ao qual é aplicada a Diretiva (EU) 2016/680 do Parlamento e do Conselho, também de 27 de abril de 2016.

O Regulamento tem um âmbito de aplicação territorial mais vasto do que o que resultava das disposições nacionais transpostas pela Diretiva que por ele foi revogada.

Em primeiro lugar, as disposições do RGPD são aplicáveis ao tratamento de dados pessoais efetuados no contexto das atividades de um estabelecimento situado no território da União Europeia, independentemente de o tratamento efetivo ocorrer dentro ou fora do território da União (cf. número 1 do artigo 3.º)[150].

Para além disso, o RGPD é aplicável às atividades de tratamento de dados desenvolvidas por responsável ou subcontratante que não estejam estabelecidos na União Europeia, quando estejam em causa atividades de tratamento de dados pessoais de titulares residentes no território da União Europeia que envolvam qualquer das situações seguintes:

- A oferta de bens ou serviços a esses titulares na União Europeia, independentemente de haver ou não pagamento (cf. número 2 do artigo 3.º, alínea a))[151].; ou
- o controlo do comportamento de residentes no território da União Europeia que tenha lugar na União (cf. número 2 do artigo 3.º, alínea b))[152].

Por último, o Regulamento também é aplicável ao tratamento de dados pessoais por um responsável que não esteja estabelecido em território da União Europeia, desde que o direito de um Estado-Membro seja aplicável ao local onde ocorra o tratamento por força do direito internacional público (cf. número 3 do artigo 3.º).[153]

Alguns dos principais conceitos a ter em conta podem ser definidos, à luz do disposto no artigo 4.º do Regulamento Geral sobre Proteção de Dados Pessoais do

[150] Ver também Considerando (22).
[151] Ver também Considerando (23).
[152] Ver também Considerando (24).
[153] Ver também Considerando (25).

modo seguinte:

- Autoridade de controlo: a Autoridade que em cada país da União Europeia seja responsável por regular, fiscalizar o tratamento de dados pessoais e a sua proteção e sancionar o incumprimento dos princípios e regras decorrentes do RGPD, nos termos do artigo 51.º (cf. número 21 do artigo 4.º);
- Estabelecimento principal: No que se refere a um responsável pelo tratamento com estabelecimentos em vários Estados-Membros, o local onde se encontra a sua administração central na União, a menos que as decisões sobre as finalidades e os meios de tratamento dos dados pessoais sejam tomadas noutro estabelecimento do responsável pelo tratamento na União e este último estabelecimento tenha competência para mandar executar tais decisões, sendo neste caso o estabelecimento que tiver tomado as referidas decisões considerado estabelecimento principal. No que se refere a um subcontratante com estabelecimentos em vários Estados-Membros, o local onde se encontra a sua administração central na União ou, caso o subcontratante não tenha administração central na União, o estabelecimento do subcontratante na União onde são exercidas as principais atividades de tratamento no contexto das atividades de um estabelecimento do subcontratante, na medida em que se encontre sujeito a obrigações específicas nos termos do RGPD (cf. número 16 do artigo 4.º);
- 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 (cf. número 7 do artigo 4.º);
- Subcontratante: a pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes (cf. número 8 do artigo 4.º);
- Tratamento transfronteiriço: O tratamento de dados pessoais que ocorre no contexto das atividades de estabelecimentos em mais do que um Estado-Membro de um responsável pelo tratamento ou um subcontratante na União, caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que um Estado-Membro. Reporta-se também ao tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de

um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estados-Membro (cf. número 23 do artigo 4.º);

- Violação de dados pessoais: uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento (cf. número 12 do artigo 4.º).

Os princípios do RGPD

O novo Regulamento de Proteção de Dados assenta em sete princípios fundamentais que têm por objetivo proteger a privacidade dos cidadãos da UE e que devem orientar os procedimentos das organizações. Nos termos do artigo 5.º, o tratamento de dados deve obedecer aos seguintes princípios:

- Licitude, lealdade e transparência: os dados pessoais devem ser tratados de forma lícita, totalmente transparente e leal perante os seus titulares (cf. número 1 do artigo 5.º, alínea a));
- Limitação das finalidades: os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades (cf. número 1 do artigo 5.º, alínea b))[154];
- Minimização dos dados: os dados objeto de tratamento devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (cf. número 1 do artigo 5.º, alínea c));
- Exatidão: os dados recolhidos devem ser sempre exatos e atualizados ao longo de todo o tratamento dos mesmos. Devem ser adotadas medidas para garantir que os dados inexatos são apagados ou corrigidos (cf. número 1 do artigo 5.º, alínea d));
- Limitação do período de conservação: os dados só podem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados (cf.

[154] Nos termos daquela disposição "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."

número 1 do artigo 5.º, alínea e))[155];

- Integridade e confidencialidade: o tratamento dos dados deve garantir a segurança dos mesmos, devendo ser adotadas as medidas técnicas ou organizativas adequadas a garantir a proteção contra o tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental (cf. número 1 do artigo 5.º, alínea f));
- Responsabilidade: os responsáveis pelo tratamento são responsáveis pelo cumprimento das normas do RGPD (cf. número 2 do artigo 5.º).

Alteração do paradigma das obrigações de notificação prévia à luz do regime do RGPD

O RGPD estabelece a passagem de um paradigma essencialmente de hétero-regulação (com notificação ou autorização prévias de praticamente todos os tratamentos pela Autoridade de Controlo) para um paradigma de autorregulação, com mais obrigações e maior responsabilidade para os responsáveis pelo tratamento de dados pessoais.

Ao abrigo do RGDP, o tratamento de dados deixou de ser sujeito a supervisão prévia, com exceção das situações abaixo apresentadas. O responsável pelo tratamento deixou de ter o dever universalmente aplicável de notificar previamente a Autoridade de Controlo da realização de um tratamento ou conjunto de tratamentos.

O número 1 do artigo 36.º do RGPD estabelece que o responsável pelo tratamento deve consultar a autoridade de controlo antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco[156]. Sempre que considerar que o tratamento em causa violaria o disposto no RGPD, nomeadamente se o responsável pelo

[155] O RGPD prevê, no entanto que ficam excecionados os dados pessoais tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, sujeitos à aplicação das medidas técnicas e organizativas adequadas. Estes dados podem ser conservados durante períodos mais longos.
[156] Nesse sentido, cf. Considerando (89).

tratamento não tiver identificado ou atenuado suficientemente os riscos, a autoridade de controlo, no prazo máximo de oito semanas a contar da receção do pedido de consulta (prorrogável até seis semanas, tendo em conta a complexidade do tratamento previsto), deverá dar orientações, por escrito, ao responsável pelo tratamento e, se o houver, ao subcontratante (cf. artigo 36./2 do RGPD).

Licitude do tratamento e reforço de direitos dos titulares dos dados

O Regulamento vem aumentar o leque de direitos dos titulares dos dados já anteriormente previstos na Diretiva 95/46/CE, bem como a relevância e as exigências de consentimento para o tratamento dos seus dados quando seja essa a causa que legitima o tratamento.

O consentimento do titular dos dados (isto é, a manifestação de vontade livre, específica, informada e explícita, através da qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, – lógica de *opt-in* - que os dados pessoais que lhe dizem respeito sejam objeto de tratamento, conforme definido pelo número 11 do artigo 4.º) é a principal fonte de legitimidade para tratamento dos dados pessoais[157].

Sempre que o tratamento seja realizado com base no consentimento, o responsável tem de estar em condições de demonstrar que obteve o necessário consentimento do titular (e que o obteve nos termos legalmente exigíveis) sem o que não poderá proceder ao tratamento dos dados em causa (cf. número 1 do artigo 7.º).

Nos termos do número 2 do artigo 7.º, são condições de validade do consentimento

[157] Nesse sentido, o Considerando (32) dispõe que "*o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido*."

que este tenha sido apresentado de uma forma que o distinga claramente desses outros assuntos de modo, quando for prestado no contexto de uma declaração escrita que diga também respeito a outros assuntos, inteligível e de fácil acesso e numa linguagem clara e simples.[158]

Ao titular dos dados é conferido o direito de retirar o consentimento em qualquer altura, devendo garantir-se que o consentimento seja tão fácil de retirar quanto de dar, designadamente através do mesmo meio em que o consentimento foi prestado (cf. número 3 do artigo 7.º). O titular dos dados deve também ser inicialmente informado desta possibilidade de retirada de consentimento e do facto de tal retirada do consentimento não comprometer a licitude do tratamento efetuado com base no consentimento previamente dado.

Além do consentimento, o RGPD estabelece, no número 1 do artigo 6.º, outros fundamentos para a licitude do tratamento. Tais fundamentos, aos quais se acresce o consentimento já anteriormente abordado, são os seguintes:

- O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados (cf. número 1 do artigo 6.º, alínea b);
- O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito (cf. número 1 do artigo 6.º, alínea c));
- O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular (cf. número 1 do artigo 6.º, alínea d));
- O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento (cf. número 1 do artigo 6.º, alínea e));

---

[158] "*Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance. Em conformidade com a Diretiva 93/13/CEE do Conselho (1), uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado*." Cf. Considerando (42).

- O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança (cf. número 1 do artigo 6.º, alínea f)). Fica excluído deste âmbito o tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.

Adicionalmente, o RGPD confere discricionariedade legislativa aos Estados-Membros, permitindo que estes mantenham ou aprovem disposições mais específicas com o objetivo de adaptar a aplicação das regras do regulamento no que diz respeito ao tratamento de dados para o cumprimento do número 1, alíneas c) e e), determinando, de forma mais precisa, requisitos específicos para o tratamento e outras medidas destinadas a garantir a licitude e lealdade do tratamento, inclusive para outras situações específicas de tratamento (cf. número 2 do artigo 6.º).

O RGPD veio alargar o elenco dos direitos conferidos aos titulares dos dados. Adicionalmente aos direitos já anteriormente previstos na Diretiva 95/46/CE, tais como direito à informação[159], o direito de acesso[160] e direito de oposição[161] e

---

[159] O RGPD determina a obrigação de prestar informações ao titular dos dados. O número 1 do artigo 13.º determina que "*quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, aquando da recolha desses dados pessoais, as seguintes informações:*
a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
b) Os contactos do encarregado da proteção de dados, se for caso disso;
c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;
e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.o ou 47.º, ou no artigo 49.º, n.º 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas."
O responsável pelo tratamento deve fornece ao titular informações adicionais, necessárias para garantir um tratamento equitativo e transparente, nomeadamente:
"*a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;*
b) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;

retificação[162], o RGPD confere ao titular dos dados o direito a que, em determinadas circunstâncias, os seus dados pessoais sejam definitivamente eliminados pelos responsáveis pelo tratamento – *direito a ser esquecido* - e o direito a que o responsável pelo tratamento lhe forneça num formato estruturado, de uso corrente e de leitura automática os dados pessoais que lhe digam respeito, consagrado como direito à portabilidade.

---

c) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea a), ou no artigo 9.º n.º 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
d) O direito de apresentar reclamação a uma autoridade de controlo;
e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;
f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados." (cf. número 2 do artigo 13.º).
O responsável pelo tratamento também deve cumprir os requisitos da prestação de informação quando a recolha não seja efetuada junto do titular dos dados (cf. artigo 14.º).

[160] Nos termos do número 1 do artigo 15.º, "*o titular dos dados tem 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 e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:*
a) As finalidades do tratamento dos dados;
b) As categorias dos dados pessoais em questão;
c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;
d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;
e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;
f) O direito de apresentar reclamação a uma autoridade de controlo;
g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;
h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados."

[161] De acordo com o disposto no artigo 21.º, "*o titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.º, n.º 1, alínea e) ou f), ou no artigo 6.º, n.º 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.*
Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta." (cf. números 1 e 2 do artigo 21.º).

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

O direito a ser esquecido foi previamente reconhecido no Acórdão do Tribunal de Justiça (Grande Seção) de 13 de maio de 2014, e ficou conhecido como o acórdão Google Spain[163]. Na sequência da jurisprudência ali firmada, é reconhecido aos titulares dos dados o direito ao apagamento dos seus dados por parte do responsável pelo tratamento. Caso os dados forem públicos, o responsável pelo tratamento deve informar os restantes responsáveis pelo tratamento que o titular dos dados em causa requereu o apagamento das ligações para esses dados e das cópias e reproduções dos mesmos, tomando as medidas razoáveis para o efeito.

Este direito ficou consagrado no artigo 17.º do RGDP, nos termos do qual o titular tem o direito de ser esquecido, quando se aplique um dos seguintes motivos:

"*a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;*

b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;

c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2;

d) Os dados pessoais foram tratados ilicitamente;

e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;

f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1."

Contudo, o número 3 do artigo 17.º estabelece que há exceções ao direito a ser esquecido, nomeadamente nos casos em que o tratamento se revele necessário:

"*a) Ao exercício da liberdade de expressão e de informação;*

b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;

---

[163] O acórdão pode ser consultado em http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT (13.03.2018).

c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.º, n.º 2, alíneas h) e i), bem como do artigo 9.º, n.º 3;
d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1, na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou
e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial."

O direito à portabilidade deve ser analisado por referência ao *Big Data*, "*prática de combinar gigantescos volumes de informação proveniente de diversas fontes e analisá-los, recorrendo frequentemente à inteligência artificial através de soluções de máquinas inteligentes*"[164]. O número 1 do artigo 20.º confere ao titular dos dados o direito a solicitar ao responsável pelo tratamento "*os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:*
a) O tratamento se basear no consentimento dado nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a), ou num contrato referido no artigo 6.º, n.º 1, alínea b); e
b) O tratamento for realizado por meios automatizados."

O RGPD ressalva também que o direito à portabilidade não prejudica o direito a ser esquecido (cf. número 3 do artigo 20.º).

O mecanismo do *one-stop-shop*

Ao abrigo da revogada Diretiva 95/46/CE e dos diplomas nacionais que a

---

[164] Buttarelli, Giovanni – **Inteligência Artificial, Robótica, Privacidade e Proteção de Dados**, in *Forum de Proteção de Dados*, n.º 4, julho, 2017, pp. 27.
Segundo este autor, "*Big Data refere-se ao crescimento exponencial quer na disponibilidade de informação quer na sua utilização automatizada; refere-se a conjuntos digitais gigantescos de dados detidos por empresas, governos e outras organizações de grande dimensão, que são extensivamente analisados (daí o nome: analytics) através de algoritmos computacionais (Parecer 3/2013 do Grupo de Trabalho do Artigo 29.º sobre o princípio da finalidade).*"

transpuseram, os operadores económicos viam-se obrigados a solicitar autorizações em cada Estado membro em cujo território pretendiam estabelecer-se ou realizar operações sobre dados sensíveis. Esta necessidade consubstanciava um entrave à livre circulação de bens, serviços e de capitais, e à liberdade de estabelecimento e de prestação de serviços dentro do espaço comunitário.

Adicionalmente, a transposição da Diretiva para os ordenamentos jurídicos dos Estados-Membros foi feita em termos bastante distintos, pelo que os regimes jurídicos da proteção de dados não apresentavam os mesmos níveis de proteção, o que funcionou como chamariz para o estabelecimento de grandes grupos económicos em determinados Estados-Membros, com a consequente perturbação da concorrência no espaço europeu e em prejuízo da tutela dos direitos fundamentais dos seus cidadãos.

O RGPD veio aprovar, nos termos do seu artigo 56.º, o *one-stop-shop,* um mecanismo de "balcão único" que permite concentrar numa única autoridade local a qualidade de entidade competente (Autoridade de Controlo Principal) para agir para agir relativamente ao tratamento transfronteiriço efetuado por determinado responsável pelo tratamento ou subcontratante.

Assim, embora o RGPD reconheça que cada Autoridade nacional de Controlo é competente para prosseguir as atribuições e exercer os poderes conferidos pelo regulamento no território do seu próprio Estado-Membro, introduz o conceito de Autoridade de Controlo Principal que passa a ser, relativamente a cada responsável ou subcontratante, a autoridade competente para agir como o único interlocutor desse mesmo responsável ou subcontratante no tratamento transfronteiriço de dados pessoais que o(s) mesmo(s) efectue(m).

A qualidade de Autoridade de Controlo Principal recai sobre a autoridade do território onde se encontra situado o estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante (*cf.* definição de *Estabelecimento Principal* supra*).*

Não obstante este princípio, por uma questão de garantia de acessibilidade dos titulares dos dados e em derrogação daquela regra, cada autoridade de controlo

mantém competência para tratar reclamações que lhe sejam apresentadas (ou lidar com eventuais violações das regras do regulamento) se a matéria em apreço afetar substancialmente titulares de dados apenas no seu Estado-Membro ou se a matéria em apreço estiver relacionada apenas com um estabelecimento que se situe no Estado-Membro da autoridade (diferente da Autoridade de Controlo Principal) (cf. número 2 do artigo 56.º).

As regras relativas à autoridade de controlo principal e ao *mecanismo de balcão único* (ou '*one-stop-shop*') não se aplicam quando o tratamento dos dados for efetuado por autoridades públicas ou organismos privados que atuem no interesse público. Nesses casos, a autoridade de controlo do Estado-Membro em que estiver estabelecida a indicada autoridade pública ou organismo privado é que será a única autoridade de controlo competente (cf. número 2 do artigo 55.º).

Privacy impact assessment **(avaliação de impacto sobre a proteção de dados)**

A avaliação de impacto sobre a proteção de dados (conhecida como '*privacy impact assessment*' ou '*PIA*') corresponde a uma avaliação prévia do impacto de um determinado conjunto de operações de tratamento previstas sobre a proteção de dados. Com esta avaliação pretende-se aferir ou determinar a origem, a natureza, a particularidade e a gravidade do risco de determinados tratamentos de dados pessoais para os direitos e liberdades dos respetivos titulares dos dados.[165]

O RGPD prevê, no seu artigo 35.º, que a avaliação de impacto deva ser realizada pelo responsável sempre que um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados a tratar.
O RGPD densificou aquela suscetibilidade através da indicação exemplificativa de três casos em que a realização de uma avaliação de impacto sobre a proteção de dados é obrigatória. Concretamente:

a. em caso de tratamento que implique uma avaliação sistemática, completa e

[165] Nesse sentido, cf. Considerando (84).

baseada em tratamento automatizado, de aspetos pessoais respeitantes aos titulares dos dados (incluindo a definição de perfis, *profiling*), com base nas quais se pretenda adotar decisões com efeitos jurídicos relativamente ao titular ou que a afetem significativamente de forma similar;

b. no caso de operações de tratamento em grande escala de dados sensíveis; ou

c. quando ocorra controlo sistemático de zonas acessíveis ao público em grande escala.

Prevê-se ainda, também numa perspetiva de densificação de conceitos, a possibilidade de elaboração e publicitação, pela(s) autoridade(s) de controlo, de uma lista dos tipos de operações de tratamento sujeitos ao requisito de *privacy impact assessment* (cf. número 5 do artigo 35.º do RGPD).

O número 7 do artigo 35.º estabelece o conteúdo mínima que a avaliação de impacto das operações de tratamento deve compreender, nomeadamente: *i)* uma descrição sistemática das operações de tratamento e a concretização das finalidades do tratamento; *ii)* uma avaliação da necessidade e da proporcionalidade das operações de tratamento em relação aos objetivos de tratamento pretendidos; *iii)* uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados; e *iv)* as medidas previstas para fazer face aos riscos identificados, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade entre o tratamento em análise e o RGPD.

A avaliação do impacto das operações de tratamento está prevista como operação prévia ao início do tratamento. Note-se que, nos termos do disposto no artigo 36.º, n.º 1, o responsável pelo tratamento deve consultar a autoridade de controlo antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco.

Privacy by design* e *privacy by default

Privacy by design e *privacy by default* são dois conceitos consagrados no Regulamento Geral sobre a Proteção de Dados relacionados com um modelo de tratamento e de proteção de dados (cf. artigo 25.º do RGDP). Estes conceitos traduzem-se em soluções tecnológicas destinadas à proteção de dados por predefinição e desde a conceção do produto ou serviço, permitindo que sejam criadas de raiz medidas de minimização de impacto e medidas de segurança nos produtos e serviços oferecidos desde a fase mais embrionária do seu desenvolvimento (*privacy by design)*, passando as definições de proteção da privacidade a ser a norma, por defeito, por exemplo, em redes sociais ou aplicações móveis (*privacy by default)*.

Os responsáveis pelo tratamento ficam obrigados a tratar os dados numa lógica de *privacy by design* e de minimização, de acordo com o contexto, o âmbito, as finalidades e os riscos do tratamento.

Uma das medidas técnicas previstas pelo RGDP é a pseudonimização (cf. número 1 do artigo 25.º). A pseudonimização corresponde ao «tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável» (cf. número 5 do artigo 5.º). Ora, esta técnica assume especial relevância na determinação da licitude de determinados dados, conforme abaixo melhor explicitado.

Obrigação de designar um *data protection officer* (encarregado da proteção de dados)

A figura do *data protection officer* já estava anteriormente prevista como possível na Diretiva (cf. n.º 2 do artigo 18.º). No entanto, com a entrada em vigor do Regulamento Geral de Proteção de Dados Pessoais, nos termos do artigo 37.º, os responsáveis pelo tratamento de dados e os subcontratantes passam a ter de

designar um encarregado da proteção de dados pessoais sempre que:

a. as suas atividades principais consistam em operações de tratamento de dados que pela sua natureza, âmbito ou finalidade impliquem um controlo regular e sistemático dos titulares dos dados;

b. as atividades principais do responsável consistam em operações de tratamento de dados sensíveis.

Sempre que o tratamento seja efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional também se impõe a nomeação de um encarregado da proteção de dados pessoais[166].

O encarregado da proteção de dados pode ser um elemento da entidade responsável pelo tratamento ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviço.

As funções do *Data Protection Officer,* previstas no artigo 39.º, passarão por controlar a conformidade do tratamento de dados com o Regulamento, cooperar com a Autoridade de Controlo e informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações. "*O delegado assume em boa medida as funções de controlo prévio e sucessivo que tradicionalmente eram da competência da autoridade administrativa (cf. artigo 37.º), constituindo a obrigação legal da sua criação uma expressiva manifestação da transferência do poder de controlo da autoridade administrativa para o próprio responsável pelo tratamento, que, noutros planos, tem vindo a ser institucionalizado (como sucede no domínio do direito do ambiente)".*[167]

Obrigação de Notificação de uma violação de dados pessoais

Nos termos do número 1 do artigo 33.º, o responsável pelo tratamento está obrigado a notificar a autoridade de controlo competente em caso de violação de dados pessoais, sem demora injustificada e, sempre que possível, até 72 horas após

[166] Cf. nesse sentido o Considerando (97) do RGPD.
[167] CALVÃO, Filipa, op. cit. pp. 44.

ter tido conhecimento da mesma. O mesmo artigo estabelece que ficam excecionadas da obrigação de notificação as violações dos dados pessoais não sejam suscetíveis de resultar num risco para os direitos e liberdades das pessoas singulares.

O subcontratante fica também obrigado a notificar o responsável pelo tratamento, sem demora injustificada, após ter conhecimento de uma violação de dados pessoais (cf. número 2 do artigo 33.º).

Note-se que esta obrigação foi inicialmente prevista na Diretiva Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, alterada pela Diretiva 2009/136/CE, do Parlamento Europeu e do Conselho, de 25 de novembro. O que o RGPD pretende agora "*é generalizar esta obrigação aos tratamentos de dados realizados em todos os setores de atividade*."[168]

Em casos em que a violação dos dados pessoais seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento também está obrigado a comunicar a violação de dados pessoais ao titular dos dados sem demora injustificada (cf. número 1 do artigo 34.º).
O titular dos dados está isento da comunicação ao titular dos dados sempre que for preenchida uma das seguintes condições:

a. O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;
b. O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados a que se refere o número 1 já não é suscetível de se concretizar; ou
c. Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz (cf. número 3 do artigo 34.º).

[168] CALVÃO, Filipa, op. cit. pp. 45.

Controlo do cumprimento das regras do Regulamento Geral sobre Protecção de Dados

A fiscalização do cumprimento do Regulamento é assegurada por uma Autoridade de Controlo existente em cada país, responsável por regular e fiscalizar o tratamento de dados pessoais e a observância dos princípios e regras impostas pelo RGPD na proteção de dados pessoais, dispondo de variados poderes de investigação e fiscalização. (cf. artigo 51.º).

As autoridades de controlo beneficiam de "estatuto independente" (cf. artigo 52.º) – e "*são competentes para prosseguir as atribuições e exercer os poderes que lhes são conferidos pelo presente regulamento no território do seu próprio Estado-Membro*» (cf. número 1 do artigo 55.º).

Entre as atribuições das autoridades de controlo, estabelecidos no número 1 do artigo 57.º, contam-se as de:

a. Controlar e executa a aplicação do RGPD;
b. Se lhe for solicitado, prestar informações a qualquer titular de dados sobre o exercício dos seus direitos nos termos do RGPD e, se necessário, cooperar com as autoridades de controlo de outros Estados-Membros para esse efeito;
c. Tratar as reclamações apresentadas por qualquer titular de dados, ou organismo, organização ou associação nos termos do artigo 80.º, e investigar, na medida do necessário, o conteúdo da reclamação e informar o autor da reclamação do andamento e do resultado da investigação num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo;
d. Cooperar, incluindo partilhando informações e prestando assistência mútua a outras autoridades de controlo, tendo em vista assegurar a coerência da aplicação e da execução do presente regulamento;
e. Conduzir investigações sobre a aplicação do RGPD, incluindo com base em informações recebidas de outra autoridade de controlo ou outra autoridade pública;
f. Adotar as cláusulas contratuais-tipo previstas no número 8 do artigo 28.º, e no número 2 do artigo 46.º , alínea d);
g. Elaborar e conservar uma lista associada à exigência de realizar uma

avaliação do impacto sobre a proteção de dados, nos termos do número 4 do artigo 35.º;

h. Dar orientações sobre as operações de tratamento previstas no número 2 do artigo 36.º;

i. Autorizar as cláusulas contratuais e disposições previstas no número 3 do artigo 46.º;

j. Aprovar as regras vinculativas aplicáveis às empresas nos termos do artigo 47.º;

k. Contribuir para as atividades do Comité Europeu para a Protecção de Dados, organismo previsto pelo Regulamento enquanto organismo da União, que assegura a aplicação coerente das regras do Regulamento;

l. Conservar registos internos de violações do presente regulamento e das medidas tomadas nos termos do número 2 do artigo 58.º.

Adicionalmente, a Autoridade de Controlo dispõe ainda de poderes sancionatórios, conforme abaixo mais bem descrito.

A Comissão Nacional de Protecção de Dados (CNPD) no novo contexto legal

No novo contexto legal, em Portugal, a fiscalização do cumprimento das regras resultantes do Regulamento Geral sobre a Proteção de Dados Pessoais é da competência da Comissão Nacional de Proteção de Dados. A CNPD compete regular e fiscalizar as atividades e operações de tratamento de dados pessoais e sancionar a inobservância dos princípios e regras impostas pelo RGPD.

Desde a Revisão Constitucional de 1997, o artigo 35.º da Constituição prevê a existência de uma "entidade administrativa independente", cujo objetivo seria garantir a proteção dos direito à proteção de dados. Ainda antes da inclusão desta previsão constitucional, a Lei n.º 10/91 criou a Comissão Nacional de Proteção de Dados Pessoais Informatizados, que viria a ser instituída em 1994. Atualmente, e desde de 1998, essa autoridade administrativa independente é conhecida por Comissão Nacional de Proteção de Dados.

Portanto, a CNPD "*é a entidade que, à luz do artigo 35.º, n.º 2 da CRP, e do artigo 22.º, n.º 2 da LPDP, detém competência para intervir em todas as situações que impliquem tratamento de dados pessoais*"[169]. Nos termos do disposto nos artigos 22.º e 23.º da Lei da Proteção de Dados Pessoais, a CNPD dispõe:

a. "*De poderes de investigação e de inquérito, podendo aceder aos dados objeto de tratamento e recolher todas as informações necessárias ao desempenho das suas funções de controlo*" (cf. número 2 do artigo 22.º, alínea a));

b. "De poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, bem como o de proibir, temporária ou definitivamente, o tratamento de dados pessoais, ainda que incluídos em redes abertas de transmissão de dados a partir de servidores situados em território português" (cf. número 2 do artigo 22.º, alínea b))[170];

c. "Do poder de emitir pareceres prévios aos tratamentos de dados pessoais, assegurando a sua publicitação" (cf. número 2 do artigo 22.º, alínea c)) e "*compete em especial à CNPA emitir pareceres sobre disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições comunitárias e internacionais, relativos ao tratamento de dados pessoais*" (cf. número 1 do artigo 23.º, alínea a));

d. Da competência para a autorização prévia[171] ou registo[172] dos tratamentos de dados pessoais;

e. Da competência para "*efetuar, a pedido de qualquer pessoa, a verificação da licitude de um tratamento de dados, sempre que esse tratamento esteja sujeito a restrições de acesso ou de informação, e informá-la da realização da verificação*" (cf. número 1 do artigo 23.º, alínea j));

---

[169] Comissão Nacional de Proteção de Dados – **Comissão de assuntos constitucionais direitos, liberdades e garantias**. Relator Luís Barroso. Parecer n.º 43/2012. Lisboa: CNPD, 2012. Disponível para consulta em http://www.cnpd.pt/bin/decisoes/par/40_43_2012.pdf (17.03.2018).

[170] MARQUES, Garcia; MARTINS, Lourenço – **Direito da Informática**. Coimbra: Edições Almedina, p. 363 e ss.

[171] Há lugar à autorização prévia quando o tratamento diga respeito a dados sensíveis, dados relativos a suspeitas de atividades ilícitas, infrações penais, contraordenações, decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias, de dados pessoais obtidos através da interconexão de dados sobre crédito e solvabilidade (nos termos do número 2 do artigo 8.º, do artigo 9.º, do artigo 23.º, das alíneas b), c) e d) do número 1 do artigo 23.º e do artigo 28.º)

[172] O registo do tratamento de dados pessoais está previsto no artigo 27.º.

f. Apreciar as reclamações, queixas ou petições dos particulares (cf. número 1 do artigo 23.º, alínea k)).

Além das referidas competências e poderes, a CNPD é competente para autorizar ou isentar do dever de notificação determinadas categorias de tratamento de dados que não sejam suscetíveis de pôr em causa direitos e liberdades dos titulares dos dados, conforme dispõe o número 2 do artigo 27.º da Lei n.º 67/98, de 26 de outubro. Outro poder conferido à Comissão Nacional de Proteção de Dados é o poder para advertir ou censurar publicamente o responsável pelo tratamento, em caso de reiterado incumprimento das disposições legais em matéria de dados pessoais, nos termos do número 4 do artigo 22.º.

Por último e ainda no que toca à CNPD, existem dúvidas quanto à compatibilidade do disposto no número 2 do artigo 7.º da Lei n.º 67/98, de 26 de outubro, com a Constituição da República Portuguesa, "*na parte em que estabelece uma competência autorizativa da Comissão*". Segundo o autor Sousa Pinheiro, "*crê-se que o n.º 2 do art.º 7.º da Lei n.º 67/98, de 26 de outubro, não é compatível com a Constituição*"[173]. No entendimento deste autor, a CRP apenas estabelece duas fontes de legitimidade para o tratamento de dados pessoais, que são o "consentimento" e a "autorização prevista por lei", não referindo uma terceira fonte, a autorização da entidade administrativa de controlo. Ainda assim, a Lei n.º 67/98, de 26 de outubro, enuncia que a CNPD é a entidade competente e elenca as situações em que pode ser emitida autorização para o tratamento de dados pessoais sensíveis, livre quer do consentimento do titular, quer de disposição específica.

Com a aplicação do Regulamento Geral sobre a Proteção de Dados Pessoais, as atribuições da CNPD em matéria de fiscalização serão mais abrangentes, incluindo, por exemplo, ordenar o fornecimento de informações por parte do responsável pelo tratamento ou do subcontratante, obter acesso a todos os dados pessoais e todas as informações necessárias, impor uma limitação definitiva ou temporária ao tratamento de dados, ordenar a retificação ou o apagamento de dados pessoais.

A CNPD passará a ter um papel de fiscalização mais ativo, podendo até realizar

[173] PINHEIRO, Alexandre Sousa, op. cit., p. 736 e 737.

investigações às empresas sobre a forma de auditorias sobre proteção de dados.

Para além disso, a CNPD dará seguimento às reclamações recebidas, conduzirá investigações sobre a aplicação do Regulamento, aplicando as coimas de acordo com as novas previsões do RGPD.

Entre outras atribuições competirá à CNPD, em Portugal, exercer as atribuições das autoridades de controlo estabelecidas nos termos do artigo 57.º, n.º 1.

Regime sancionatório

Previamente à entrada em vigor do RGPD, a matéria sancionatória no que toca a infrações relacionadas com dados pessoais no Direito da União Europeia era regulada pelo artigo 24.º da Diretiva 95/46/CE. Nos termos daquele artigo 24.º, "*[o]s Estados membros tomarão as medidas adequadas para assegurar a plena aplicação das disposições da presente diretiva a determinarão, nomeadamente, as sanções a aplicar em caso de violação das disposições adotadas nos termos da presente diretiva*".

A norma do artigo 24.º é igualmente aplicável à Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva Privacidade e Comunicações Eletrónicas) e da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações[174], e que altera a Diretiva 2002/58/CEO, por força das remissões operadas pelos artigos 15.º, n.º 2 da Diretiva 2002/58/CE e artigo 13.º,

[174] A diretiva 2006/24/CE impõe a conservação de determinados dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas, com o objetivo de garantir a disponibilidade desses dados para efeitos de investigação, deteção e repressão de crimes graves, de acordo com a definição adotada no direito nacional de cada Estado membro. No dia 8 de abril de 2014 (processos apensos C-293/12 e 594/12), o tribunal de Justiça declarou a Diretiva 2006/24/CE inválida, por violação dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, pelo facto de a diretiva impor uma significativa intromissão nos direitos fundamentais ao respeito pela vida privada e aos dados pessoais. Para uma análise da decisão de invalidade da diretiva.

n.º 1, da Diretiva 2006/24/CE.

Verificou-se, contudo, que, devido ao elevado grau de indeterminação do artigo 24.º da diretiva 95/46/CE, a sua transposição para os ordenamentos jurídicos dos Estados-Membros foi feita em termos bastante distintos, quer quanto à qualificação da natureza infração (quer como crime, contraordenação ou infração punível com sanção administrativa), quer quanto à medida legal da sanção abstratamente aplicável.

O RGPD, com o propósito claro de estabelecer "*um quadro de protecção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras"*, bem como "*sanções equivalentes para os infractores nos Estados membros*"[175], prevê um aumento relevante do valor das coimas que podem ser aplicadas pelas Autoridades de Controlo em consequência da violação de normas do mesmo Regulamento e cujo valor máximo passa a poder ir até € 20.000.000,00 ou 4% do volume de negócios do infrator.

Ora, ao contrário do que aparenta ter sido o objetivo do RGPD[176], a aplicabilidade direta do RGPD não resulta clara do diploma no que toca ao regime sancionatório, na medida em que "*os Estados-Membros estabelecem as regras relativas às outras sanções aplicáveis em caso de violação do disposto no presente regulamento, nomeadamente às violações que não são sujeitas a coimas nos termos do artigo 79.º a 83.º, e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas."*

Ainda assim, o RGPD faz uma diferenciação clara entre **i)** as sanções qualificadas como "coimas", aplicáveis às infrações previstas nos n.ºs 4 a 6 do artigo 83.º - relativamente às quais se verifica a aplicabilidade direta do Regulamento; **ii)** às outras sanções aplicáveis em caso de violação do disposto no Regulamento,

[175] Cf. nesse sentido os Considerandos (7), (9) e (11) do RGPD.

[176] De acordo com a exposição de motivos da Proposta de Regulamento, é referido que «[a] sua aplicabilidade direta, prevista no artigo 288.º do TFUE, permitirá reduzir a fragmentação jurídica e proporcionar maior segurança jurídica, introduzindo um conjunto harmonizado de regras de base, melhorando a proteção dos direitos fundamentais das pessoas singulares e contribuindo para o bom funcionamento do mercado interno» - Cf. Exposição de motivos da proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, COM(2012) 11 final, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017PC0495 (17.05.2018).

relativamente às quais o 84.º prevê-se que os Estados-Membros devem estabelecem as regras aplicáveis, nomeadamente às violações que não são sujeitas a coimas nos termos do artigo 83.º/6. Segundo José Lobo Moutinho, resulta "*claro que cabe aos Estados membros, não só (i) a determinação de outras sanções (designadamente penais) para as infrações ao disposto do Regulamento, como ainda (ii) a previsão de sanções aplicáveis às infrações que não são sujeitas a coimas nos termos do artigo 83.º".*[177] [178]

Nos termos artigo 83.º, n.º 9, as sanções aplicáveis às infrações diretamente puníveis por força do Regulamento são expressamente qualificadas como "coimas", nomeadamente "coimas impostas pelas autoridades de controlo". Esta qualificação tem como consequência a aplicabilidade do RGCO naquilo que não for expressamente regulado no Regulamento, por estarmos perante contraordenações[179].

Por último, em relação à questão de quem são os responsáveis pelas infrações, importa atentar que o RGPD não é muito claro na solução adotada. O artigo 83.º (nos seus números 3,4 e 5) utiliza a expressão "empresa" para determinar o montante máximo da coima. No entanto, parece resultar daqueles artigos que a expressão "empresa" não tem o significado apresentado no artigo 4.º do Regulamento. Segundo essa disposição, «empresa», é "uma pessoa singular ou coletiva que, independente- mente da sua forma jurídica, exerce uma atividade económica, incluindo as sociedades ou associações que exercem regularmente uma

---

[177] MOUTINHO, José, «Legislador português. Precisa-se. Algumas notas sobre o regime sancionatório no Regulamento Geral sobre a Proteçãode Dados (Regulamento (UE) 2016/679), in *Forum de Proteção de Dados*, n.º 4, julho. 2017, pp. 43.

[178] Esta solução é a que resulta dos Considerandos (152) e (149).
Nos termos do Considerando n.º 152 "sempre que o presente regula- mento não harmonize sanções administrativas, ou se necessário noutros casos, por exemplo, em caso de infrações graves às disposições do presente regulamento, os Estados-Membros deverão criar um sistema que preveja sanções efetivas, proporcionadas e dissuasivas. A natureza das sanções, penal ou administrativa, deverá ser determinada pelo direito do Estado-Membro". Por sua vez, pode ler-se no considerando n.º 149 que "os Estados-Membros deverão poder definir as normas relativas às sanções penais aplicáveis por violação do presente regulamento, inclusive por violação das normas nacionais adotadas em conformidade com o presente regulamento, e dentro dos seus limites. Essas sanções penais podem igualmente prever a privação dos lucros auferidos em virtude da violação do presente regulamento. Contudo, a imposição de sanções penais por infração às referidas normas nacionais, bem como de sanções administrativas, não deverá implicar a violação do princípio *ne bis in idem*, conforme é interpretado pelo Tribunal de Justiça"

[179] Atendendo ao critério formal para a definição de contraordenação –a prática de um facto que preencha um tipo legal no qual se comine uma "coima" (artigo 1.º do RGCO).

atividade económica" (número 18) e «grupo empresarial» é "um grupo composto pela empresa que exerce o controlo e pelas empresas controladas" (número 19). Ora, o artigo 83.º não prevê o caso dos grupos empresariais, o que leva a afastar a utilização da definição constante do artigo 4.º

José Lobo Moutinho defende que a solução deve ser interpretada segundo o considerando n.º 150, que «*parece pretender esclarecer este mistério ao afirmar que "sempre que forem impostas coimas a empresas, estas deverão ser entendidas como empresas nos termos dos artigos 101.º e 102.º do TFUE para esse efeito". Portanto, podem ser sancionadas empresas ou "coimas a pessoas que não sejam empresas nesse sentido"*.» [180]

Caberá ao Comité elaborar as "*diretrizes dirigidas às autoridades de controlo em matéria de aplicação das medidas a que se refere o artigo 58.º, n.ºs 1, 2 e 3, e de fixação de coimas nos termos do artigo 83.º*" (cf. número 1 do artigo 70.º, alínea k)).

A EXPERIÊNCIA PORTUGUESA EM PROTEÇÃO DE DADOS

A EVOLUÇÃO: DA CONSTITUIÇÃO DE 1976 AOS DIAS DE HOJE

O primeiro texto constitucional da Europa[181] a consagrar, ainda que indiretamente, a proteção dos dados pessoais, foi a Constituição da República Portuguesa de 1976[182], no seu art.º 35.º, consagrado no título respeitante dos Direitos, Liberdades e Garantias. Referimos que a consagração foi indireta pois a disposição do artigo

---

[180] MOUTINHO, José - **Legislador português. Precisa-se. Algumas notas sobre o regime sancionatório no Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679)**, in *Forum de Proteção de Dados*, n.º 4, julho. 2017, pp. 49.

[181] Neste sentido, CASTRO, Catarina Sarmento e – **Direito da Informática, Privacidade e Dados pessoais**. Coimbra: Edições Almedina, p. 32; e, TEIXEIRA, Maria Leonor da Silva - **A União Europeia e a Protecção de Dados Pessoais – Uma visão futurista**. Lisboa: Sindicato dos Magistrados do Ministério Público, p.75.

[182] "*ARTIGO 35.º (Utilização da informática) 1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização. 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos. 3. É proibida a atribuição de um número nacional único aos cidadãos*". Constituição da República Portuguesa de 1976. Disponível em http://www.parlamento.pt/Parlamento/Documents/CRP1976.pdf. (17.03.2018)

35.º não fazia "referência em qualquer dos seus três números à "proteção de dados" ou ao "direito à proteção de dados"[183].

Este artigo sofreu alterações resultantes das revisões constitucionais de 1982[184], de 1989[185], e por último, de 1997. Esta última alteração impôs alterações profundas[186] e aprovou o texto constitucional atualmente vigente, no qual pode ler-se:

«Artigo 35.º

Utilização da informática

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a

---

[183] PINHEIRA, Alexandre Sousa, op. cit., p. 665.

[184] Esta alteração, perpetrada pela Lei n.º 1/82, de 30 de Setembro e determinava, no seu artigo 27.º, que:

«*"1 - No n.º 1 do artigo 35.º a expressão 'registos mecanográficos' é substituída pela expressão "registos informáticos".*

2 - É aditado ao artigo 35.º um novo n.º 2, com a seguinte redação: "2. São proibidos o acesso de terceiros a ficheiros com dados pessoais e a respetiva interconexão, bem como os fluxos de dados transfronteiras, salvo em casos excecionais previstos na lei."

3 - O n.º 2 do artigo 35.º passa a constituir o n.º 3 do mesmo artigo, sendo o seu texto substituído por: "3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada, salvo quando se trate do processamento de dados estatísticos não individualmente identificáveis."

4 - Ao artigo 35.º é aditado um n.º 4, com a seguinte redação: "4. A lei define o conceito de dados pessoais para efeitos de registo informático."

5 - O n.º 3 do artigo 35.º passa a constituir o n.º 5 do mesmo artigo.»

[185] O artigo 20.º da Lei n.º 1/89 de 8 de julho de determinou que:

«*1 - O n.º 1 do artigo 35.º é substituído por: "Todos os cidadãos têm o direito de tomar conhecimento dos dados constantes de ficheiros ou registos informáticos a seu respeito e do fim a que se destinam, podendo exigir a sua retificação e atualização, sem prejuízo do disposto na lei sobre segredo de Estado e segredo de justiça."*

2 - O n.º 2 do artigo 35.º é substituído por: "2. É proibido o acesso a ficheiros e registos informáticos para conhecimento de dados pessoais relativos a terceiros e respetiva interconexão, salvo em casos excecionais previstos na lei.2

3 - O n.º 4 do artigo 35.º é substituído por: "4. A lei define o conceito de dados pessoais para efeitos de registo informático, bem como de bases e bancos de dados e respetivas condições de acesso, constituição e utilização por entidades públicas e privadas."

4 - Ao artigo 35.º é aditado um novo n.º 6, com a seguinte redação: "6. A lei define o regime aplicável aos fluxos de dados transfronteiras, estabelecendo formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.»

[186] Esta revisão constitucional deste artigo esteve largamente fundada na necessidade de proceder à transposição da Diretiva de Proteção de Dados. Sobre a matéria ver PINHEIRO, Alexandre Sousa e BRITO FERNANDES, Mário João de – Comentário à IV Revisão Constitucional. Lisboa: AAFDL, 1999, p. 135 e MAGALHÃES, José – Dicionário da Revisão Constitucional. Lisboa: Edital Notícias, 1999, p. 132 *apud* PINHEIRO, Alexandre Sousa, op. cit., p. 666.

sua proteção, designadamente através de entidade administrativa independente.

3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.

5. É proibida a atribuição de um número nacional único aos cidadãos.

6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.»

Tal como defendem Gomes Canotilho e Vital Moreira[187], o direito à proteção de dados é decorrente de outros «*"direitos-mãe", tais como o direito à dignidade da pessoa humana*[188]*, do desenvolvimento da personalidade, da integridade pessoal e da autodeterminação informativa*[189]». Em conformidade, e sem prejuízo da aplicabilidade direta dos direitos liberdades e garantias[190], o disposto no número 2 do artigo 35.º da CRP atribui à lei a definição do «*conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização*». Importa então analisar a legislação portuguesa aprovada no âmbito da proteção de dados.

---

[187] CANOTILHO, J. J. Gomes; MOREIRA Vital – Constituição da República Portuguesa Anotada. Coimbra: Coimbra Editora, p. 251 - 273

[188] O artigo 1.º da Constituição da República Portuguesa preconiza que «Portugal é uma república soberana, baseada na dignidade da pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária».

[189] Acerca do *Recht auf informationelle Selbstbestimmung* (Direito à Autodeterminação Informativa) ver CASTRO, Catarina Sarmento – **Privacidade Versus Publicidade: Proteção de Informações Pessoais e Atividade Registral**. Coimbra: Coimbra Editora, p. 376 e 377.

[190] Garantia constitucionalmente prevista por força do art.º 18.º, n.º 1 da CRP

A entrada em vigor do Regulamento Geral da Proteção de Dados acarreta diversas implicações para o normativo constitucional em análise.

Em primeiro lugar, o artigo 35.º da CRP faz, desde logo, a referência expressa à lei. Ora, considerando que o regulamento "*é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros*", fará sentido recorrer à expressão "nos termos das disposições legais aplicáveis" em substituição da redação atual.

O número 1 do artigo 9.º do RGPD impõe uma alteração à redação do número 3 do artigo 35.º da CRP, na medida em que aquele normativo comunitário prevê apenas a proibição do tratamento de dados "*que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa*." No que toca às exceções da proibição estabelecida, também aqui seria necessário introduzir alterações para espelhar o previsto no nº2 do artigo 9.º do RGPD. Note-se também que o RGPD não prevê a proibição do número único, inserta no n.º 5 do artigo 35.º da CRP. De facto, o número único é utilizado em mais do que um país da União Europeia.

Adicionalmente, há que notar que os fluxos transfronteiras no interior da União Europeia não podem estar submetidos a regulamentação da lei nacional, conforme determina o número 6 do artigo 35.º da CRP. O RGPD é bastante explícito ao estabelecer que "*a livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais*». Adicionalmente, as transferências de dados pessoais para países terceiros ou organizações internacionais vem regulada nos artigos 44.º e seguintes do RGPD.

Por fim, a formulação contida no número 7 do artigo 35.º da CRP difere da formulação do número 1 do artigo 2.º do RGPD. Por um lado, o RGPD é aplicável ao "*tratamento por meios não automatizados de dados pessoais contidos num ficheiro*

ou a ele destinados", enquanto o número do artigo 35.º da CRP faz referência aos "*dados constantes de ficheiros manuais".*[191]

A LEI N.º 67/98, DE 26 DE OUTUBRO

Embora a proteção de dados pessoais[192] seja referenciada na Constituição como um direito fundamental, no disposto no artigo 35.º, a Constituição, desde a Revisão Constitucional de 1982, remete para a lei a definição do conceito de dados pessoais. No entanto, só em 1991, com a Lei n.º 10/91, de 27 de abril, que aprovou a Lei da Proteção de Dados Pessoais face à Informática, que o legislador regulou a matéria da proteção de dados, em harmonização com os princípios da Convenção 108 do Conselho da Europa sobre a proteção das pessoas relativamente ao tratamento automatizado de dados pessoais. Atualmente, tal definição encontra-se desenvolvida na Lei da Proteção de Dados Pessoais, aprovada pela Lei n.º 67/98, de 26 de outubro[193], conforme alterada pela Lei n.º 103/2015, de 24 de agosto. A Lei da Proteção de Dados Pessoais transpõe para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995.

---

[191] Sobre esta questão ver LOPES, Joaquim de Seabra – **O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível**, in *Forum de Proteção de Dados*, n.º 2, jan. 2016.

[192] A expressão "proteção de dados" constitui uma tradução literal da fórmula alemã Datenschutz, que se impôs na linguagem universal". PINHEIRO, Alexandre de Sousa – **A proteção de dados na proposta de regulamento comunitário apresentada pela Comissão Europeia (2012): primeiras reflexões**. Lisboa: Diário de Bordo, p. 9 e 10.

[193] A Lei n.º 67/98, de 26 de outubro revogou a Lei n.º 10/91, de 29 de abril, que aprovara a Lei da Proteção de Dados Pessoais face à Informática. Esta Lei n.º 10/91, de 27 de abril, que foi a primeira Lei da Proteção de Dados surgiu na sequência de um Acórdão do Tribunal Constitucional que deu por verificada a existência de uma inconstitucionalidade por omissão em virtude da inexistência de uma Lei que regulasse estes aspetos: Acórdão do Tribunal Constitucional n.º 182/89, publicado no DR I-A, de 2 de março de 1989 e disponível para consulta em http://www.tribunalconstitucional.pt/tc/acordaos/19890182.html (17.03.2018). Sobre o assunto, ver CASTRO, Catarina Sarmento e – op. cit., p. 35 e ss.

Diversas críticas foram feitas à Lei n.º 10/91, designadamente o facto **1)** de não fazer referência à proteção de dados no seu princípio geral (e sim à reserva da vida privada e familiar), **2)** de restringir o seu âmbito de aplicação material considerando identificável apenas aquela pessoa cuja identificação não tivesse custos ou prazos desproporcionados, o que resultada na sua inconstitucionalidade. Nesse sentido GOUVEIA, Jorge Bacelar de – **Os Direitos Fundamentais à Proteção dos Dados Pessoais Informatizados**, Revista da Ordem dos Advogados, Ano 51, Dezembro 1992, p. 716 *apud* PINHEIRO, Alexandre Sousa, op. cit.,p. 704.

A Lei da Proteção de Dados Pessoais está dividida em VII capítulos e o seu âmbito de aplicação encontra-se regulamentado no artigo 4.º, delimitando tanto o âmbito de aplicação material como o âmbito de aplicação territorial. Deste modo, a Lei da Proteção de Dados Pessoais aplica-se "ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados" [194][195], sempre que o tratamento seja "*no âmbito das atividades de estabelecimento do responsável do tratamento situado em território português*" quer as atividades sejam realizadas "fora do território nacional, em local onde a legislação portuguesa seja aplicável por força do direito internacional". A Lei da Proteção de Dados também é aplicável ao tratamento realizado "*por responsável que, não estando estabelecido no território da União Europeia, recorra, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território português, salvo se esses meios só forem utilizados para trânsito através do território da União Europeia.*"[196] [197]

Uma exclusão à qual importa fazer referência é a exclusão do âmbito de aplicação da Lei da Proteção de Dados dos tratamentos de dados pessoais efetuados por pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas[198]. Conforme nota Alexandre Sousa Pinheiro, "*a interpretação do art.º 4.º, n.º 2, da Lei n.º 67/98, de 26 de outubro, pode causar dificuldades no que respeita*

---

[194] Ver o disposto no número 1 do artigo 4.º da Lei da Proteção de Dados Pessoais.

[195] Nesse sentido, a CNPD foi chamada a pronunciar-se sobre os limites da aplicabilidade da Lei a dados manuais, num caso relativo à transmissão de informação ao Instituto do Consumidor, tendo aprovado a Deliberação n.º 107/2003, afirmando que "*o âmbito das competências da CNPD restringe-se à possibilidade de apreciação de tratamento efetuado com recurso a meios total ou parcialmente automatizados ou em ficheiros manuais estruturados. Verifica-se que a correspondência trocada se encontra arquivada – de forma "não estruturada" na aceção da Lei 67/98 – em pastas ou arquivos. Ora, não há quaisquer elementos que permitam concluir que as alegadas "referências negativas" ou "juízos de valor" transmitidos ao Instituto do Consumidor constem de um "tratamento" a que é aplicável a Lei 67/98.*"Esta deliberação pode ser consultada em https://www.cnpd.pt/bin/decisoes/2003/htm/del/del107-03.htm (17.03.2018).

[196] O âmbito territorial de aplicação da Lei da Proteção de Dados Pessoais está previsto no número 2 do artigo 4.º. Sobre a matéria ver CASTRO, Catarina Sarmento e – **Direito da Informática, Privacidade e Dados pessoais**. Coimbra: Edições Almedina p. 51.

[197] "*Mas a lei portuguesa já não será aplicável quando o meio que serve de recolha de dados é, v.g., um PC pertencente ao titular dos dados, que por sua iniciativa consulta uma página Internet e envia as suas informações pessoais para um país terceiro a fim de serem utilizados por uma entidade não estabelecida em território onde a lei portuguesa seja aplicável, mesmo que esse titular se encontre em território português.*" CASTRO, Catarina Sarmento e – op. cit., p. 53 e ss.

[198] Ver o disposto no número 2 do artigo 4.º da Lei n.º 67/98, de 26 de outubro, e no número 2 do artigo 3.º da Diretiva 95/46/CE de 24 de outubro.

à aplicação. A exclusão dos dados tratados para finalidades exclusivamente pessoais ou domésticas pode levantar problemas quando estejam em causa tratamentos de dados com finalidade distinta". O autor defende que, sempre que o tratamento de dados inclui mais finalidades que não apenas finalidades exclusivamente pessoais, o disposto na Lei n.º 67/98, de 26 de outubro deve ser aplicado[199].

O número 1 do artigo 5.º estabelece os requisitos dos dados pessoais, estabelecendo que cabe ao responsável pelo tratamento assegurar a sua observância. Nesse sentido, os dados pessoais devem ser:

a. *"Tratados de forma lícita e com respeito pelo princípio da boa fé;*
b. *Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades;*
c. *Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados;*
d. *Exatos e, se necessário, atualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou retificados os dados inexatos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente;*
e. *Conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior."*

A Lei da Proteção de Dados determina, tal como o fazia a Diretiva e faz o RGPD, que o consentimento é a principal fonte de licitude do tratamento de dados. À parte do consentimento, o tratamento de dados pessoais pode também ser efetuado se o tratamento for necessário para:

a. Execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efetuadas a seu pedido;

[199] O autor apresenta como exemplos a instalação de câmaras quer para controlo dos trabalhadores como para controlo da via pública, casos em que as regra da Lei da Proteção de Dados são aplicáveis e não há lugar à exclusão da sua aplicação. PINHEIRO, Alexandre Sousa – op. cit., p. 721.
No mesmo âmbito, o autor chama também atenção para os problemas que podem surgir aquando do tratamento de caráter pessoal ou doméstico de dados pessoais contidos em agendas, manuais ou eletrónicas, ou noutro tipo de equipamento, sempre que a informação for utilizada para uma finalidade distinta da natureza pessoal ou doméstica (por exemplo, no caso de através, por exemplo de leilões de agenda.).

b. Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito;

c. Proteção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento;

d. Execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

e. Prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados. (cf. artigo 6.º da Lei).

No que se refere ao tratamento de dados sensíveis, funciona a regra de proibição sob reserva de autorização. Quer isto dizer que, de acordo com o disposto no artigo 7.º, é proibido o tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos. No entanto, mediante disposição legal ou autorização da CNPD, pode ser permitido o tratamento dos dados referidos no número anterior quando por motivos de interesse público importante esse tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, ou quando o titular dos dados tiver dado o seu consentimento expresso para esse tratamento, em ambos os casos com garantias de não discriminação e com as medidas de segurança adequadas.

O tratamento de dados sensíveis também é permitido quando se verificar uma das seguintes condições:

a. Ser necessário para proteger interesses vitais do titular dos dados ou de uma outra pessoa e o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento;

b. Ser efetuado, com o consentimento do titular, por fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas atividades legítimas, sob condição de o tratamento respeitar apenas aos membros desse organismo ou às pessoas que com ele

mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem consentimento dos seus titulares;

c. Dizer respeito a dados manifestamente tornados públicos pelo seu titular, desde que se possa legitimamente deduzir das suas declarações o consentimento para o tratamento dos mesmos;

d. Ser necessário à declaração, exercício ou defesa de um direito em processo judicial e for efetuado exclusivamente com essa finalidade.

Por força da Diretiva 95/46 que transpôs, a Lei da Proteção de Dados consagra os seguintes direitos dos titulares dos dados: direito de informação (cf. artigo 10.º); direito de acesso (cf. artigo 11.º); direito de oposição do titular dos dados (cf. artigo 12.º); direito a não ficar sujeito a decisões individuais automatizadas (cf. artigo 13.º).

Antes de abordar o tema sectorial específico deste trabalho, convém verificar os conceitos definidos pela Lei da Proteção de Dados. O artigo 3.º apresenta as definições adotadas para efeito da Lei da Proteção de Dados, que são as seguintes:

- *«"Dados pessoais": qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ("titular dos dados")* [200]*; é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social*[201]*»;*

---

[200] Esta definição está em consonância com o previsto na Diretiva n.º 95/46/CE, de 24 de outubro, já anteriormente abordada.

[201] Entende-se que também integram o conceito de dados pessoais aqueles dados que permitam identificar uma pessoa singular através da utilização de meios disponíveis a terceiros.

2 "(…) Por assim entender é que deve considerar-se que, no âmbito dos dados tratados a propósito de comunicações através da internet, os dados do endereço IP do utilizador são dados pessoais: podem ser sempre identificáveis, ainda que com recursos a meios de que dispõem outros intervenientes nestas comunicações […]".CASTRO, Catarina Sarmento e – op. cit., p. 71.

Adicionalmente, o Tribunal de Justiça, no caso Tietosuojavaltuutettu, destacou que "(…) as atividades de tratamento de dados pessoais, relativas a ficheiros das autoridades públicas que contenham dados pessoais que abranjam apenas informações inalteradas já publicadas nos meios de comunicação social, enquadram-se no âmbito de aplicação da Diretiva n.º 95/46/CE" . Esta decisão pode ser consultada em http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd52ff4da201ef4b0d8c7a8875e96eb2f7.e34KaxiLc3qMb40Rch0SaxuQa310?text=&docid=76075&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=666398 (17.03.2018).

- *«"Tratamento de dados pessoais" ("tratamento"): qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados[202], tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;*
- *"Ficheiro de dados pessoais" ("ficheiro"): qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;*
- *"Responsável pelo tratamento": a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinados por disposições legislativas ou regulamentares, o responsável pelo tratamento deve ser indicado na lei de organização e funcionamento ou no estatuto da entidade legal ou estatutariamente competente para tratar os dados pessoais em causa;*
- *"Subcontratante": a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento;*
- *"Terceiro": a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular dos dados, o responsável pelo*

A qualificação como "dado pessoal" está sujeita a um princípio de reconhecimento. Em conformidade, não podem ser considerados dados pessoais aqueles dados que não permitam identificar uma pessoa. Nesse sentido veja-se o acórdão do Tribunal de Justiça da União Europeia no âmbito do processo n.º C-101/01, disponível para consulta em http://curia.europa.eu/pt/actu/communiques/cp03/aff/cp0396pt.htm. (17.03.2018).
Diferentemente será a questão da anonimização, que vem permitir que caso exista "informação pessoal apenas identificável com meio sofisticados e custos elevados, essa só deve considerar-se protegida pelo regime da Diretiva caso seja ultrapassada a prova da razoabilidade".

[202] O Tratamento também pode ser realizado de forma parcialmente automatizada. Catarina Sarmento e Castro descreve como exemplo de um tratamento parcialmente automatizado o tratamento, ainda que realizado com recurso a meios informáticos, que se limite a organizar os nomes dos utentes de um serviço público aos quais esteja ligado um número de processo, que permita, depois, mediante identificação desse mesmo número associar uma pasta em papel de que constam outros elementos. Em relação aos ficheiros manuais, a autora refere as fichas de atendimento de um consultório, organizadas por ordem alfabéticas, ou de uma conta-corrente numa mercearia. CASTRO, Catarina Sarmento, op. cit., p.106.

tratamento, o subcontratante ou outra pessoa sob autoridade direta do responsável pelo tratamento ou do subcontratante, esteja habilitado a tratar os dados;

- *"Destinatário": a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo a quem sejam comunicados dados pessoais, independentemente de se tratar ou não de um terceiro, sem prejuízo de não serem consideradas destinatários as autoridades a quem sejam comunicados dados no âmbito de uma disposição legal;*
- *"Consentimento do titular dos dados": qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objeto de tratamento;*
- *"Interconexão de dados": forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade.»*

OS MECANISMOS DE GEOLOCALIZAÇÃO

Por um lado, o surgimento de novas tecnologias cria cada vez mais riscos à privacidade e à proteção de dados dos utilizadores. O uso da internet e de redes móveis digitais, com um custo acessível à maioria das pessoas, faz com que o número de utilizadores cresça todos os dias, pelo que importa analisar os seus impactos nos direitos dos utilizadores. Por outro lado, grande parte da informação partilhada na internet e nas redes móveis é informação sobre a localização geográfica e o recurso a tecnologias e meios de localização é cada vez mais frequente[203].

Atualmente, os dados de localização assumem especial relevância e diversas indústrias não funcionam sem estes dados. Olhemos para a indústria automóvel - em termos de *hardware* e de *software* – e para a prestação de serviços tais como a

[203] A título de exemplo, podemos indicar os serviços de navegação, os serviços realidade aumentada, a monitorização do paradeiro de amigos, o controlo de crianças, a publicidade baseada na localização, sistemas de portagem para automóveis, entre outros

Uber, Taxify ou Cabify, que beneficiam dos dados de localização para implementarem o seu modelo de negócio, apenas possível graças à combinação de localização de veículo e localização do requerente do serviço.

Iremos abordar o método de funcionamento dos três principais tipos de infraestruturas e mecanismos utilizados na obtenção de dados de geolocalização, designadamente GPS, estações de base GSM e WiFi, e a proteção dos dados obtidos por estas tecnologias no contexto comunitário e nacional.

DADOS DAS ESTAÇÕES DE BASE

De forma a poder aceder aos serviços de telecomunicações 3G ou superiores, o dispositivo móvel em questão deve estar conectado à antena ("estação de base") que assegura a cobertura pelo operador de telecomunicações na área geográfica em que se encontra ("célula")[204]. Sempre que esteja ligado e ativo, um dispositivo móvel está sempre ligado a uma determinada estação de base e o operador de telecomunicações que opera a respetiva estação de base procede ao registo contínuo das ligações feitas pelo dispositivo à estação.

Cada estação de base possui um código de identificação único e está registada com uma localização específica, o que permite que, tanto o operador de telecomunicações como os próprios dispositivos móveis, utilizem os sinais de células sobrepostas (ou seja, os sinais de estações de base vizinhas) para determinar a localização do dispositivo móvel com certa exatidão. Esta técnica é também conhecida como triangulação.

Ainda que este método forneça apenas uma indicação rápida e grosseira da localização, muito menos precisa do que a que pode ser obtida através de dados GPS e WiFi, a margem de erro é de cerca de 50 metros em zonas urbanas densamente povoadas e tem vindo a diminuir exponencialmente[205].

---

[204] As células abrangem zonas de dimensão diversa, variando em função do número de estações de base existentes e em funcionamento e das circunstâncias do ambiente e do clima, como por exemplo, a existência de montanhas ou edifícios altos.

[205] Segundo o Grupo do Artigo 29.º, a margem de erro pode chegar a vários quilómetros em zonas rurais, mas tem vindo a decrescer rapidamente. Ver Grupo do Artigo 29.º – **Parecer 13/2011**

TECNOLOGIA GPS

O *Global Position System* é a tecnologia mais utilizada nos dias de hoje para a obtenção de dados de localização. Atualmente, a grande maioria dos dispositivos móveis inteligentes estão equipados com circuitos integrados que constituem recetores GPS, ou seja, recetores que determinam a sua localização através da utilização de satélites colocados em diferentes órbitas e que calculam a longitude, latitude e altitude do dispositivo.

"*O sistema GPS baseia-se em 24 satélites, mais 4 de reserva, equipados com relógios atómicos, que giram em torno da terra, em diferentes órbitas, duas vezes por dia. (...). O recetor GPS recebe o sinal de 4 satélites, calculando em seguida a que distância cada um destes se encontra, através da medição do tempo que as ondas de sinal rádio demoram a chegar do satélite ao recetor. Este cálculo permite determinar a latitude, a longitude e a altitude do recetor*"[206]. Para o efeito da localização, cada satélite emite um sinal rádio muito preciso, sendo que a localização só é determinada quando o sensor GPS captar pelo menos quatro desses sinais[207].

PONTOS DE ACESSO WIFI

Outra fonte de dados de geolocalização são os pontos de acesso WiFi, cuja tecnologia é semelhante à utilizada para as estações de base na medida em que ambas se baseiam num identificador único que pode ser detetado pelo dispositivo móvel e enviado a um serviço que conhece a localização correspondente a esse identificador. O identificador único de cada ponto de acesso WiFi é o seu endereço

---

sobre serviços de geolocalização em dispositivos móveis inteligentes, 16 de Maio de 2011, p. 4. Disponível para consulta em http://www.gpdp.gov.mo/uploadfile/2014/0505/20140505071557367.pdf (17.03.2018).

[206] SILVA, Fernando – **Sistemas de geolocalização e monitorização de veículos: do início do GPS às novas tendências**, in *Fórum de Proteção de dados*, n.º3, julho, 2016, pp. 34

[207] Note-se que, ao contrário dos dados de localização obtidos através dos dados das estações de base, o sinal GPS é unidirecional e, assim sendo, as entidades que gerem os satélites não têm a possibilidade de manter registos dos dispositivos que receberam o sinal rádio. Nesse sentido, Grupo do Artigo 29.º, op. cit. p .5.

MAC, que corresponde a um identificador único atribuído a uma interface de rede e que, em geral, está registado no respetivo *hardware*[208].

A posição geográfica de cada ponto de acesso WI-FI é passível de ser determinada com relativa precisão dentro do limite de 20 metros. Com recurso a esta técnica, é possível determinar o momento em que o sinal é mais forte e revelar a posição com um recetor GPS. "A técnica utilizada é denominada de *wardriving*, utilizada em veículos equipados com um computador, uma placa WI-FI e um recetor GPS"[209].

Os dispositivos de localização podem ser divididos em duas categorias: os passivos e os ativos. «*Os dispositivos "passivos" armazenam as localizações GPS, velocidade, direção e, em alguns casos, eventos como início/paragem, porta fechada ou aberta, travagens, etc. Quando o veículo regressa ao local pré-determinado o dispositivo é removido ou envia os dados para um servidor para posterior avaliação dos mesmos. Os dispositivos "ativos", como o nome indica, além de recolherem informações como os passivos, transmitem-nas em tempo real (ou quase) através de rede de comunicações, sendo a mais comum a GSM, para um centro de dados. A combinação dos dois modos é a mais frequente. (...). A localização do veículo é assim obtida e registada pela utilização dos sistemas GPS e GSM, que se complementam na monitorização de um veículo em andamento e reportam o seu estado. Estes dispositivos de localização/monitorização de posição fornecem em tempo real a atividade dos veículos monitorizados, para dispositivos móveis ou para servidores que disponibilizam a informação em sites*».[210]

A GEOLOCALIZAÇÃO NO RGPD E NA DIRETIVA PRIVACIDADE E COMUNICAÇÕES ELETRÓNICAS

No âmbito do direito comunitário, o quadro jurídico aplicável aos dados de geolocalização é composto pelo RGPD e pela Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas

[208] O endereço MAC de um ponto de acesso WiFi denomina-se BSSID (*Basic Service Set Identifier* , ou seja identificador de componente básico de serviço.
[209] SILVA, Fernando, op. cit., pp. 36.

[210] SILVA, Fernando, op. cit., pp. 38.

(Diretiva Privacidade e Comunicações Eletrónicas)[211] [212], conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de novembro de 2009[213].

Tratamento realizado por operadores de telecomunicações

Nos termos da Diretiva Privacidade e Comunicações Eletrónicas, são dados de localização "*quaisquer dados tratados numa rede de comunicações eletrónicas ou por um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público*"[214] [215].

Ora, considerando que os dados das estações de base são continuamente tratados pelos operadores de telecomunicações no âmbito da sua oferta de serviços públicos de comunicações eletrónicas[216], na medida em que se relacionem com pessoas físicas identificadas ou identificáveis, os dados de localização derivados das estações de base são abrangidos pelas disposições que regem a proteção dos dados pessoais, constantes tanto do RGPD como da Diretiva 2002/58/CE.

---

[211] Em conformidade com o âmbito de aplicação material desta Diretiva, esta aplica-se apenas ao tratamento de dados das estações de base pelos serviços e redes de comunicações eletrónicas públicas. De facto, o número 1 do artigo 1.º da Diretiva 2002/58/CE determina que esta visa harmonizar "*as disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, no que respeita ao tratamento de dados pessoais no sector das comunicações eletrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na Comunidade*".

[212] Ver também Grupo do Artigo 29.º –**Parecer 13/2011 sobre serviços de geolocalização em dispositivos móveis inteligentes**, op. cit.

[213] A Diretiva n.º 2009/136/CE altera a Diretiva n.º 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor.

[214] Alínea c) do seu artigo 2.º.

[215] Se um operador de telecomunicações oferecer um serviço híbrido de geolocalização que se baseie também no tratamento de outros tipos de dados de localização, como os dados GPS ou WiFi, essa atividade é considerada um serviço público de comunicações eletrónicas.

[216] Note-se que a oferta de pontos de acesso WiFi público pelos fornecedores de serviços de telecomunicações é também considerada um serviço público de comunicações eletrónicas, pelo que deverá, acima de tudo, respeitar o disposto na Diretiva Privacidade e Comunicações Eletrónicas.

Nos termos do número 1 do artigo 9.º da Diretiva Privacidade e Comunicações Eletrónicas, apenas o consentimento[217] ou a anonimização[218] são fontes de legitimidade para o tratamento de dados de localização[219].

No âmbito da Diretiva Privacidade e Comunicações Eletrónicas, o único responsável pelo tratamento de dados é o próprio operador de comunicações eletrónicas e/ou os seus subcontratados.

Tratamento realizado por fornecedores de serviços da sociedade da informação

Normalmente, os serviços e aplicações de localização com recurso a uma combinação de dados de estações de base, GPS e WiFi são considerados serviços da sociedade da informação. Ora, estes serviços da sociedade de informação estão explicitamente excluídos do âmbito de aplicação da Diretiva Privacidade e

---

[217] O consentimento deve poder ser retirado a qualquer momento, sendo-lhe conferida também a possibilidade de "por meios simples e gratuitos, recusar temporariamente o tratamento desses dados para cada ligação à rede ou para cada transmissão de uma comunicação", nos termos do disposto no número 2 do artigo 9.º da Diretiva Privacidade.

[218] A anonimização deve ser distinguida da pseudonimização na medida em que a primeira "camuflagem das identidades" seja feita de modo a "impossível a reidentificação, por exemplo, através de criptografia de sentido único que, em geral, cria dados anónimos". Grupo de Trabalho do Artigo 29.º – **Parecer 4/2007 sobre o conceito de dados pessoais**, op. cit., p. 18.
Por outro lado, a "a criação de pseudónimos pode ser realizada mantendo a possibilidade de identificação, utilizando algoritmos de criptografia de duplo sentido. Grupo de Trabalho do Artigo 29.º – **Parecer 4/2007 sobre o conceito de dados pessoais**, op. cit., p. 18.
No mesmo sentido, o Grupo de Trabalho do artigo 29.º afirmou que "os dados pseudónimos identificáveis podem ser considerados como informação sobre pessoas que são diretamente identificáveis. De facto, utilizar um pseudónimo significa que é possível remontar até à pessoa, de modo que a identidade da pessoa pode ser a descoberta, mas isto apenas em circunstâncias pré-definidas. Nesse caso, apesar de se aplicarem as regras de proteção de dados, os riscos existentes para as pessoas no que toca ao tratamento dessa informação indiretamente identificável serão na maioria dos casos reduzidos, de forma que a aplicação destas regras será justificadamente mais flexível do que a informação tratada sobre pessoas diretamente identificáveis". Grupo de Trabalho do Artigo 29.º, op. cit., p. 22.
Numo outra perspetiva, o autor Alexandre Sousa Pinheiro, afirma que "*apesar do conceito amplo que a diretiva apresenta de dado pessoal, não parece que a sua funcionalização à identificação ou identificabilidade de pessoas singulares esgote a ratio do texto comunitário. Dados há que, provavelmente, ainda não permitem identificar um titular, mas permitem admitir a sua existência. Veja-se o recurso a alcunhas, nomes alterados ou pseudónimos, numa fase em que não seja identificável o titular dos dados. O mais que se pode afirmar consiste em verificar a probabilidade da existência de um titular de dados pessoais*". PINHEIRO, Alexandre Sousa – op. cit., p. 645.

[219] Nos casos em que são processados dados de localização, para além dos dados de tráfego, relativos a utilizadores ou assinantes de redes públicas de comunicações ou de serviços de comunicações eletrónicas publicamente disponíveis, esses dados só podem ser tratados se forem tornados anónimos ou com o consentimento dos utilizadores ou assinantes, na medida do necessário e pelo tempo necessário para a prestação de um serviço de valor acrescentado.

Comunicações Eletrónicas, com base na definição estrita de serviço de comunicações eletrónicas da Diretiva 2002/21/CE, de 7 de Março de 2002[220]. Assim sendo, a Diretiva Privacidade e Comunicações Eletrónicas não se pode aplicar ao tratamento de dados de localização por serviços da sociedade da informação, mesmo quando o referido tratamento seja efetuado através de uma rede pública de comunicações eletrónicas[221].

Nos casos em que a Diretiva Privacidade e Comunicações Eletrónicas não seja aplicável, em resultado do disposto no número 2 do seu artigo 1.º era aplicável a Diretiva 95/46/CE até à sua revogação, passando a ser aplicável o RGPD[222]. No entanto, para esta aplicação é necessário que se verifique o critério estabelecido para a determinação de dados pessoais.

No Considerando (26) do RGPD, relativo ao termo "identificável", pode ler-se o seguinte: "*Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica.*"[223]. Acontece que os dispositivos

---

[220] Nos termos da Diretiva 2002/21/CE, de 7 de Março de 2002, artigo 2.º, alínea c): «"Serviço de comunicações eletrónicas", o serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações eletrónicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão, excluindo os serviços que prestem ou exerçam controlo editorial sobre conteúdos transmitidos através de redes e serviços de comunicações eletrónicas; excluem-se igualmente os serviços da sociedade da informação, tal como definidos no artigo 1.º da Diretiva 98/34/CE que não consistam total ou principalmente no envio de sinais através de redes de comunicações eletrónicas.»

[221] Um utilizador pode optar por transmitir dados GPS através da Internet, nomeadamente quando acede a serviços de navegação na Internet. Nesse caso, o sinal GPS é transmitido no nível das «aplicações» da comunicação na Internet, independentemente da rede GSM. O fornecedor de serviços de telecomunicações atua como simples transportador e não tem qualquer acesso aos dados de localização, a menos que recorra a meios muito intrusivos, como a inspeção aprofundada dos pacotes.

[222] «Para os efeitos do n.º 1, as disposições da presente diretiva especificam e complementam a Diretiva 95/46/CE».

[223] No seu parecer sobre o conceito de dados pessoais, o Grupo de Trabalho do Artigo 29.º forneceu amplas orientações sobre a definição de dados pessoais. Grupo de Trabalho do Artigo 29.º –**Parecer 4/2007 sobre o conceito de dados pessoais**, adotado em 20 de junho. Disponível para consulta em http://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf (17.03.2018).

móveis inteligentes, através dos quais são utilizadas as tecnologias de localização, estão indissociavelmente ligados a pessoas singulares, pelo que da sua utilização resulta tanto uma identificabilidade direta como uma identificabilidade indireta.

Em primeiro lugar, o operador de telecomunicações possui, regra-geral, um registo do utilizador, de onde consta o seu nome, endereço, informação fiscal e as referências bancárias dos clientes, em combinação com vários números únicos do dispositivo, como o IMEI e o IMSI. Em segundo lugar, a compra de *software* suplementar (*aplicações*) para o dispositivo exige normalmente um número de cartão de crédito, o que enriquece a combinação de números únicos e dados de localização com dados de identificação direta. "*A identificação indireta pode obter-se através da combinação dos números únicos do dispositivo com uma ou várias posições determinadas por cálculo. Cada dispositivo móvel inteligente tem, pelo menos, um identificador único, o seu endereço MAC, mas pode ter outros números de identificação únicos, acrescentados pelo criador do sistema operativo*."[224] A transmissão e tratamento destes identificadores únicos no contexto dos serviços de geolocalização, conjugados com observações recorrentes pode resultar na identificação do proprietário do dispositivo[225]. Segundo o parecer 4/2007[226] sobre o conceito de dados pessoais, os identificadores únicos permitem rastrear o utilizador de um dispositivo específico e, por conseguinte, destacá-lo, mesmo quando o seu nome verdadeiro não é conhecido[227][228].

---

[224] Grupo de Trabalho do Artigo 29.º – **Parecer 13/2011 sobre serviços de geolocalização em dispositivos móveis inteligentes**, op. cit., p. 10.

[225] A facilidade de identificação do proprietário com base no endereço MAC depende do meio envolvente, sendo que em zonas pouco povoadas, nas quais o endereço MAC pode até apontar para uma única casa, o proprietário da mesma pode ser determinado diretamente com recurso a instrumentos públicos, tais como os registos prediais, as listas telefónicas, os registos eleitorais. Em zonas mais densamente povoadas, é possível, com base, na intensidade do sinal e/ou no SSID (que é passível de ser detetado por qualquer pessoa com um dispositivo dotado da função WiFi), determinar a localização precisa do ponto de acesso e, em muitos casos, a identidade da pessoa ou pessoas que vivem no local (casa ou apartamento) onde está instalado o ponto de acesso.
Há casos em que não é possível, sem um esforço irrazoável, identificar com precisão a pessoa que vive no apartamento onde se situa o ponto de acesso, mesmo recorrendo à informação sobre a intensidade do sinal. Isto acontece em zonas muito densamente povoadas, em que o endereço MAC aponta para vários apartamentos onde poderá situar-se o ponto de acesso.

[226] Grupo de Trabalho do Artigo 29.º –**Parecer 4/2007 sobre o conceito de dados pessoais**, op. cit., p.14 e 15.

[227] Esta identificabilidade indireta aplica-se igualmente aos pontos de acesso WiFi, sendo que os pontos de acesso WiFi podem mesmo ser diretamente identificáveis, caso o fornecedor de acesso à Internet mantenha um registo dos endereços MAC dos encaminhadores WiFi que fornece aos seus clientes identificados.

Assim, o RGPD será aplicável na exata medida em que os dados de localização configuram informação relativa a uma pessoa singular identificada ou identificável, nos termos dos artigos 2.º/2 e 4.º/1 do RGPD.

Tal como acima explicado no Capítulo relativo ao RGPD, as obrigações em matéria de proteção de dados resultantes do RGPD recaem sobre o responsável pelo tratamento (cf. número 2 d artigo 5.º/2). Acontece que, em função das três funcionalidades diferentes oferecidas por cada um, podemos ter três responsáveis pelo tratamento distintos: responsável pelo tratamento dos dados de uma infraestrutura de geolocalização[229], fornecedor de uma aplicação ou serviço específico de geolocalização[230] e criador do sistema operativo de um dispositivo móvel inteligente[231]. Acontece que, frequentemente, as grandes empresas desempenham simultaneamente duas ou até três destas funções.

Tal como definido na RGPD, os titulares dos dados têm o direito à informação, o direito de acesso e direito de oposição, à retificação, o *direito a ser esquecido* e o direito à portabilidade. (cf. capítulo acima relativa aos direitos dos titulares dos dados no âmbito do RGPD).

A GEOLOCALIZAÇÃO NO ÂMBITO DA LEGISLAÇÃO PORTUGUESA

Nos termos da Lei da Proteção de Dados, consubstanciam dados pessoais qualquer informação relativa a uma pessoa singular identificada ou identificável. Ora, os

---

[228] Convém lembrar que não é necessário que a finalidade do tratamento desses dados de geolocalização seja a identificação dos utilizadores. A necessidade de um esforço irrazoável para identificar os proprietários dos pontos de acesso WiFi é, em grande parte, determinada pelos meios técnicos de que o responsável pelo tratamento ou qualquer outra pessoa dispõe para identificar os utilizadores.

[229] Estes são os proprietários das bases de dados de pontos de acesso WiFi cartografados, na medida em que tratem dados pessoais quando calculam a localização de um determinado dispositivo móvel inteligente.

[230] O fornecedor de uma aplicação capaz de tratar dados da geolocalização é o responsável pelo tratamento dos dados pessoais resultantes da instalação e utilização dessa mesma aplicação. O Grupo de Trabalho do artigo 29.º refere como exemplo de casos em que o responsável é o fornecedor da aplicação os casos das aplicações de serviços meteorológicos. Grupo de Trabalho do artigo 29.º – **Parecer 13/2011 sobre serviços de geolocalização em dispositivos móveis inteligentes**, op. cit., p.13.

[231] O criador do sistema operativo do dispositivo móvel inteligente pode ser o responsável pelo tratamento dos dados de geolocalização se esse sistema interagir diretamente com o utilizador e recolher dados pessoais (nomeadamente quando exige o registo inicial do utilizador e/ou recolhe dados de localização para melhorar os serviços).

dados de localização são um elemento que permitem, com relativa facilidade, identificar um indivíduo, através do controlo dos seus hábitos comportamentais, percursos efetuados, tempos de permanência em cada local. Nessa exata medida, os dados de localização devem ser considerados dados pessoais e o seu tratamento (designadamente recolha, registo, conservação, consulta, entre outros) está abrangido pela Lei da Proteção de Dados.

Segundo Alexandre Sousa Pinheiro e Carolina Moura, "*as condições de legitimidade de tratamento de dados através da tecnologia de geolocalização diferirá consoante estivermos perante dados pessoais sensíveis ou não (cf. alínea e) do artigo 6.º ou n.º 2 do artigo 7.º da LPD)*."[232]

Assim, sempre que os dados de localização correspondam a dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, à saúde e à vida sexual, incluindo os dados genéticos, o seu tratamento será proibido nos termos previstos no artigo 7.º da Lei da Proteção de Dados. O tratamento destes dados será, todavia, possível mediante disposição legal ou autorização da CNPD nos casos previstos no número 2 do mesmo artigo 7.º.

Se os dados de localização não configurarem dados sensíveis, o seu tratamento será lícito desde que se verifique qualquer das circunstâncias de licitude previstas no artigo 6.º da Lei.

Tratamento realizado por operadores de telecomunicações

Em Portugal, a Diretiva n.º 2002/58/CE foi transposta para ordenamento jurídico português através da Lei n.º 41/2004, de 18 de agosto[233], que regula o tratamento

[232] PINHEIRO, Alexandre Sousa Pinheiro e MOURA, Carolina – "Utilizaçãode tecnologia de geolocalização e o tratamentode dados pessoais no regime jurídico português: a propósitoda Deliberaçãon.º 7680/2014 da ComissãoNacional de Protecçãode Dados e jurisprudência posterior", in Forum de Proteçao de dados, n.º3, julho, 2016, pp. 20

[233] Esta lei foi posteriormente alterada pela Lei n.º 46/2012, de 29 de agosto de 2012, que procede à transposição da Diretiva n.º 2009/136/CE 174.
O âmbito de aplicação da Lei n.º 46/2012 abrange o tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicação públicas, nomeadamente nas redes públicas de comunicações que sirvam de suporte a dispositivos

de dados pessoais e a proteção da privacidade no setor das comunicações eletrónicas. Entre as matérias reguladas por esta lei encontramos os serviços de localização do utilizador de um terminal de comunicações móveis[234], na medida em que "*atribuição de um local de referência para um equipamento terminal fixo constitui um dado indispensável ao próprio estabelecimento da prestação do serviço de comunicações*".

Tal como disposto no número 1 do artigo 9.º da Diretiva n.º 2002/58/CE, a Lei n.º 41/2004 também dispõe que o tratamento de dados de localização só será possível se esses dados relativos a assinantes ou utilizadores se tornarem anónimos ou ainda quando houver consentimento dos mesmos para a prestação de serviços de valor acrescentado[235], nos termos do disposto nos números 1 e 3 do artigo 7.º. Para efeitos do consentimento, os prestadores de serviços devem informar o utilizador acerca do tipo de dados de localização, para além dos dados de tráfego que, serão tratados, dos fins, da duração do tratamento, bem como da eventual transmissão a terceiros para fornecimento de serviço de valor acrescentado, antes da obtenção do consentimento dos utilizadores ou assinantes. Se o assinante e o utilizador não são a mesma pessoa, e se este vai ser localizado, sendo para tal a informação de localização um dado pessoal que lhe respeita, este deve consentir no seu uso.

Ainda que o consentimento para determinado tratamento de dados de localização tenho sido concedido pelo seu titular, o utilizador ou assinante, sempre deverá ter a possibilidade de recusar temporariamente o tratamento desses dados, de forma gratuita e por meios simples.

---

de recolha de dados e de identificação, especificando e complementando as disposições da Lei n.º 67/98, de 26 de outubro175.Esta Lei introduziu novas definições, nomeadamente as definições de comunicação e de dados de localização, sendo que esta última passou a incluir os dados tratados no âmbito de um serviço de comunicações eletrónicas. Ver as alíneas a), b) e) e g) do número 1 do arrigo 2.º da Lei n.º 46/2012, de 29 de agosto.

[234] O regime jurídico aplicável aos dados de localização resulta do disposto no art.º 7.º da Lei n.º 41/2004, aplicável aos casos "em que sejam processados dados de localização, para além dos dados de tráfego", no que diz respeito ao regime legal apenas abrange aqueles dados de localização que não devam ser considerados como dados de tráfegos e submetidos ao preceito do artigo 6.º.

[235] Nos termos do disposto no número 3 do artigo 7.º, ainda que haja consentimento do titular dos dados, o tratamento é apenas permitido na medida e pelo tempo necessário para a prestação dos serviços de valor acrescentado.

O legislador nacional, em transposição da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, veio, na Lei n.º 32/2008, de 17 de julho, impor às empresas que prestam serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas o dever de conservação de tais dados pessoais e da sua transmissão para efeitos de investigação de crimes graves. Nos termos desta lei, o legislador prevê um regime excecional face à a proibição geral de conservação e acesso aos dados pessoais relativos a comunicações eletrónicas estabelecida na Lei n.º 41/2004. Dentre estes dados estão também os dados de localização.

Acontece que a Diretiva que a Lei n.º 32/2008 transpõe foi declarada inválida pelo Tribunal de Justiça da União Europeia (TJUE) – no acórdão de 8 de abril de 2014, processos C-293/12 e C-594/12 – e que o legislador nacional ainda não retirou as consequências devidas de tal declaração. Ora, esta situação gera desconformidades entre a legislação nacional e a comunitária, que irão impor a intervenção do legislador.

O CASO ESPECÍFICO DOS CARROS VEÍCULOS SEM CONDUTOR E DOS VEÍCULOS CONECTADOS

Temos assistido à crescente difusão da inteligência artificial e os carros sem condutor são provavelmente o exemplo mais conhecido da inteligência artificial e da robótica.

Os *self-driving cars* (também chamados de carro sem condutor ou carro autónomo) são veículos programados com inteligência artificial que os torna capazes de realizar percursos sem qualquer intervenção humana. Estes carros apresentam diversas vantagens, mas não são isentos de contras [236]. Independentemente da posição ética que se tome em relação a estes carros autónomas, a verdade é que estes automóveis recorrem à utilização de dados que, na maior parte das vezes, são dados pessoais. "*Para funcionarem, os carros sem condutor precisam de uma*

[236] Recorde-se o atropelamento por um carro autónomo de testes de Uber, ocorrido no estado do Arizona, nos Estados Unidos, que resultou na morte de uma mulher. A notícia pode ser consultada em https://www.publico.pt/2018/03/19/tecnologia/noticia/carro-sem-condutor-mata-mulher-e-leva-uber-a-parar-testes-1807243 (07.07.2018).

cartografia tão perfeita quanto possível, bem como de tanta informação quanto viável sobre os outros veículos e as suas viagens (por exemplo, para a gestão do congestionamento do trânsito)"[237]. Necessitam também de informação relativa ao destino, itinerário e utilizador do serviço.

Ora, em relação aos dados de localização a serem utilizados pelos *self-driving cars,* e considerando a ausência de um quadro legal específico, o regime irá depender da possibilidade de identificação de um titular daqueles dados com recursos razoáveis, tanto para efeitos do RGPD quanto para efeitos da Lei da Proteção de Dados nacional (nos termos dos artigos 2.º/2 e 4.º/1 do RGPD, e dos artigos 3.º/1 e 4.º/a) da Lei da Proteção de Dados). Caso a identificação do titular seja possível, estamos perante dados pessoais a serem tratados no cumprimento das disposições daqueles dois diplomas.

No que se refere à Diretiva n.º 2002/58/CE, a nível comunitário, e à Lei n.º 41/2004, de 18 de agosto, a nível nacional, a aplicação destes dois diplomas ficará dependente da concreta configuração do sistema.

Ora vejamos, nos modelos de carros autónomos atualmente em fases de testes, os serviços de conectividade necessários são prestados por operadores de telecomunicações aos quais os fabricantes contratam os serviços de comunicações eletrónicas – não sendo prestados pelo "próprio carro" (entenda-se, pelo fabricante ou prestador de serviço automóvel). Assim sendo, quer-nos parecer que existem bases sólidas para concluir ao tratamento de dados realizado por carros autónomos não será de aplicar o regime relativo aos serviços de comunicações eletrónicas.

Para esta conclusão concorrem os factos de os serviços prestados pelos carros autónomos estarem estão fora do escopo de aplicação da Lei Portuguesa de Comunicações Eletrónicas (Lei n.º 5/2004, de 10 de fevereiro, alterada por diversas vezes, sendo a última alteração introduzida pelo Decreto-Lei n.º 92/2017, de 31 de julho ("Lei das Comunicações Eletróncias), já que não se qualificam como "serviços de comunicações eletrónicas", na aceção do artigo 3.º, alínea ff), da Lei das Comunicações Eletrónicas.

[237] BUTTARELLI, Giovanni, op. cit. pp. 33.

A Lei das Comunicações Eletrónicas define, no seu artigo 3.º, alínea f), que serviço de comunicações eletrónicas como "*o serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações eletrónicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão, sem prejuízo da exclusão referida nas alíneas a) e b) do n.º 1 do artigo 2.º*". O nº 1, alíneas a) e b), do artigo 2º, referido na definição citada, excluem os «*serviços da sociedade da informação, definidos no Decreto-Lei n.º 58/2000, de 18 de Abril, que não consistam total ou principalmente no envio de sinais através de redes de comunicações eletrónicas;* b) *os serviços que prestem ou exerçam controlo editorial sobre conteúdos transmitidos através de redes e serviços de comunicações eletrónicas, incluindo os serviços de programas televisivos e de rádio e os serviços de audiotexto e de valor acrescentado baseados no envio de mensagem*».

A definição de "serviço de comunicações eletrónicas" para efeitos da Lei das Comunicações Eletrónicas é, conforme acima demonstrado, essencialmente idêntica à estabelecida na diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (Diretiva-quadro), para a qual remete a Diretiva Privacidade e Comunicações Eletrónicas. Esta definição centra-se também nos seguintes três critérios:

a. O serviço deve ser normalmente prestado por remuneração;
b. O serviço deve consistir, total ou principalmente, no encaminhamento de sinais em redes de comunicações eletrónicas;
c. O serviço deve consistir na transmissão de conteúdo (e não na produção de conteúdo).

Ressalva-se que o regulador nacional do sector das telecomunicações, a ANACOM, ainda não emitiu quaisquer decisões ou pareceres especificamente sobre esta definição ou sobre a sua aplicação a casos concretos.

No que toca à remuneração, assumiremos, como parece ser a intenção dos fabricantes e prestadores de serviços, que os serviços dos carros autónomos serão oferecidos mediante uma contraprestação a ser incluída no preço de compra do veículo ou de quaisquer componentes adicionais ou de serviços de manutenção.

Tendo isto em conta, é nossa opinião que os serviços são prestados em troca de remuneração, para os fins da definição contida no artigo 3, alínea ff) da Lei das Comunicações Eletrónicas.

Passando para o segundo ponto, não parece que os serviços dos carros autónomos consistam "total ou principalmente" na transmissão de um sinal, pelo que os fabricantes automóveis ficariam excluídos de se qualificar como prestadores de serviços de comunicações eletrónicas. Esta avaliação está altamente relacionada com o terceiro critério, em relação à transmissão de conteúdo.

Nos termos do número do artigo 2.º, alínea b), da Lei das Comunicações Eletrónicas, os serviços que fornecem ou que exercem o controlo editorial do conteúdo transmitido através de redes de comunicações eletrónicas não são abrangidos pelo seu âmbito de aplicação. Para qualificar os serviços como serviços de comunicações eletrónicas, é essencial determinar se são predominantemente baseados na transmissão de sinais ou se apresentam principalmente um caráter de conteúdo. Embora os serviços dos carros autónomos envolvam a transmissão de sinais, como mencionado anteriormente, o seu foco principal não reside no transporte de sinal. Na verdade, o transporte de sinal constitui um requisito técnico e operacional para a prestação dos serviços, mas não o próprio núcleo daqueles. O foco principal é permitir o intercâmbio de informações técnicas relevantes sobre os veículos e permitir que aqueles possam aceder a uma ampla gama de conteúdos informativos sobre localização, informações de tráfego, previsão do tempo, etc.[238]

No entanto, esta conclusão não é totalmente infalível na medida em que os serviços são efetivamente prestados pelo fabricante automóvel ou prestador de serviços ao utilizador.[239]

---

[238] Sobre o tema, ver o relatório do Organismo de Reguladores Europeus das Comunicações Electrónicas (" BEREC "), intitulado "**Enabling the Internet of Things**", de 12 de fevereiro de 2016, disponível e acessível em https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things (21.07.2018).

[239] Ainda assim, o referido Relatório do BEREC aponta também para a não qualificação dos serviços de carros autónomos como serviços de comunicações eletrónicas, tendo em conta a definição constante da Diretiva-Quadro. Com relação especificamente ao caso de um «*usuário de IoT (por exemplo, fabricante de automóveis, fornecedor de eletricidade) ", o relatório indica que "normalmente, um usuário de IoT que inclui conectividade como um produto de entrada em seus produtos ou serviços*

Assim, e em consequência do exposto, a Diretiva n.º 2002/58/CE e a Lei n.º 41/2004 não seriam aplicáveis ao fabricante automóvel ou prestador de serviços de carros autónomos. No entanto, continuariam sim a ser aplicáveis aos operadores de comunicações eletrónicas nos termos gerais, conforme o regime já descrito.

O mesmo entendimento acima explicitado deverá ser igualmente aplicado, com as necessárias adaptações, aos carros que não sendo autónomos, são "carros conectados"[240].

não parece fornecer um ECS ao vender um dispositivo conectado ou serviço "inteligente" (a menos que revenda total ou principalmente a conectividade com seus clientes). Nesse caso, o usuário da IoT é semelhante a um produtor e/ou fornecedor de equipamento terminal».

[240] São considerados carros conectados aqueles veículos capazes de otimizar sua própria operação e manutenção através do recurso a sensores de bordo e utilizam tecnologias de comunicação para interagir com o motorista, outros carros na estrada; infraestruturas na beira da estrada; com a nuvem e qualquer outro dispositivo inteligente. Mais informação sobre as valias tecnológicas pode ser consultada em http://autocaat.org/Technologies/Automated_and_Connected_Vehicles/ (11.08.2018).

CONCLUSÕES

A informação é cada vez mais valiosa e, com os avanços tecnológicos, é tratada cada vez mais, mais rápido e em maiores quantidades. Nesse contexto, surge a necessidade de proteger a informação relacionados com os indivíduos, conferindo-lhes o direito de dispor da informação que lhe diga respeito. Começam então a surgir diversos diplomas que regulam os direitos dos titulares de informação pessoal, face à nova realidade da sociedade de informação.

Em resultado das diversas construções que foram desenvolvidas sobre o direito à proteção de dados, atualmente decorre claro que este direito está intrinsecamente relacionado com o princípio da dignidade da pessoa humana.

Analisámos a evolução da *privacy* nos Estados Unidos e da Datenschutz na Alemanha, com as consequências que destes paradigmas decorreram para o direito internacional, comunitário e português. Principalmente no caso Alemão, foram visíveis as influências que a Datenschutz e a demarcação do direito à autodeterminação informacional tiveram no quadro jurídico europeu.

Quanto ao âmbito da geolocalização, abordamos os aspectos ligados às comunicações eletrónicas.

É de notar que o quadro jurídico objeto da presente dissertação sofrerá alterações em breve. De facto, em de janeiro de 2018, a Comissão Europeia tornou pública a proposta de Regulamento sobre Privacidade e Comunicações Eletrónicas (Regulamento ePrivacy), que deverá substituir a Diretiva 2002/58/CE (Diretiva e-Privacy). A proposta, que visa complementar o Regulamento Geral sobre a Proteção de Dados (RGPD), surge com o propósito declarado de adaptar o quadro jurídico vigente em matéria de privacidade à nova realidade tecnológica e ao desenvolvimento do mercado. A nível nacional, já foi objeto de consulta a Proposta de Lei n.º 120/XIII/3.ª (GOV), que pretende assegurar a execução, na ordem jurídica nacional do RGPD. Em conformidade, a sua aprovação deverá estar para breve.

BIBLIOGRAFIA

WEBB, Diana **- *Privacy and Solitude***. Londres/Nova Iorque: Hambledon Continuum, 2007.

FESTAS, David de Oliveira **- *Do conteúdo patrimonial do direito à imagem***. Coimbra: Coimbra Editora, 2009.

WARREN, Samuel D. e Brandeis, Louis D. **- *The Right to Privacy***, in Harvard Law Review, Volume IV, n.º 15, 15 de dezembro de 1890.

SOLOVE, Daniel J. e SCHWARTZ, Paul M. **- *Privacy and the Media.*** Austin, Boston, Chicago e Nova Iorque: Wolters Kluwer, 2008.

Cooley, Thomas – ***A Treatise on the Law of Torts*, or the Wrongs which arise independent of Contract**. Chicago: Callaghan, 1888.

PRATT, Walter F.**- *Privacy in Britain***. Londres: Bucknell University press, 1979.

SOMA, John T **– *Privacy law***.St. Paul: Thomson/West, 2008.

ROSSER, William Lloyd **– *Privacy.*** California Law Review, vol. 48, 1960.

ALLEN, Anita L. e MACK, Erin **– How Privacy Got its Gende.** Northen Illinois Law Review, vol. 10, 1999-2000.

ZIMMERMAN, Diane L. **– Requiem to a Heavyweight: A Farewell to Warren and Brandeis**. Connecticut Law Review, vol. 68, 1982-83.

BARRON, James H. **– Warren and Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890): Desmystifying a Landmark Citation.** Suffolk University Law Review, vol. XIII, 1979.

WESTIN, Alan, **– Privacy and Freedman**. Londres: The Bodley Head, 1970.

PEMBER, Don R. **– Privacy and the Press. The Law, The Mass Media and the First Amendment.** Seatle/Londres: University of Washington Press, 1972.

KAMLAH, Ruprecht **- Right of privacy**, 1969.

BLOUSTEIN, Edward J. **- Privacy as an aspect of human dignity: an answer to dean Prosser**. New York University Law Review, v. 32, 1964..

RICHARDS, Neil M. **- Griswold v. Connecticut**, in Encyclopedia of Privacy, vol. I.

GARROW,David J. – **Liberty and Sexuality. The Right to Privacy and making of Roe v. Wade**. Berkeley, Los Angeles e Londres: University of California Press.

National Consumer Law Center – **Fair Credit Reporting Act**, Connecticut: Grolier Educational Corporation, 1988.

LINDON, Raymond – ***Une Création Prétorienne: Les droits de la Personnalité***", Paris: Dalloz, 1974.

CORDEIRO, António Menezes – **Tratado de Direito Civil Português: Parte Geral – Pessoas. Vol. 1, tomo III**. Lisboa: Almedina, 2004.

Conselho da Europa, "**Manual da legislação Europeia sobre protecção de dados**", p. 14 e 15. Disponível em https://www.cnpd.pt/bin/legis/internacional/fra-2014-handbook-data-protection-pt.pdf

RAMIRO, Mónica Arenas – **El Derecho Fundamental a la Protección de Datos Personales en Europa**. Valência: Tirant lo Blanch, 2006, p. 56.

GONÇALVES, Maria Eduarda – "A Proteção de Dados Pessoais em Direito Internacional e em Direito Interno, **Revista do Ministério Público**, ano 10, n.º 40, 1989, p. 101 *apud* PINHEIRO, Alexandre Sousa, op. cit.,p. 660.

Comissão Europeia – **Comunicado de imprensa da Comissão Europeia**, de 21 Dezembro de 2015, disponível para consulta em http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (17.03.2018)

CASTRO, Catarina Sarmento e – **Direito da Informática, Privacidade e Dados pessoais**. Coimbra: Edições Almedina.

CASTRO, Catarina Sarmento – **Privacidade Versus Publicidade: Proteção de Informações Pessoais e Atividade Registral**. Coimbra: Coimbra Editora.

TEIXEIRA, Maria Leonor da Silva - **A União Europeia e a Protecção de Dados Pessoais – Uma visão futurista**. Lisboa: Sindicato dos Magistrados do Ministério Público.

PINHEIRO, Alexandre de Sousa – **A proteção de dados na proposta de regulamento comunitário apresentada pela Comissão Europeia (2012): primeiras reflexões**. Lisboa: Diário de Bordo, p. 9 e 10.

PINHEIRO, Alexandre de Sousa – **Privacy e proteção de dados pessoais: a construção dogmática do Direito à identidade informacional**. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 2015.

MARQUES, Garcia; MARTINS, Lourenço – **Direito da Informática**. Coimbra: Edições Almedina.

Grupo do Artigo 29.º – **Parecer 13/2011 sobre serviços de geolocalização em dispositivos móveis inteligentes**, 16 de Maio de 2011, p. 4. Disponível para consulta em http://www.gpdp.gov.mo/uploadfile/2014/0505/20140505071557367.pdf (17.03.2018).

Grupo de Trabalho do Artigo 29.º –**Parecer 4/2007 sobre o conceito de dados pessoais**, adotado em 20 de junho. Disponível para consulta em http://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf (17.03.2018).

CALVÃO, Filipa - **O modelo de supervisão de tratamentos de dados pessoais na União Europeia: da atual diretiva ao futuro regulamento**, in *Fórum de Proteção de Dados*, n.º 1, julho. 2015.

GONÇALVES, Pedro Costa - **Reflexões sobre o Estado Regulador e o Estado Contratante**, in *Direito Público e Regulação 8*, Cedipre, Coimbra Editora, Coimbra 2013.

LOPES, Joaquim de Seabra – **O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível**, *in Fórum de Proteção de Dados*, n.º 2, jan. 2016.

MOUTINHO, José, «Legislador português. Precisa-se. Algumas notas sobre o regime sancionatório no Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679), in *Fórum de Proteção de Dados*, n.º 4, julho. 2017.

BUTTARELLI, Giovanni – **Inteligência Artificial, Robótica, Privacidade e Proteçãode Dados**, in *Fórum de Proteção de Dados*, n.º 4, julho, 2017.

PINHEIRO, Alexandre Sousa Pinheiro e MOURA, Carolina –**Utilização de tecnologia de geolocalização e o tratamento de dados pessoais no regime jurídico português: a propósito da Deliberação n.º 7680/2014 da Comissão Nacional de Proteção de Dados e jurisprudência posterior**, in *Fórum de Proteção de Dados*, n.º3, julho, 2016.

SILVA, Fernando – **Sistemas de geolocalização e monitorização de veículos: do início do GPS às novas tendências**, in *Forum de Proteçao de Dados*, n.º 3, julho, 2016.

Organismo de Reguladores Europeus das Comunicações Electrónicas (" BEREC ") – Relatório intitulado "**Enabling the Internet of Things**", de 12 de fevereiro de 2016. Disponível para consulta em https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things (21.07.2018).