REVISTA DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

LISBON LAW REVIEW

Número Temático: Tecnologia e Direito

ANO LXIII 2022 NÚMEROS 1 E 2

REVISTA DA FACULDADE DE DIREITO
DA UNIVERSIDADE DE LISBOA
Periodicidade Semestral
Vol. LXIII (2022) 1 e 2

LISBON LAW REVIEW

COMISSÃO CIENTÍFICA

Alfredo Calderale (Professor da Universidade de Foggia)
Christian Baldus (Professor da Universidade de Heidelberg)
Dinah Shelton (Professora da Universidade de Georgetown)
Ingo Wolfgang Sarlet (Professor da Pontifícia Universidade Católica do Rio Grande do Sul)
Jean-Louis Halpérin (Professor da Escola Normal Superior de Paris)
José Luis Díez Ripollés (Professor da Universidade de Málaga)
José Luís García-Pita y Lastres (Professor da Universidade da Corunha)
Judith Martins-Costa (Ex-Professora da Universidade Federal do Rio Grande do Sul)
Ken Pennington (Professor da Universidade Católica da América)
Marc Bungenberg (Professor da Universidade do Sarre)
Marco Antonio Marques da Silva (Professor da Pontifícia Universidade Católica de São Paulo)
Miodrag Jovanovic (Professor da Universidade de Belgrado)
Pedro Ortego Gil (Professor da Universidade de Santiago de Compostela)
Pierluigi Chiassoni (Professor da Universidade de Génova)

DIRETOR

M. Januário da Costa Gomes

COMISSÃO DE REDAÇÃO

Paula Rosado Pereira
Catarina Monteiro Pires
Rui Tavares Lanceiro
Francisco Rodrigues Rocha

SECRETÁRIO DE REDAÇÃO

Guilherme Grillo

PROPRIEDADE E SECRETARIADO

Faculdade de Direito da Universidade de Lisboa
Alameda da Universidade – 1649-014 Lisboa – Portugal

EDIÇÃO, EXECUÇÃO GRÁFICA E DISTRIBUIÇÃO
LISBON LAW EDITIONS

Alameda da Universidade – Cidade Universitária – 1649-014 Lisboa – Portugal

ISSN 0870-3116 Depósito Legal n.º 75611/95

Data: Outubro, 2022

ÍNDICE 2022

LIVROS & ARTIGOS

O consentimento do titular de dados no contexto da *Internet*

The consent of the data subject in the Internet

Mariana Pinto Ramos[*]

Resumo: A *Internet* coloca diversos desafios no âmbito da privacidade e proteção de dados. Nesse contexto, o consentimento do titular de dados poderá, enquanto ato positivo com relevância jurídica, ser entendido como

Abstract: The *Internet* poses several challenges in the context of privacy and data protection. Thus, the data subject's consent may, as a positive act with legal relevance, be understood to legitimize the processing of personal

[*] Doutoranda em Ciências Jurídico-Empresariais pela Faculdade de Direito da Universidade de Lisboa. Advogada.

Abreviaturas mais utilizadas: AEPD – *Agencia Española de Protección de Datos*; CC – Código Civil, aprovado pelo Decreto-Lei n.º 47344/66, de 25 de novembro; CDFUE – Carta dos Direitos Fundamentais da União Europeia; CE – Conselho de Europa; cf. – Confrontar; Cit./ Op. Cit. – Citado, *opus citatum*; CNIL – *Commission Nationale de l'Informatique et des Libertés*; CNPD – Comissão Nacional de Proteção de Dados; COM – Comissão Europeia; Coord.(s) – Coordenação / Coordenados; CRP – Constituição da República Portuguesa; DCE – Diretiva 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno ("Diretiva sobre o Comércio Eletrónico"); DEP – Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas ("Diretiva *E-Privacy*"); DPD – Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ("Diretiva de Proteção de Dados Pessoais"); EDPB – *European Data Protection Board*; EDPS – *European Data Protection Supervisor*; EEE – Espaço Económico Europeu; EM – Estado(s)-Membro(s); EUA – Estados Unidos da América; GT29 – Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados da Comissão Europeia; ICO – *Information Commissioner's Office*; *i.e* – *id est*; LCCG – Decreto-Lei n.º 446/85 de 25 de outubro ("Lei das Cláusulas Contratuais Gerais"); LEN – Lei n.º 58/2019, de 8 de agosto ("Lei de Execução Nacional do RGPD"); n.º(s) – Número(s); p./pp. – página e páginas; RGPD – Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril, 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"); TC – Tribunal Constitucional; TEDH – Tribunal Europeu dos Direitos do Homem; TFUE – Tratado sobre o Funcionamento da União Europeia; TJUE – Tribunal de Justiça da União Europeia; TUE – Tratado da União Europeia; UE – União Europeia; vol. – Volume.

forma de legitimar o tratamento de dados pessoais. Sucede que, não obstante a sua positivação legal para efeitos do RGPD, a noção de consentimento suscita diversos problemas cuja resolução resulta de uma (necessária) articulação entre diversos instrumentos normativos, incluindo com a dogmática civilística nacional. Deste modo, o presente estudo visa proceder à análise e problematização da natureza jurídica e dos elementos caracterizadores do conceito de consentimento do titular de dados à luz do RGPD e dos demais instrumentos normativos aplicáveis em matéria de regulação da *Internet*.

Palavras-chave: Consentimento; Proteção de Dados; *Internet.*

data. Notwithstanding its legal recognition in the GDPR, the notion of consent raises various problems whose solution arises from a (necessary) articulation between various different normative acts, including the national civil law doctrine. Thus, this study aims to analyse and address the legal nature and the elements that define the concept of consent of the data subject according to GDPR and other legal acts applicable to *Internet* regulation.

Keywords: Consent; Data Protection; *Internet.*

1 Introdução

1.1 Identificação e delimitação do âmbito do estudo

A *Internet*[1] caracteriza-se pela sua a-territorialidade, o que dá origem a múltiplas dificuldades em termos de atribuição de um facto e da sua classificação jurídica, bem como em termos de responsabilidade, criminalização, jurisdição territorial e, por último, de lei aplicável[2].

A utilização da *Internet* pelos utilizadores ("users") coloca diversos desafios já conhecidos no âmbito da privacidade e proteção de dados. No entanto, a verdade é que, apesar dos riscos, ninguém se inibe de utilizar a *Internet* no seu dia-a-dia. Existe, portanto, uma gestão de risco (à partida consciente)[3] do *user* na utilização

---

[1] O conceito de *Internet* foi avançado, pela primeira vez, pela *Federal Networking Council*, na sua Resolução de 24 de outubro de 1995, onde foi dada a seguinte definição: "*Internet* refers to the global information system that – (i) is logically linked together by a globally unique address space based on the *Internet* Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/*Internet* Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein." – para mais desenvolvimentos sobre a história da *Internet*, cf. Barry M. Leiner *et. al.*, *Brief History of the Internet*, *Internet* Society, 1997, disponível *online* em www.internetsociety.org. Também referida como "a rede das redes" (ou "network of networks"), a *Internet* é "uma rede mundial de redes informáticas que partilham uma tecnologia de comunicação comum" – neste sentido, cf. Luís de Lima Pinheiro, "Direito aplicável aos contratos celebrados através da *Internet*", in *Direito da Sociedade de Informação*, VII, 2008, pp. 363 e ss.

[2] Cf. Celine Husson-Rochcongar, "La Gouvernance D'*Internet* et les droits de l'Homme", in Quentin Van Enis et Cécile de Terwangne (dir.), *L'Europe des Droits de l'Homme à l'heure d'Internet*, Ed. Bruylant, Bélgica, 2019, p. 49. Para a Autora, o estudo da *Internet* apresenta-se como um problema de Direito Internacional Privado, por excelência, face à impossibilidade de resolução, a nível interno, dos diversos problemas que coloca. Ao nível da jurisprudência, cf. Acórdão do TEDH, caso n.º 2872/02, de 2 de dezembro de 2008, *K.U. vs Finlândia*, no qual se discutiu, em particular, se o Estado Finlandês não tinha cumprido a sua obrigação positiva de proteger o direito ao respeito pela vida privada do Autor, nos termos do artigo 8º da CDFUE.

[3] O que nem sempre acontece, na medida em que, de acordo com estudos comportamentais efetuados no âmbito da *Internet*, verifica-se que, na sua maioria, os utilizadores não leem os termos e condições *online*, não têm capacidade ou conhecimentos para compreender o que estão a ler ou até preferem partilhar mais informação do é que necessário para subscrever serviços mais rapidamente. Cf. René Arnold / Annette Hillebrand / Martin Waldburguer, "Informed Consent in Theorie und Praxis – Warum Lesen, Verstehen und Handeln auseinanderfallen", in *39 DuD*, 2015, (pp. 730-734) p. 731; Yannis Bakos / Florencia Marotta Wurgler / David R. Trossen, "Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts", in *The Journal of Legal Studies*, vol. 43, n.º 1, 2014, pp. 1-35; Johan Högberg, The effect of effort, control and value frames on

da *Internet*, quer no âmbito da tutela da privacidade, quer da tutela da proteção de dados[4], quando este acede a *sites* ou disponibiliza os seus dados pessoais para diversos efeitos.

O consentimento poderá, então, ser entendido como forma de legitimar o tratamento de dados pessoais, neste caso em particular, dos *users* no âmbito da *Internet*. A tutela dos dados pessoais e o conceito de consentimento, no âmbito da proteção de dados, pressupõem um ato positivo que, como veremos, tem relevância jurídica.

Na ordem jurídica supranacional, a proteção de dados está consagrada, como direito fundamental, nos termos da CDFUE, a par com o direito ao respeito pela vida privada e familiar[5]. Por sua vez, na ordem jurídica portuguesa, a proteção dos

---

online users privacy decision (Dissertation), 2013, disponível *online* em www.kau.diva-portal.org/. Adicionalmente, a análise sociodemográfica das perceções dos riscos associados à divulgação de informações pessoais aquando da criação de redes sociais mostra que a idade, a educação e a ocupação fazem toda a diferença – cf. COM, "Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union", 2011, pp. 62-63, disponível *online* em www.ec.europa.eu. A 30 de julho de 2020, o *World Economic Forum* publicou o seu White Paper: "Redesigning Data Privacy: Reimagining Notice & Consent for human tecnhnology Interaction", no qual adverte para os riscos do consentimento *online*, esclarecendo a necessidade de se adotar estratégias focadas na tutela de todo o tipo de utilizadores, incluindo aqueles que sejam particularmente vulneráveis e menos esclarecidos – disponível *online* em www.weforum.org.

[4] Cf. Nicola Lugaresi, "Principles and Regulations about Online Privacy: 'Implementation Divide and Misunderstanding in the European Union", in *TPRC*, Working Paper n.º 42, 2002, pp. 1-23, disponível *online* em www.ssrn.com. A Autora refere que a proteção da privacidade na *Internet* é muitas vezes confundida com a legislação de proteção de dados pessoais e observa que a proteção da privacidade é frequentemente ajustada para satisfazer as necessidades de proteção de dados pessoais. Certamente, a lei de proteção de dados pessoais é uma faceta da proteção da privacidade, mas a privacidade tem muitas *nuances* e abrange tanto mais como menos do que a noção de dados pessoais. Para mais desenvolvimentos sobre o impacto da *Internet* na vida privada dos internautas e dos seus dados pessoais, cf. Cecile de Terwagne, "*Internet* et la Protection de La Vie Privée et des données à caractere personnel", in *L'Europe des Droits de l'Homme à l'heure d'Internet*, Ed. Bruylant, Bélgica, 2019, pp. 325-368.

[5] Sobre a autonomização dos direitos à privacidade e da proteção de dados, alguma doutrina descreve a privacidade e a proteção de dados como direitos fundamentais diferentes, mas complementares. Por defeito, a lei da privacidade protege a opacidade do indivíduo através de medidas proibitivas (de não-interferência), enquanto a proteção de dados exige transparência do processador de dados pessoais, permitindo o seu controlo pelos indivíduos, estados e autoridades. Enquanto a privacidade constrói um "escudo" em torno do indivíduo, criando uma zona de autonomia e liberdade, a proteção de dados coloca a atividade do processador em destaque, conferindo ao indivíduo direitos subjetivos para controlar o tratamento dos seus dados pessoais e reforça a responsabilidade do processador. Ferramentas de opacidade, como as da privacidade, estabelecem limites à ingerência do poder com a autonomia do indivíduo e, como tal, têm uma forte natureza normativa, enquanto

dados pessoais constitui um direito fundamental[6], sendo que a necessidade de consentimento decorre, desde logo, do artigo 35.º da CRP e de diversos preceitos normativos do CC referentes à tutela de direitos de personalidade. Ademais, a força normativa do consentimento reflete-se, igualmente, através do RGPD, enquanto regulamento de aplicação direta (artigo 288º do TFUE) em todos os EM da UE e que visa a unificação dos direitos internos, mas também na LEN[7].

---

os instrumentos de transparência, tais como a proteção de dados, tendem a regular o exercício aceite do poder canalizando-o, regulando-o e controlando-o – neste sentido, cf. S. Gutwirth / Paul De Hert, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in E. Claes / A. Duff / S. Gutwirth, *Privacy and the criminal law,* Antwerp/Oxford, Intersentia, 2006, pp. 61-104. Em sentido contrário, o TJUE tem reiterado a proximidade entre o direito à proteção de dados e o direito à intimidade da vida privada, previsto no artigo 7º da CDFUE. É o caso do Acórdão *Schecke* (Casos C-92/09 e C-93/09) de 9 de novembro de 2010, n.º 47; e, mais precisamente, do Acórdão *Digital Rights Ireland* (Casos C-293/12 e C-594/14 de 8 de abril de 2014). Nestes últimos casos, estava em causa a compatibilização da Directiva 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 electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE, com o disposto na CDFE em matéria de proteção de dados e de privacidade. Segundo o órgão jurisdicional de reenvio, existem dúvidas, por um lado, quanto ao facto de esta Diretiva poder alcançar os objetivos que prossegue e, por outro, quanto ao caráter proporcionado da ingerência nos direitos fundamentais em causa. Assim, pronunciou-se o TJUE referindo que, por um lado, "[n]o caso vertente, tendo em conta, por um lado, o importante papel desempenhado pela proteção dos dados pessoais na perspetiva do direito fundamental ao respeito da vida privada e, por outro, a amplitude e a gravidade da ingerência neste direito que a Diretiva 2006/24 comporta, o poder de apreciação do legislador da União fica reduzido, havendo que proceder a uma fiscalização estrita." (p. 48), mas que "[a] este propósito, importa observar, em primeiro lugar, que a Diretiva 2006/24 abrange de maneira geral todas as pessoas, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego, não sendo efetuada nenhuma diferenciação, limitação ou exceção em função do objetivo de luta contra as infrações graves." (p. 57).

[6] A CRP terá sido, inclusive, a primeira Lei Fundamental a reconhecer, diretamente, alguma proteção constitucional aos titulares de dados pessoais. Nesse sentido, e para uma análise histórica mais aprofundada, cf. Alexandre Sousa Pinheiro, *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015, pp. 665-777; e António Barreto Menezes Cordeiro, *Direito da Protecção de Dados à luz do RGPD e da Lei n.º 58/2019*, Coimbra, Almedina, 2020, pp. 73-76. Quanto ao seu campo de aplicação, alguns autores entendem que a importância atribuída ao consentimento pela CRP não é tão evidente, pois apenas surge como necessário para tratamentos relativos a "convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica", sendo a expressão "vida privada" que dá alguma abertura a esse campo de aplicação. Cf. António Barreto Menezes Cordeiro, "O consentimento do titular de dados no RGPD", in *Fintech II – Novos estudos sobre tecnologia financeira*, Almedina, 2019, pp. 33 e ss..

[7] Apesar de o RGPD ter aplicação direta, conforme decorre do artigo 288.º do TFUE, na prática, este instrumento normativo contém cerca de 70 cláusulas de abertura, *i.e.*, normas que atribuem

É, igualmente, defendido por alguns autores que existe um direito de personalidade à autodeterminação e identidade informacional, com relevância civil[8].

Neste contexto, e atendendo à evolução do mercado da *Internet* e da consequente preocupação com a proteção dos dados pessoais dos indivíduos, torna-se inequívoca a atualidade e o papel central que o consentimento ocupa ao nível da proteção de dados.

Tem sido unânime na doutrina e jurisprudência que, com a aprovação e entrada em vigor do RGPD, se estabeleceu um padrão elevado para o consentimento[9], não

---

competências legislativas ou de outra índole aos EM e à própria UE, impondo ou permitindo que estes apliquem medidas concretizadoras, complementares ou modificativas dos próprios regulamentos – cf. António Barreto Menezes Cordeiro, *Direito da Proteção de Dados à luz do RGPD e da Lei nº 58/2019*, cit., pp. 41-42. É, por este motivo, que se poderá dizer que o RGPD é, na verdade, um Regulamento "com vestes de Diretiva". Nessa medida, apesar de alguma doutrina considerar este facto cada vez mais comum – neste sentido, cf. Richard Král, "National Normative Implementation of EC Regulations: An Exceptional or Rather Common Matter", in *EL Review*, 33, 2008, pp. 243-256 – e até de alguma, por sua vez, denominar o RGPD como um diploma híbrido – cf. Jürgen Kühling / Mario Martini, "Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?", in *Europäische Zeitschrift für Wirtschaftsrecht*, 27, 2018, pp. 448-449 –, entre regulamento e diretiva, a verdade é que se pode falar numa verdadeira cooperação legislativa, na qual os EM têm um papel preponderante na aplicação nacional do diploma europeu, o que justifica a importância e necessidade da Lei n.º 58/2019 (LEN). Contudo, as leis nacionais não podem contrariar o disposto no RGPD, de modo que a CNPD emitiu a Deliberação/2019/494 (disponível *online* em www.cnpd.pt) onde declarou que desaplicaria algumas normas da LEN por, no seu entender, violarem o RGPD. Uma dessas normas foi o artigo 28º, n.º 3, alínea a) a propósito do consentimento do trabalhador no âmbito das relações laborais.

[8] Alexandre Sousa Pinheiro, *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*, cit., pp. 914 e ss. Para o Autor, quer a autodeterminação informacional (de origem alemã), quer a proteção de dados, fundaram-se doutrinária e jurisprudencialmente, no princípio da dignidade humana. Adicionalmente, a proteção de dados deve ser qualificada como um direito de personalidade, na medida em que protege um bem de personalidade composto por várias posições jurídicas. Portanto, enquanto a proteção de dados é pensada como uma garantia, o seu fundamento, *i.e*, a autodeterminação informacional, exprime-se como uma liberdade, uma vez que o elemento consentimento lhe garante essa natureza de liberdade.

[9] Cf. artigo 6º do RGPD, bem como os Considerandos 32 e 33, que explicam 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

só por funcionar como uma condição de licitude da recolha e tratamento dos dados, mas por prever, inclusive, o direito específico à sua retirada. Neste sentido, de acordo com o artigo 7.º, n.º 3, do RGPD, o responsável pelo tratamento de dados deve informar os titulares dos dados sobre o seu direito de retirar o consentimento dado e oferecer-lhes maneiras fáceis de o fazer a qualquer momento.

Assim, intrinsecamente ligado ao consentimento, está a importância do princípio da transparência e dos deveres de informação, pois se estamos perante uma autorização do titular dos dados para a sua utilização por terceiros, então essa autorização só poderá ser válida, nos termos previstos no RGPD, se o sujeito tiver exata noção do alcance do ato que está a praticar.

De igual relevância para a análise do tema do consentimento, é a compreensão das finalidades do tratamento de dados, pois, como se sabe, o tratamento de dados deve obedecer a finalidades específicas e justificadas, sob pena de não ser lícito o seu tratamento[10].

Com efeito, é do consentimento do titular de dados, em especial no âmbito da *Internet*, que o nosso estudo se focará, nomeadamente sobre a natureza jurídica do consentimento, os seus principais problemas práticos no âmbito da *Internet*, propondo possíveis linhas de solução aos problemas com que nos formos deparando ao longo da presente investigação.

Pelo contrário, exclui-se desta análise outras questões relacionadas com o tema do consentimento do titular de dados, nomeadamente aqueles sem ligação direta ao contexto da *Internet*, como, *v.g.*, o problema do consentimento no âmbito das relações laborais ou com autoridades públicas ou a questão do seu âmbito espacial e lei aplicável.

1.2 Ordenamentos jurídicos apreciados

Atendendo ao tema da presente investigação, os ordenamentos jurídicos apreciados serão, essencialmente, o ordenamento jurídico português, com a necessária

---

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.".

[10] A este propósito, Alexandre Sousa Pinheiro esclarece que "o consentimento válido para um tratamento implica o conhecimento dos fins a que se destina a recolha", pois, caso contrário, "a declaração de vontade mostra-se oca e destituída de conexão com o tratamento de dados" – cf. Alexandre Sousa Pinheiro, *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*, cit., p. 949.

referência ao direito da UE e a ordenamentos estrangeiros de EM com origem Romano-Germânica, tais como França e Alemanha, mas também Espanha.

A escolha por estes ordenamentos jurídicos prende-se, essencialmente, por se tratar de ordenamentos jurídicos considerados "cabeças de estirpe"[11], influentes sobre vários outros direitos, em particular no direito português[12].

Adicionalmente, e em alguns pontos deste trabalho, serão analisados ordenamentos jurídicos de *Common Law*, nomeadamente o ordenamento jurídico inglês e o ordenamento jurídico federal norte-americano[13], por forma a se proceder a uma análise comparada entre as opções legislativas de ambos os sistemas jurídicos de *Common Law* e Românico-Germânico.

Contudo, não será objeto de tratamento do presente estudo a análise de direito comparado, ao nível da micro comparação entre ordenamentos jurídicos concretos (*v.g.*, entre o ordenamento jurídico português e o brasileiro), limitando-se a nossa análise à identificação de soluções estrangeiras sobre determinados temas abordados ao longo deste trabalho, em particular no que concerne às autoridades de controlo no âmbito da proteção de dados pessoais.

1.3 Fontes de direito – delimitação e âmbito de aplicação no contexto da *Internet*

O consentimento do titular de dados, como explicado, insere-se na temática do Direito da Proteção de Dados. Na sua génese, não podemos ignorar que as

---

[11] Expressão utilizada por Carlos Ferreira de Almeida / Jorge Morais Carvalho, *Introdução ao Direito Comparado*, Almedina, 3ª edição, reimpr., 2018, p. 41.

[12] Estes ordenamentos, ainda que tenham diferenças históricas e culturais que os separem, têm uma base comum, ligada ao Direito Romano, e apresentam influências comuns, nomeadamente no âmbito da religião e da moral cristãs, da distinção entre direito e outras ordens normativas (religião, moral, convivência social), pelas tradições culturais de humanismo e racionalismo, pela conceção do direito e da estrutura da regra jurídica, pela primazia do direito substantivo sobre o direito processual, pela distinção do Direito em ramos jurídicos, pela organização do poder político em conformidade com Constituições escritas e respetiva consagração constitucional de direitos, liberdades e garantias e pelo primado da lei, entre outros. Para mais desenvolvimentos, cf. Dário Moura Vicente, *Direito Comparado*, vol. I, 4ª edição, 2020, pp. 41-43.

[13] A escolha por estes ordenamentos prende-se, igualmente, por, em primeiro lugar, o direito inglês constituir um antecedente histórico do direito norte-americano, mas também por se tratar de ordenamentos jurídicos de génese distinta dos ordenamentos da família romano-germânica, nomeadamente pelas diferenças históricas, pela doutrina do precedente e primazia do direito processual perante o direito substantivo, tão afastada da realidade romano-germânica. Sem prejuízo das diferenças assinaladas, são ordenamentos jurídicos que, pela sua relevância sociopolítica, merecem a devida análise.

primeiras iniciativas legislativas partiram dos EUA, em 1965[14], tendo o regime norte-americano evoluído, atualmente, para um regime altamente complexo, não só pela natureza federal dos EUA, como pela inexistência de um diploma geral, semelhante ao RGPD europeu, privilegiando-se uma regulação setorial com reais dificuldades de articulação com o regime europeu[15].

Sem prejuízo desta referência, a legislação de proteção de dados na Europa partiu de influências sueca e alemã, na década de 70 do século passado, tendo evoluído para um quadro legislativo tendencialmente harmonizado, como veremos de seguida.

Assim, no âmbito do nosso estudo, o consentimento do titular de dados suscita diversas questões, cujas soluções estão espalhadas por diversas fontes normativas internacionais, europeias e nacionais, sendo que identificaremos aquelas que, a nosso ver, são as essenciais ao estudo deste tema, sem prejuízo de outras a que, pontualmente, se fará referência.

1.3.1 Fontes Internacionais

No que concerne as fontes internacionais, assinalamos as Convenções e outros instrumentos do CE, em particular a Convenção n.º 108 para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal[16], mas também, ainda que se tratem de instrumentos de *soft law*, a Recomendação do Comité de Ministros aos Estados-Membros sobre um "Guia dos direitos

---

[14] Referimo-nos, em especial, ao "Special Subcommittee on Invasion of Privacy". Para mais desenvolvimentos sobre a evolução história da legislação de proteção de dados nos EUA, cf. António Barreto Menezes Cordeiro, *Direito da Proteção de Dados*, cit. pp. 53-63.

[15] Para mais desenvolvimentos sobre a evolução da legislação norte-americana e suas diferenças com o regime europeu, cf. Lee A. Bygrave, *Data Privacy Law: An International Perspective*, OUP, Oxford, 2014, pp. 99 e ss.; Dorothee Heisenberg, *Negotiating Privacy: The European Union, the United States, and Personal Data Protection*, Lynne Rienner Pub, 2005, pp. 179-195.

[16] Ratificada por Portugal apenas em 1993 pela Resolução da Assembleia da República n.º 23/93, de 12 de maio e Decreto do Presidente da República n.º 21/93, de 9 de julho. Para Simitis, a Convenção 108 foi o diploma mais importante até ao RGPD. Cf. Spiros Von Simitis *et. al.*, *Datenschutzrecht – Kommentar*, Buch, 2019, p. 92. Para mais desenvolvimentos sobre a Convenção n.º 108 e sua importância para o direito de proteção de dados, cf. Graham Greenleaf, "Strengthening and 'Modernising' Council of Europe Data Privacy Convention 108", University of New South Wales Faculty of Law Research Series 2012, WP 27, 2012, pp. 1-5, disponível *online* em www.ssrn.com; Paul De Hert / Eric Schreuders, "The relevance of Convention 108", in *European Conference on Data Protection 2001*, pp. 63-76; Olga Estadella-Yuste, "The relevance of the data protection principles set out in Convention 108 and its Additional Protocol", in *European Conference on Data Protection*, Warsaw, 2001, pp. 47-58.

humanos para os utilizadores da *Internet*"[17] e a Recomendação n.º 2 de 27/03/2019 relativa à proteção de dados pessoais de saúde[18].

1.3.2 Fontes da União Europeia

No âmbito das fontes europeias, destaca-se, em particular, o artigo 8.º da CDFUE, relativo à proteção de dados pessoais[19], bem como o artigo 16.º, n.º 1, do TFUE, que consagra o direito à proteção dos dados de caráter pessoal, sendo que ambos reconhecem a natureza fundamental e universal do direito à proteção de dados.

Adicionalmente, o Direito da União prevê, igualmente, uma panóplia diversificada de diplomas relativos à proteção de dados, sendo o mais relevante o RGPD, o qual veio estabelecer um desenvolvido complexo de regras materiais uniformes sobre a proteção de dados pessoais[20].

O RGPD visa não só a proteção de dados pessoais de pessoas singulares, mas também assegurar a livre circulação desses dados no interior da União, atendendo ao objetivo de contribuir para a realização de um espaço de liberdade, segurança

---

[17] Cf.CM/Rec (2014) 6, adotada pelo Comité de Ministros em 16 de abril de 2014, disponível *online* em www.rm.coe.int.

[18] Cf. CM/Rec (2019) 2, disponível *online* em www.edoc.coe.int.

[19] Esta disposição determina, designadamente, que os dados pessoais 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 (n.º 2). A CDFUE consagra, portanto, o consentimento como principal fundamento de licitude do tratamento de dados pessoais. Sobre o respetivo valor jurídico, cf. Ana Maria Guerra Martins, *Manual de Direito da União Europeia*, 2ª edição, reimpr., 2019, pp. 267 e ss. Note-se, contudo, que a CDFUE apenas pode ser invocada nos termos do seu artigo 51º, *i.e.*, contra as respetivas partes contratantes, mas não contra terceiros. Para mais desenvolvimentos, cf. Mariana Canotilho / Alessandra Silveira, *Carta dos Direitos Fundamentais da União Europeia Comentada*, Coimbra, 2013, pp. 120 e ss. e pp. 572 e ss.. Sobre o entendimento do TJUE de que o direito à proteção de dados é, ainda que parcialmente, uma manifestação ou extensão do direito ao respeito pela intimidade da vida privada, cf. António Barreto Menezes Cordeiro, *Direito da Proteção de Dados*, cit., p. 70.

[20] O RGPD resultou de um intenso e árduo processo de negociação, iniciado, formalmente, em 2009 com o *The Stockholm Programmme*, seguido da Comunicação da COM sobre as linhas gerais da reforma a implementar (COM (2010) 609 final, 4 de novembro de 2010). Apesar do objetivo de harmonização dos direitos nacionais estar, desde sempre, bastante presente na lista de intenções da reforma que conduziu ao RGPD, a verdade é que após diversas revisões do diploma, e ao contrário do que se verificava na Proposta da COM, a versão final do RGPD acabou por conter diversas cláusulas de abertura em benefício dos EM e da própria UE. Estas alterações que colocaram em crise o objetivo original de unificação legislativa reflete a pressão e dificuldade do processo negocial e o compromisso que teve de se alcançar, de modo a que, efetivamente, o RGPD fosse aprovado.

e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares – cf. Considerando 2 do RGPD.

Quanto ao seu âmbito material, o RGPD aplica-se ao tratamento de dados pessoais realizados por meios total ou parcialmente automatizados, bem como por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados – cf. artigo 2.º, n.º 1, do RGPD. O legislador europeu não define, contudo, o que se entende por meios autonomizados, o que poderá ter sido propositado.

Todavia, são excluídos do âmbito material do RGPD algumas operações de tratamento de dados pessoais, designadamente os que são efetuados: (i) no exercício de atividades não sujeitas à aplicação do Direito da União; (ii) pelos EM no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; (iii) por pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; e (iv) pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais.

Por conseguinte, e *a contrario*, o RGPD aplica-se ao tratamento de dados pessoais por fornecedores de bens e serviços na *Internet* – cf. Considerando 24.

O artigo 2.º, n.º 4, inclusive, determina que o RGPD não prejudica a aplicação da DCE, nomeadamente as normas que limitam a responsabilidade dos prestadores intermediários de serviços nos casos de simples transporte, armazenagem temporária [*caching*] e armazenagem em servidor e estabelecem a ausência de dever geral de vigilância.

Contudo, tal não significa, como esclarece Lima Pinheiro[21] – cuja posição acolhemos –, que o RGPD não seja aplicável à proteção de dados pessoais no contexto de serviços da sociedade de informação, até porque a DCE salvaguarda a aplicação plena da legislação europeia sobre proteção de dados pessoais a esses serviços e exclui do seu âmbito de aplicação as questões respeitantes aos serviços da sociedade da informação abrangidas pelo regime europeu da proteção de dados pessoais – cf. Considerando 14 e artigo 1.º, n.º 5, alínea b), da DCE.

Com efeito, apesar de ser pacífico que o objetivo do legislador europeu era assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União através de uma uniformização das principais regras substantivas sobre a matéria e que, por isso, o RGPD vai além da DPD, também é questionável que, em virtude das várias cláusulas de abertura

[21] Luís de Lima Pinheiro, "Direito aplicável à proteção de dados pessoais na *Internet*: Alguns aspetos de direito internacional privado", in *Cyberlaw by CIJIC, Direito: a pensar tecnologicamente*, VII (maio de 2019), p. 6.

previstas, não será um ato normativo da União com "forma de lei, mas espírito de diretiva", na medida em que carece, em alguns aspetos, de densificação pelo direito dos EM.

1.3.3 Fontes Nacionais

No âmbito das fontes nacionais, destaca-se, desde logo, o artigo 35.º da CRP, que, desde a sua versão originária até à sua versão atual (fruto da revisão constitucional de 1997), resultou no alargamento progressivo da proteção concedida aos titulares dos dados, bem como estabeleceu as bases fundamentais do Direito à Proteção de Dados, posteriormente densificadas e concretizadas pelo RGPD e, internamente, pela LEN[22] e demais legislação avulsa.

Adicionalmente, e atendendo à abrangência dos problemas associados ao consentimento do titular de dados, entendemos relevante a referência a outros diplomas nacionais, tais como o CC, a LCCG, o Decreto-Lei n.º 7/2004, de 7 de janeiro (Lei do Comércio Eletrónico), a Lei n.º 12/2005, de 26 de janeiro, que regula a informação genética pessoal e informação de saúde, e a Lei n.º 41/2004, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.

1.3.4 Fontes de natureza infralegal e de *soft law*

O RGPD não atribui às autoridades de supervisão competências para elaborar regulamentos ou diplomas legais com força análoga. Nessa medida, os pareceres, orientações e recomendações genéricas emitidas pelas autoridades de supervisão nacionais (entre nós, pela CNPD) não têm conteúdo normativo próprio e, portanto, não são, *per si*, vinculativas[23]. Contudo, estas orientações e pareceres ilustram os

---

[22] Também este diploma, um pouco à semelhança do RGPD, atravessou um processo legislativo conturbado, altamente criticado pela autoridade de supervisão nacional – CNPD. Esta autoridade, inclusive, após a publicação da lei, emitiu a Deliberação n.º 2019/494 de 3 de setembro, onde declarou que iria desaplicar algumas normas da LEN, em virtude de, no seu entender, serem contrárias ao RGPD. Para mais desenvolvimentos sobre o processo legislativo e âmbito de aplicação, cf. António Barreto Menezes Cordeiro, *Direito da Proteção de Dados*, cit., pp. 101-105, bem como os pareceres emitidos pela CNPD, disponíveis *online* em www.cnpd.pt.

[23] Sem prejuízo, cumpre, ainda, ressalvar que, sobretudo na era pré-RGPD, as orientações do GT29, bem como as autorizações das autoridades de controlo (a nível nacional, da CNPD), tinham bastante relevo, porquanto as mesmas eram pressuposto de aplicação de certas normas que apenas admitiam determinado tipo de tratamento de dados (*v.g.*, câmaras de vigilância) quando as referidas autorizações

entendimentos e interpretações veiculadas pelas autoridades de supervisão, auxiliando na interpretação do RGPD e na sua aplicação prática.

No âmbito do nosso estudo, estes instrumentos de *soft law*, apesar de não vinculativos, são de preciosa relevância para a interpretação do conceito do consentimento e sua concretização em situações especificas (*v.g*. sobre o consentimento de menores, consentimento através de *cookies*, entre outros).

1.3.5 Articulação entre o RGPD e a Diretiva *E-Privacy*

No que concerne à relação entre o RGPD e a DEP, em particular sobre o tema do consentimento, colocam-se algumas questões no âmbito de aplicação da lei no espaço.

Em particular, estes instrumentos normativos da União relevam, quando estamos perante questões de privacidade e associadas ao consentimento para a utilização de *cookies* ou "testemunhos de conexão".

Antes da entrada em vigor do RGPD, quer a legislação de privacidade, quer de proteção de dados, era regulada através de diretivas. Contudo, com a entrada em vigor do RGPD, e a ausência de um regulamento de idêntica força para regular os temas de privacidade, criou-se um desequilíbrio legislativo que, na prática, tem suscitado várias questões.

Assim, no que concerne ao consentimento, em particular, com a revisão de 2009, a DEP assumiu o nome de *The Cookie Law* porque exigia explicitamente o consentimento dos utilizadores para processar os seus *web cookies*. Na verdade, a DEP estipula uma exceção para os *cookies* que são estritamente necessários para fins legítimos, mas os *cookies* mais intrusivos, visados para monitorizar ou para efeitos de marketing, são abrangidos pelo seu âmbito de aplicação e, consequentemente, é exigido o consentimento do *user*.

A DEP remete para o conceito de consentimento que estava definido na DPD, a predecessora do RGPD. Como sabemos, o conceito atual de consentimento, ao abrigo do RGPD, é um conceito mais exigente face à sua predecessora, o que coloca a questão de saber se o intérprete tem (i) de interpretar o conceito à luz do conceito literal, ou (ii) de proceder a uma interpretação atualista do conceito, e analisá-lo à luz do RGPD.

---

fossem necessárias. A título exemplificativo, o artigo 21.º, n.º 1 do Código do Trabalho dispõe que "A utilização de meios de vigilância a distância no local de trabalho está sujeita a autorização da Comissão Nacional de Protecção de Dados". Sucede, porém, que após a entrada em vigor do RGPD, fez-se uma interpretação ab-rogante do referido artigo, no sentido em que, atualmente, não é necessária a autorização da CNPD.

Assim, tem-se entendido, genericamente, que a DEP é *lex specialis* face ao RGPD, no que concerne ao tratamento de dados no âmbito de *cookies* e ao consentimento exigido. Ainda assim, cumpre interpretar a DEP num sentido em que o nível mínimo de proteção garantido pelo RGPD não seja posto em causa[24]. Assim, relevarão todas as condições associadas ao consentimento para fins de tratamento de dados, nos termos do artigo 7º do RGPD, o que garante um nível de proteção superior ao que existia antes da entrada em vigor do Regulamento.

Este entendimento deverá, em princípio, manter-se quando entrar em vigor o Regulamento *E-Privacy*, já em preparação desde 2017 e cujo objetivo inicial era ter entrado em vigor na mesma data que o RGPD, garantindo aos EM uma unificação legislativa em ambos os setores[25]. Contudo, tal não aconteceu, permanecendo o Regulamento *E-Privacy* por aprovar.

2 O consentimento do titular de dados no âmbito do RGPD

2.1 Noção de consentimento

A definição de consentimento plasmada no RGPD indica a intenção do Regulamento em concretizar um conceito autónomo de consentimento e que não fica dependente da regulação interna dos EM, nem da lei reguladora do contrato.

Assim, e para efeitos do presente estudo, o conceito relevante de consentimento é o que consta do artigo 4.º, n.º 11, do RGPD: "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".

---

[24] Este é, também, o entendimento do EDPB, ao referir, no ponto 7 do "Guidelines 05/2020 on consent under Regulation 2016/679", de 4 de maio de 2020, p. 6 (disponível *online* em www.edpb.europa.eu), o seguinte: "With regard to the existing e-Privacy Directive, the EDPB notes that references to the repealed Directive 95/46/EC shall be construed as references to the GDPR. This also applies to references to consent in the current Directive 2002/58/EC, as the ePrivacy Regulation will not (yet) be in force from 25 May 2018. (...) The EDPB notes that the requirements for consent under the GDPR are not considered to be an 'additional obligation', but rather as preconditions for lawful processing. Therefore, the GDPR conditions for obtaining valid consent are applicable in situations falling within the scope of the e-Privacy Directive".

[25] Neste sentido, o EDPB emitiu a "Declaração relativa à revisão do Regulamento Privacidade Eletrónica e ao seu impacto sobre a proteção das pessoas singulares no que diz respeito à privacidade e à confidencialidade das suas comunicações" de 25 de maio de 2018 e a "Declaração 3/2019 sobre um regulamento relativo à privacidade e às comunicações eletrónicas Adotada em 13 de março de 2019", de 13 de março de 2019, todos os documentos disponíveis *online* em www.edpb.europa.eu.

Com base nesta definição, podemos identificar cinco critérios essenciais para aferir se determinado consentimento é válido: (i) se estamos perante uma manifestação de vontade, (ii) se a mesma é livre, (iii) específica, (iv) informada e (v) explícita[26].

Estes critérios cumulativos criam um limiar elevado para um consentimento válido, daí que haja uma tendência para as autoridades de controlo os interpretarem de forma restritiva[27].

O consentimento está no cerne dos ideais da autonomia pessoal e privacidade, particularmente quando estes são concebidos em termos do desenvolvimento do conceito de "autodeterminação informativa". As regras que exigem o consentimento da pessoa em causa também constituem e manifestam um princípio central geral da lei de proteção de dados, nomeadamente o princípio da influência da pessoa em causa, que defende que as pessoas devem poder participar e ter uma certa influência sobre o tratamento dos dados que lhes dizem respeito, em particular quando tratados por terceiros. Contudo, a controvérsia e a incerteza têm rodeado a natureza e os requisitos do consentimento válido do titular de dados, já no âmbito da DPD[28], mas também no âmbito do RGPD.

---

[26] Nas versões originais do RGPD, o termo "explícito" fazia parte da definição de consentimento. Contudo, curiosamente, na versão final do RGPD, apenas na versão portuguesa é que se manteve a referência ao adjetivo explícito, tendo sido suprimido das demais versões do RGPD por se entender que esta referência dava a entender que o consentimento teria de ser dado, obrigatoriamente, por escrito, o que tornaria o processo demasiado moroso. Cf. António Barreto Menezes Cordeiro, "O consentimento...", cit., p. 40.

[27] Neste sentido, cf. Lee Andrew Bygrave / Christopher Docksey, *The EU General Data Protection Regulation (GDPR),* cit., p. 181.

[28] No Acórdão *Orange Romania* (Caso C-61/19) foi solicitado ao TJUE que esclarecesse quais as condições que devem ser preenchidas para que o consentimento seja considerado específico, informado e dado livremente nos termos do artigo 2.º, alínea h) da DPD. Embora o caso diga respeito à definição de consentimento nos termos da DPD, sem dúvida que também tem relevo para a definição nos termos do RGPD. Assim, a 11 de novembro de 2020, o TJUE proferiu acórdão, decidindo que os preceitos normativos em causa "devem ser interpretados no sentido de que cabe ao responsável pelo tratamento dos dados demonstrar que a pessoa em causa manifestou, através de um comportamento ativo, o seu consentimento para o tratamento dos seus dados pessoais e que obteve previamente uma informação a respeito de todas as circunstâncias relativas a esse tratamento, de modo inteligível e de fácil acesso e numa linguagem clara e simples, que lhe permitiu determinar facilmente as consequências desse consentimento, de modo a garantir que este foi dado com conhecimento de causa", sendo que tal não sucede em contratos de fornecimento de serviços de telecomunicações com cláusulas pré-validadas antes da assinatura do referido contrato. Para mais desenvolvimentos, cf. João Pinto Ramos, "Comentário ao Acórdão TJUE, 11-Nov.-2020, Proc. N.º C-61/19 (Orange Rom ânia v. ANSPDCP) – Consentimento do titular dos dados e o problema das opções pré-validadas", in *Revista De Direito e Tecnologia*, vol. 3 (2021), No. 1, pp. 171-182.

Assim, com o RGPD, deixou de se partir do consentimento como principal fundamento de licitude para o incluir num elenco mais abrangente de fundamentos de licitude (*v.g.* execução do contrato, interesses legítimos, etc.), sem existência de um nexo hierárquico ou de prevalência entre os vários fundamentos. Na prática, dada a fragilidade do consentimento, como veremos, costuma procurar-se fundamentar o tratamento de dados noutro fundamento de licitude, acabando por remeter o consentimento para um requisito subsidiário, que apenas é utilizado na falta de outro fundamento de licitude.

2.1.1 Manifestação de vontade

Em primeiro lugar, o responsável pelo tratamento de dados deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.

Ademais, se o consentimento do titular dos dados for obtido no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples.

Para alguns autores, apresentar o consentimento como uma manifestação de vontade é reconduzi-lo ao universo dos negócios jurídicos[29],sendo que o conceito de consentimento é igualmente aplicável aos atos jurídicos *stricto sensu*, porquanto estes consubstanciam factos jurídicos em que releva a vontade humana.

Por conseguinte, o consentimento sempre terá de se encontrar sujeito à dogmática civilística, na medida em que o RGPD não contempla um completo regime negocial, aplicando-se, com as necessárias adaptações, as disposições legais de Direito Civil sempre que o RGPD não consagre uma solução especial.

De qualquer modo, a aplicação e a interpretação das disposições legais do CC, em casos de tratamento de dados pessoais, sempre teriam de ser conformes ao Direito Europeu.

Deste modo, e apesar de não ser uma posição unânime na doutrina[30], também acolhemos a posição de que cabe ao intérprete-aplicador recorrer às bases legais

---

[29] António Barreto Menezes Cordeiro, "O Consentimento...", cit., p. 41.

[30] A doutrina alemã tem-se mostrado dividida quanto a esta questão. Cf. Patricia Maria Rogosch, *Die Einwilligung im Datenschutzrecht*, Nomos, Baden-Baden, 2013, pp. 37 e ss.; Michael Funke, *Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht*, Nomos, Baden Baden, 2017, pp. 74 e ss.

nacionais, nomeadamente do Direito Civil, para interpretar e aplicar as normas de direito da proteção de dados, garantindo que não contrariam o entendimento do RGPD enquanto lei supranacional e lei especial.

No demais, não acolhemos a posição, fundada na autonomia do Direito Europeu, que defende a natureza *sui generis* do consentimento e o seu afastamento dos ordenamentos jurídicos nacionais[31]. Efetivamente, o recurso às normas do CC para efeitos de integração do disposto no RGPD demonstra que o conceito de consentimento nunca poderá ser interpretado única e exclusivamente à luz do ordenamento jurídico europeu.

Assim, a manifestação de vontade comporta dois elementos essenciais: (i) a vontade humana e (ii) a sua exteriorização, ou seja, a manifestação dessa vontade.

Portanto, o consentimento pressupõe uma situação ativa, um "ato positivo inequívoco" de exteriorização da vontade do titular de dados pessoais[32].

2.1.2 Manifestação de vontade livre

O consentimento pressupõe uma escolha genuína pelo titular de dados e o respetivo controlo sobre o modo como terceiros utilizam e tratam os seus dados. Portanto, se o indivíduo não tiver uma escolha real, o consentimento não é dado livremente e, consequentemente, será tido como inválido – cf. Considerando 42 do RGPD[33].

Isto significa que os indivíduos devem poder recusar o consentimento sem qualquer prejuízo ou receio de retaliação[34], e devem poder retirá-lo facilmente, a

---

[31] Benedikt Buchner / Jürgen Kühling, *Die Einwilligung in der Datenschutzordnung*, 2018, pp. 544-548.

[32] Para alguns autores, o consentimento é mais do que uma simples manifestação de vontade, pois pode ser encarado como um bem, na medida em que é transacionado, ou como parte integrante de um contrato, por exemplo – cf. António Barreto Menezes Cordeiro "O Consentimento...", cit., p. 43.

[33] Sobre a remissão da exigência de liberdade para o consentimento como referência ao instituto da coação civil (artigos n.os 246º e 255º do CC) ou da *undue influence* do regime de *Common Law*, cf. António Barreto Menezes Cordeiro, "O Consentimento...", cit., pp. 43-45. No caso do direito português, por aplicação do instituto da coação, esta invalidade seria um caso de anulabilidade – cf. artigos 287.º e ss. do CC.

[34] A necessária liberdade inerente à manifestação de vontade do titular de dados, poderá, contudo, não existir nas chamadas situações de "desequilíbrio de posições" – cf. Considerando 43 do RGPD. Embora o conceito de desequilíbrio de posições não se encontre legislativa ou jurisprudencialmente preenchido, na prática tem sido associado a situações em que o titular de dados, fruto da sua posição, não estará em condições para prestar um consentimento livre como, *v.g.*, nas relações laborais em

qualquer momento. Significa também que o consentimento deve ser separado de outros termos e condições, incluindo, *v.g.*, opções de consentimento "granular" separadas para diferentes tipos de tratamento.

O RGPD é claro ao dispor que o consentimento não deve ser agrupado como uma condição à prestação de um serviço, exceto se for necessário para esse serviço – *v.g.,* seguradoras que necessitam de acesso aos dados pessoais do tomador do seguro para que possam celebrar o contrato de seguro. Isto decorre do artigo 7.º, n.º 4, e do Considerando 43 do RGPD. Ou seja, o consentimento deve ser evidente e exigir uma ação positiva para se optar por participar. Os pedidos de consentimento devem ser inequívocos, desagregados de outros termos e condições, concisos e fáceis de compreender e de utilizar.

Face ao exposto, conclui-se que o consentimento tem de ser prestado livremente e, para tal, tem de ser esclarecido, daí que o titular dos dados tenha direito à prestação de uma série de informações necessárias à sua compreensão da finalidade de tratamento de dados que está prestes a consentir.

2.1.3 Manifestação de vontade específica e informada

O consentimento deve ser específico, *i.e*, orientado para as finalidades a que o responsável de tratamento de dados se propõe, nos termos do artigo 12.º e ss. do RGPD[35], não sendo suficiente um consentimento generalizado.

---

que se verifica uma relação contratual de subordinação empregador/trabalhador e poderá este último ter receio de retaliações, caso se recuse a prestar consentimento a pedido do seu empregador ou até no caso dos ensaios clínicos. Sobre este tema, *vide* a obra de Maria do Rosário Palma Ramalho / Teresa Coelho Moreira, *O Regulamento Geral de Proteção de Dados e as Relações Laborais*, Estudos APODIT, n.º 6, AAFDL Editora, Lisboa, 2020. Adicionalmente, este problema também colocou questões novas no âmbito da pandemia COVID-19, aquando da intenção das entidades empregadoras de procederem a medições de temperatura aos seus trabalhadores para despiste de sinais de contágio. Sobre este tema a CNPD emitiu Orientações sobre recolha de temperatura corporal e sobre recolha de dados de saúde dos trabalhadores, de 23 de abril de 2020, esclarecendo que o contexto das relações laborais é um dos que mais desafios coloca à concretização de tais condições [do consentimento]. Essa é a razão pela qual as autoridades de proteção de dados pessoais dos EM da UE sempre interpretaram a legislação europeia como apenas admitindo a relevância do consentimento dos trabalhadores "em circunstâncias excecionais, quando o ato de dar ou recusar o consentimento não produza quaisquer consequências negativas". Neste sentido, cf. Orientações sobre o consentimento no RGPD, revistas e aprovadas em 10 de abril de 2018 pelo do GT 29, e assumidas pelo EDPB em 25 de maio de 2018, disponíveis *online* em www.ec.europa.eu.

[35] No Parecer WP259 – Orientações relativas ao consentimento, com última revisão a 10 de abril de 2018, p. 13, o GT29 esclarece que o elemento da especificidade compreende três dimensões: "(i) especificação em função da finalidade como salvaguarda contra o desvirtuamento da função,

Adicionalmente, o consentimento deve ser esclarecido e informado, na medida em que o pedido para o consentimento cumpra com os seguintes requisitos de informação mínima[36]: (i) identidade do responsável pelo tratamento; (ii) finalidades do tratamento; (iii) as atividades de processamento, *i.e.*, sempre que possível, o responsável pelo tratamento deve fornecer opções de consentimento para cada tipo de processamento, em separado, a menos que essas atividades sejam claramente interdependentes; e (iv) o direito de retirar o consentimento a qualquer momento, *i.e.*, o responsável pelo tratamento deve informar o titular desse direito e, idealmente, explicar como o titular o pode fazer, de forma clara e concisa.

Contudo, estas regras sobre pedidos de consentimento são separadas das suas obrigações de transparência ao abrigo do direito de ser informado, que se aplicam quer o tratamento de dados esteja ou não dependente do consentimento do titular dos dados.

É necessário, portanto, uma linguagem clara e acessível. O responsável pelo tratamento deve explicar claramente aos indivíduos o que estão a consentir, de uma forma que consigam compreender facilmente. Sucede que o RGPD não esclarece, contudo, de que forma ou em que suporte deve a informação ser prestada, cabendo ao responsável pelo tratamento dos dados identificar, na situação concreta, qual a forma mais adequada de o fazer. Parece-nos, ainda assim, que o pedido de consentimento deve ser apresentado de modo inequívoco, conciso, separado de outros termos e condições, e em linguagem clara.

Assim, se o pedido de consentimento for vago, demasiado lato ou de difícil compreensão (utilizando linguagem propositadamente confusa), o mesmo será inválido. Ora, atendendo ao regime da interpretação dos negócios / atos jurídicos, a informação terá de ser percetível e compreensível de acordo com o critério do declaratário normal (cfr. artigo 236.º, n.º 1, do CC). Em termos práticos, isto significa que, de um ponto de vista formal, a informação deverá ser disponibilizada na língua materna dos destinatários e não, como usualmente acontece, em inglês, por se tratar da língua mais utilizada, principalmente no contexto da *Internet*. O

(ii) granularidade nos pedidos de consentimento, e (iii) separação clara entre as informações relacionadas com a obtenção de consentimento para atividades de tratamento de dados e as informações sobre outras questões.". A estes requisitos, acrescenta António Barreto Menezes Cordeiro, "O Consentimento...", cit., p. 50, um quarto: a especificação dos dados a tratar. Salvo melhor opinião, entendemos que este quarto requisito já se encontra englobado na especificação em função da finalidade a que o GT29 se refere, na medida em que o grau de especificidade exigido para o consentimento requer, na prática, a identificação dos dados pessoais a tratar.

[36] Indicados pelo GT29, Parecer WP259, cit., pp. 14-15. Em sentido contrário, cf. António Barreto Menezes Cordeiro, "O Consentimento...", cit., p. 52.

Considerando 32 também esclarece que 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 – *v.g.*, desenvolvendo informações estratificadas de fácil utilização e consentimentos "just-in-time".

É necessário assinalar, ainda, que a consagração de um direito do titular dos dados à informação implica, na esfera jurídica do responsável pelo tratamento – ou até do subcontratante – uma situação jurídica passiva, correspondente a um dever de informar. Sem prejuízo do exposto no RGPD, este dever de informação decorreria igualmente dos deveres acessórios de boa fé no âmbito das relações negociais, enquanto manifestação do subprincípio da tutela da confiança – cf. artigos 227.º, n.º 1, e 762.º, n.º 2, do CC.

Contudo, o direito à informação, no qual as características inerentes ao consentimento se apoiam, tem um âmbito e uma intencionalidade mais vastos do que de mero instrumento de esclarecimento conducente à licitude do consentimento, o que significa que, no contexto da *Internet*, as exigências do RGPD deverão ser analisadas em conjugação com as de outros diplomas legislativos aplicáveis, quer em matéria de consumo, quer em matéria de contratação eletrónica ou à distância.

Por um lado, a licitude do tratamento de dados pode continuar a existir, quando o tratamento se baseie noutros fundamentos que não o consentimento do titular e, por outro lado, este revela-se essencial para que o titular dos dados pessoais possa acompanhar o tratamento que deles seja feito. Parece, aliás, ser esta a *ratio* do direito à informação a que se refere o artigo 15.º do RGPD e que surge associado ao direito de acesso do titular dos dados.

Adicionalmente, cabe, ainda, esclarecer que, apesar de o RGPD não prever nenhuma norma expressa sobre a duração do consentimento, existe uma necessidade de atualização do consentimento, *i.e.*, o consentimento não deverá ser dado *ad aeternum*. Desse modo, o responsável pelo tratamento de dados deverá manter os consentimentos recebidos sob análise constante e atualizá-los em caso de as suas finalidades ou atividades específicas evoluírem além do que originalmente foi apresentado e especificado ao titular de dados. Por conseguinte, mesmo que a sua nova finalidade seja considerada "compatível" com a sua finalidade original, isso não substitui a necessidade de novo consentimento para cumprir com o requisito da especificidade do consentimento, conforme determina o artigo 7.º do RGPD[37].

[37] Numa posição mais liberal, pronunciou-se o TJUE, no Acórdão *Deutsche Telekom AG vs Bundesrepublik Deutschland* (Processo C-543/09 de 05 de maio de 2011), no qual considerou não ser necessário renovar o consentimento sempre que um novo tratamento estiver abrangido pelas finalidades originariamente

Por fim, importa assinalar que o RGPD não estabelece um prazo específico para o exercício do consentimento. De qualquer modo, cumpre ter em conta que: (i) é necessário analisar o escopo do consentimento original e as expectativas do indivíduo; (ii) se as finalidades de processamento de dados sofrerem alterações, os consentimentos originais deixam de ser específicos ou informados e é necessário solicitar um novo consentimento ou identificar outra base legal; (iii) se alguém retirar o consentimento, é necessário cessar o processamento com base no consentimento o mais rápido possível, de acordo com as circunstâncias; e que (iv) é necessário manter os consentimentos sob revisão e considerar a possibilidade de atualizar o consentimento periodicamente.

2.1.4 Manifestação de vontade explícita e inequívoca

O RGPD não faz depender a validade do consentimento de uma qualquer forma especial. Contudo, deve ser óbvia (i) a manifestação que o titular de dados consentiu com o tratamento de dados e (ii) sobre que tratamento de dados, em concreto, é que deu o seu consentimento.

O Considerando 32 do RGPD é, aliás, claro ao determinar que o consentimento requer uma ação positiva, afirmativa e clara. Tal confirmação de consentimento requer, a nosso ver, muito mais do que a mera confirmação de que o titular dos dados leu os termos e condições para o tratamento dos dados apresentado pelo responsável pelo tratamento, ou seja, além dos requisitos de especificidade e informação já mencionados, deverá haver um sinal claro e inequívoco da concordância do titular de dados para o consentimento. Se houver espaço para dúvidas, então é provável que o consentimento não seja válido. Deve ficar claro, portanto, que o indivíduo deliberada e ativamente escolheu o consentimento[38].

---

consentidas. Em concreto, e sem prejuízo de o TJUE ainda ter de abordar diretamente a definição de consentimento no RGPD, neste acórdão o Tribunal considerou o âmbito do consentimento nos termos do artigo 12.º, n.º 2, da DEP, o que condiciona a publicação, em diretórios impressos ou eletrónicos, de dados pessoais relativos a assinantes de serviços de comunicações eletrónicas (*v.g.*, serviços de telefonia e correio eletrónico) ao consentimento desses assinantes. De facto, nos termos da DEP, os assinantes são livres de decidir se os seus dados pessoais devem ser incluídos num diretório público e, em caso afirmativo, quais os dados pessoais. O Tribunal considerou ainda que não era necessário novo consentimento para permitir que os dados do assinante introduzidos numa lista fossem transmitidos a uma empresa terceira com o objetivo de serem incluídos numa nova lista pública mantida por essa empresa, depois de o assinante ter consentido em ser registado na primeira lista e de ter sido informado, ao dar o seu consentimento inicial, da possibilidade de tal transferência de dados.

[38] Concretizando, a exigência de uma "ação positiva" clara significa que alguém deve tomar uma ação deliberada e explícita para optar ou concordar com o processamento dos dados, mesmo que

Neste contexto surge, portanto, a ideia de um ato afirmativo que, contudo, deixa espaço, ainda, para métodos implícitos de consentimento em algumas circunstâncias, particularmente em situações *offline* mais informais.

A questão fundamental é que ainda deve haver uma ação positiva que deixe claro que o titular dos dados concorda com o seu uso para um propósito específico. Veja-se, por exemplo, o caso de um indivíduo que submete uma pesquisa *online* sobre seus hábitos alimentares. Ao enviar o formulário, o indivíduo está a indicar claramente o consentimento para processar os seus dados para os fins da pesquisa em si. O envio do formulário não será, no entanto, suficiente para, por si só, demonstrar um consentimento válido para quaisquer outras utilizações dos dados em causa.

O consentimento explícito também está relacionado com o requisito de que o consentimento deve ser verificável. O artigo 7.º, n.º 1, do RGPD, torna claro que o responsável pelo tratamento de dados deve ser capaz de demonstrar que o titular desses dados consentiu no seu tratamento.

Ao abrigo do regime anterior, colocava-se o problema de saber se o consentimento poderia ser tácito, sendo que alguma doutrina defendia que o caráter não expresso da declaração, nos termos do artigo 217.º do CC, não contrariava essa inequivocidade[39].

Contudo, com o RGPD, como referido, exige-se que o responsável pelo tratamento consiga demonstrar que o titular dos dados deu, efetiva e inequivocamente, o respetivo consentimento. Portanto, é discutível se a exigência do RGPD se subsume a uma mera questão probatória[40], que não pode ser confundida com a

---

isso não seja expresso como uma caixa de opção de inclusão. *V.g*, outros métodos de *opt-in* afirmativos podem incluir a assinatura de uma declaração de consentimento, confirmação oral, uma escolha binária com igual proeminência, ou a mudança de configurações técnicas para fora do padrão. O ponto-chave é, no entendimento das autoridades de controlo europeias, que todo o consentimento deve ser um consentimento *opt-in*, ou seja, uma ação ou indicação positiva. Contrariamente, não existe tal coisa como "consentimento *opt-out*". O *opt-out* não é consentimento, pois não envolve um ato afirmativo claro. Igualmente inválido é o silêncio, inatividade, configurações-padrão, caixas pré-selecionadas ou seus termos e condições gerais, ou procurar tirar vantagem da inércia, desatenção ou viés padrão de qualquer outra forma. Todos esses métodos envolvem ambiguidade – e para que o consentimento seja válido, deve ser explicito, inequívoco e afirmativo.

[39] Neste sentido, cf. Mafalda Miranda Barbosa, "Proteção de Dados e Direitos de Personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil" in *AB Instantia*, Ano V, n.º 7, 2017, pp. 16-17.

[40] Para António Barreto Menezes, "O Consentimento...", cit., pp. 56-57, trata-se de uma exigência de prova que vai mais além de um mero dever. Assim, o dever de provar o consentimento é acompanhado do dever de provar o cumprimento de todas as exigências e requisitos inerentes a um válido e legítimo consentimento. Deixando o RGPD, em aberto, a forma como o consentimento é prestado, cabe ao responsável pelo tratamento de dados acautelar que a forma utilizada seja suficiente para provar que obteve licitamente o consentimento do titular de dados. Por conseguinte, quanto mais informal for

modalidade da declaração em causa ou se, efetivamente, estamos perante uma maior exigência formal, ainda que, como referido, o próprio RGPD não faça depender a validade do consentimento de uma qualquer forma especial.

Em rigor, mesmo que se exigisse que o consentimento fosse prestado segundo uma determinada forma – algo que o RGPD não dispõe expressamente –, nos termos do artigo 217.º, n.º 2, do CC, tal caráter formal não impediria, em tese, que ela fosse emitida tacitamente, desde que a forma tivesse sido observada quanto aos factos de que a declaração se possa deduzir.

Ora, embora haja alusão à natureza explícita da manifestação da vontade, o RGPD afirma que esta tem lugar mediante declaração ou ato positivo inequívoco.

Ainda que, para certas autoridades de controlo (*v.g.*, ICO), o consentimento explícito deva ser expressamente confirmado por palavras e não por qualquer outra ação positiva, parece-nos, no entanto, que se é de admitir, à luz do ordenamento jurídico português, e atenta a amplitude com que se compreendem os comportamentos declarativos, que haja consentimento tácito, desde que prestado de forma explícita e inequívoca, então tais comportamentos também se poderão subsumir na noção prevista no artigo 4.º do RGPD.

Neste sentido, importa ter em consideração que o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais, bem como o disposto a este propósito no Considerando 32 do RGPD, nos termos do qual "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 RGPD não define, portanto, qual o modo em que o consentimento deve ser prestado, adiantando, apenas, um leque exemplificativo de situações que correspondem a modos lícitos de consentimento. Nos termos do Considerando 32, 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 elemento *explícito* de qualquer consentimento deve também ser separado de quaisquer outros consentimentos que pretenda obter, em conformidade com as orientações do Considerando 43.

---

a forma como é prestado o consentimento, mais difícil será a sua demonstração. Em sentido contrário, cf. Mafalda Miranda Barbosa, "Proteção de Dados e Direitos de Personalidade", cit., pp. 17-18.

O consentimento explícito também pode, a nosso ver, ser obtido oralmente, garantindo que se mantém um registo do respetivo guião (*v.g.*, no caso das chamadas gravadas) para acautelar o dever de comprovação da manifestação do consentimento.

No entanto, o silêncio, as opções pré-validadas ou a omissão não deverão constituir um consentimento válido. Isto significa que o RGPD exclui expressamente – e em consonância com a regra ditada pelo artigo 218º do CC – a relevância do silêncio como declaração de vontade.

Persistem, todavia, dúvidas acerca da admissibilidade de comportamentos concludentes como via de manifestação da vontade do sujeito[41]. Pense-se, por exemplo, na assistência por telefone que indica ao consumidor que a chamada será gravada e que, caso não consinta com a gravação e prossiga com a chamada, se assumirá que consentiu com a mesma.

Nada se estabelecendo a este respeito, valem, entre nós, numa interpretação sistemática dos preceitos do RGPD, as regras atinentes às declarações negociais, aplicáveis a esta questão diretamente ou por força do artigo 295º do CC.

Ora, os comportamentos concludentes que consubstanciem atos positivos e que, com toda a probabilidade, permitam deduzir a existência de declaração negocial – ainda que de modo tácito – poderão ser uma forma lícita de consentimento, para efeitos do RGPD.

Pelo contrário, comportamentos omissivos e que não permitam presumir, com elevado grau de certeza ou probabilidade, a vontade do titular dos dados em consentir o seu tratamento, não preenchem os requisitos exigidos pelo RGPD e, por conseguinte, não serão admissíveis. Pegando no exemplo acima mencionado, o prestador do serviço de atendimento telefónico deverá pedir, expressamente, o consentimento do consumidor à gravação de chamada (pressionando um número como forma de confirmar o seu consentimento ou solicitando que diga, por palavras, que aceita), sob pena de se entender que o consentimento é inválido.

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.

Por fim, uma nota para esclarecer que na versão portuguesa do RGPD, a definição de consentimento suscita dúvidas interpretativas, na medida em que nos termos do artigo 4.º, alínea 11) do RGPD já é definido como sendo uma manifestação

---

[41] Mafalda Miranda Barbosa, "Proteção de Dados e Direitos de Personalidade, cit., p. 24; Paulo Mota Pinto, *Declaração Tácita e Comportamento Concludente no Negócio Jurídico*, Almedina, Coimbra, 1995, pp. 194 e ss..

de vontade explícita, pelo que se poderá afigurar redundante a redação do artigo 9º (categorias especiais de dados) e da alínea a) do n.º 1 do artigo 49.º do RGPD (transferências de dados pessoais para países terceiros).

Contudo, o conceito de "consentimento explícito" nos termos dos artigos 9º e 49º não está definido no RGPD, mas, ainda assim, é entendimento maioritário que o RGPD exige um consentimento reforçado face a outras categorias de dados. Este consentimento reforçado justifica-se, seja pela maior sensibilidade dos dados pessoais alvo de consentimento, seja pelo maior risco de desproteção do titular de dados face a terceiros nas referidas situações.

Assim, de acordo com as orientações das autoridades de controlo europeias (*v.g.*, ICO), podem entender-se como requisitos adicionais para o consentimento ser "explícito", os seguintes: (i) o consentimento explícito deve ser confirmado numa declaração clara (oral ou escrita), em vez de por qualquer outro tipo de ação afirmativa; (ii) deve especificar a natureza dos dados da categoria especial; e (iii) deve ser separado de quaisquer outros consentimentos.

Note-se que o consentimento explícito pode ser a única condição que pode ser aplicada a uma ampla gama de circunstâncias, e em alguns casos pode ser a sua única opção. Em caso afirmativo, o responsável pelo tratamento de dados deve certificar-se de que oferece às pessoas uma escolha genuína sobre como utilizar os seus dados e garantir a prova desse consentimento.

2.2 O consentimento enquanto condição de licitude do tratamento de dados

2.2.1 Outras condições aplicáveis ao consentimento

Além das caraterísticas inerentes ao conceito de consentimento, o artigo 7.º do RGPD também estabelece outras "condições" para o consentimento, com disposições específicas sobre: (i) manutenção de registos para demonstrar o consentimento (prova); (ii) transparência e clareza dos pedidos de consentimento; (iii) direito de retirar o consentimento facilmente e a qualquer momento; e (iv) consentimento livre e esclarecido se o contrato estiver sujeito a consentimento.

2.2.2 O consentimento dos menores no contexto da *Internet*

O tratamento de dados de menores coloca diversos desafios, em particular quando os enquadramos no contexto da sociedade de informação.

Desde logo, coloca-se uma questão prévia sobre a sua capacidade para prestar consentimento. O RGPD não contém disposições específicas sobre a capacidade

de consentir dos menores, mas essas questões de capacidade estão intrinsecamente ligadas, a nosso ver, ao conceito de consentimento informado.

Na perspetiva de direito nacional, salvo disposição em contrário, os menores (de 18 anos) carecem de capacidade para o exercício de direitos (artigo 123º do CC), mas essa incapacidade pode ser suprida pelos titulares de responsabilidades parentais ou tutores (artigo 124º do CC). A nosso ver, a disposição do RGPD não afasta, necessariamente, a aplicação do regime da menoridade previsto nos artigos 122.º e ss. do CC.

Deste modo, consideramos que a capacidade para consentir o tratamento de dados pessoais por parte de menores com idade entre os 13 anos (idade limite estabelecida no artigo 16.º da LEN) e os 17 anos (inclusive) teria sempre de ser aferida casuisticamente de acordo com o regime da menoridade previsto no CC. Mais, o próprio RGPD e a LEN não obstam ao reconhecimento da capacidade dos menores para consentir no contexto dos serviços da Sociedade de Informação. Porém, ao não concretizarem como é que o exercício do referido consentimento é ou deverá ser executado, sempre se terá de aplicar o regime geral previsto no CC.

Em caso de falta de capacidade, o RGPD não proíbe que o consentimento seja prestado através de mandato, ou seja, por procuração, ainda que se exija que os demais requisitos (dever de informação, por exemplo), sejam cumpridos. No caso dos menores com idade inferior à legalmente estabelecida, o consentimento é dado pelos titulares de responsabilidades parentais em representação legal dos menores[42]. Contudo, o consentimento dado pelos pais em representação do filho menor não expira, automaticamente, quando a criança atinge a idade em que pode consentir diretamente, mas será necessário, a nosso ver, atualizar o consentimento, devido à sua granularidade.

Assim, o tema do consentimento dos menores deve ser analisado, antes de mais, a propósito do respetivo caráter livre. Ora, comparando com a DPD, o RGPD cria um nível adicional de proteção para os dados pessoais de *pessoas singulares vulneráveis*[43], em especial crianças. Com efeito, importa considerar que o RGPD

---

[42] O GT29 esclarece que, nem sempre, o titular da responsabilidade parental é o progenitor da criança e que a responsabilidade parental pode caber a várias partes, que podem incluir pessoas singulares e pessoas coletivas. Cf. Parecer WP259, cit., pp. 29-30.

[43] Apesar de o RGPD não prever uma definição do conceito de pessoas singulares vulneráveis, o Considerando 75 exemplifica as crianças e menores como um dos grupos de pessoas singulares vulneráveis. Para mais desenvolvimentos sobre o problema da vulnerabilidade nos menores, cf. Jonathan Herring, *Vulnerability, Childhood and the Law*, Springer Briefs in Law, 1ª edição, Springer, 2018, pp. 17-25; e, em especial, no contexto da proteção de dados, cf. Valentina Vincenza Cuocci, "Vulnerabilità, dati personali e mitigation measures. Oltre la protezione dei minori", in

estabelece regras específicas atinentes ao consentimento por menores. Tal resulta do artigo 8º e do Considerando 38 do RGPD, que dispõem uma proteção especial às crianças, nomeadamente impondo um limite de idade para o consentimento. Tratando-se de uma das cláusulas abertas do RGPD, cabe aos EM definir, internamente, a partir de que idade é que o menor é considerado capaz para prestar o seu consentimento. A LEN, como lei especial face ao CC, prevê, no seu artigo 16º, que no âmbito relativo à oferta direta de serviços da sociedade de informação, o consentimento dos menores só é válido quando os mesmos já tenham completado 13 anos de idade.

As maiores dificuldades relacionadas com o tema do consentimento dos menores têm a ver, no nosso entender, com (i) o dever de demonstração ou prova do consentimento pelos pais ou representantes, e (ii) garantia de cumprimento do dever de informação e respetiva compreensão das informações prestadas pelo menor habilitado a dar consentimento.

Assim, e quanto à primeira questão da prova, importa referir que, quando prestam serviços da sociedade da informação aos menores com base no consentimento, espera-se que os responsáveis pelo tratamento envidem *esforços razoáveis* para verificar se o utilizador já ultrapassou a idade para o consentimento digital e que essas medidas sejam proporcionais à natureza e aos riscos das atividades de tratamento[44].

Se os utilizadores afirmarem que já ultrapassaram a idade para o consentimento digital, então o responsável pelo tratamento pode – e deve – realizar verificações adequadas para comprovar que essa afirmação é verdadeira. Embora a necessidade de *envidar esforços razoáveis* para verificar a idade não conste explicitamente no RGPD, trata-se de uma exigência implícita porque o facto de a criança consentir sem ter idade suficiente para dar consentimento válido em nome próprio torna o tratamento dos dados ilícito. Se o utilizador afirmar que não tem idade para dar consentimento digital, então o responsável pelo tratamento pode aceitar esta declaração sem mais verificações, mas precisará de obter autorização parental e verificar se a pessoa que está a dar o consentimento é, efetivamente, o titular da responsabilidade parental.

Revista da Faculdade de Direito da Universidade de Lisboa (Lisbon Law Review), Ano LXII, n.º 1, Tomo 2, 2021, pp. 963-990, disponível *online* em www.fd.ulisboa.pt.

[44] Sobre o problema do controlo de dados – *dataveillance* –, em especial no caso dos menores, cf. Deborah Lupton / Ben Williamson, "The Datafied Child: The Dataveillance of Children and Implications for Their Rights.", in *New Media & Society*, vol. 19, n.º 5, maio de 2017, pp. 780-794.

A verificação da idade não deve, contudo, conduzir a um tratamento de dados excessivo. O mecanismo escolhido para verificar a idade de um titular de dados deve envolver a avaliação do risco do tratamento proposto. Nalgumas situações de baixo risco, pode ser adequado exigir que o novo subscritor do serviço revele o seu ano de nascimento ou preencha um formulário onde declara (não) ser menor. Em caso de dúvidas, o GT29[45] recomenda que o responsável pelo tratamento deve reavaliar os seus mecanismos de verificação da idade num determinado caso e considerar se são necessárias verificações alternativas.

Já quanto à segunda questão, o RGPD impõe que as informações devam ser compreensíveis para o público-alvo do responsável pelo tratamento, com especial atenção para a posição das crianças. Para obter "consentimento informado" de uma criança, o responsável pelo tratamento deve explicar em linguagem clara e simples para crianças de que forma pretende tratar os dados que irá recolher. Caso seja o progenitor quem supostamente deve consentir, então pode ser necessário um conjunto de informações que permita aos adultos tomar uma decisão informada.

O que precede demonstra claramente que o artigo 8.º do RGPD só é aplicável quando (i) o tratamento está relacionado com oferta direta de serviços da sociedade da informação a uma criança e (ii) o tratamento se baseia no consentimento.

Sobre o conceito de "Serviços da sociedade da informação", o RGPD, no seu artigo 4.º, n.º 25, remete para a Diretiva 2015/1535[46], segundo a qual "«Serviço» significa qualquer serviço da sociedade da informação, isto é, qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços". Identificamos, então, os seguintes elementos: (i) serviço prestado à distância, por via eletrónica; (ii) normalmente mediante remuneração; e (iii) mediante pedido individual de um utilizador ou beneficiário dos serviços.

Ao avaliar o âmbito desta definição, o GT29 remeteu para jurisprudência do TJUE[47], entendendo que a prestação de serviços em linha se insere no âmbito da expressão *serviços da sociedade da informação* que consta do artigo 8.º do RGPD.

Relativamente à autorização de um titular da responsabilidade parental, o RGPD não especifica formas práticas para obter o consentimento parental, nem tampouco para determinar se alguém está em posição de realizar essa ação. Por

[45] Cf. GT29, Parecer WP259, cit., pp. 30-32.
[46] Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação.
[47] Cf. Acórdão TJUE, Processo C-108/09 *Ker-Optika bt vs ÀNTSZ Dél-dunántúli Regionális Intézete*, de 2 de dezembro de 2010.

conseguinte, o GT29 recomendava a adoção de uma abordagem proporcionada, em consonância com os artigos 8.º, n.º 2, e 5.º, n.º 1, alínea c), do RGPD (*i.e.*, minimização dos dados). Neste sentido, uma abordagem proporcionada pode ser dar ênfase à obtenção de uma quantidade limitada de informações, tais como dados de contacto de um dos progenitores ou tutores. De qualquer modo, o que é razoável, tanto para verificar se o utilizador tem idade suficiente para dar consentimento, como para verificar se a pessoa que dá o consentimento em nome da criança é o titular da responsabilidade parental, pode depender dos riscos inerentes ao tratamento, bem como à tecnologia disponível.

O artigo 8.º, n.º 2, do RGPD acrescenta, em particular, que "o responsável pelo tratamento envida todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível". Cabe ao responsável pelo tratamento determinar quais são as medidas adequadas em cada caso específico. Regra geral, os responsáveis pelo tratamento devem evitar soluções de verificação que envolvam, elas mesmas, uma recolha excessiva de dados pessoais. No fundo, esta norma permite um nível de prova para o responsável pelo tratamento de dados inferior – ou menos exigente – ao que garante o regime geral, pois bastará demonstrar que envidou os esforços necessários para verificar o consentimento.

Já quanto aos serviços oferecidos diretamente a uma criança, a inclusão da expressão "oferta direta [...] às crianças" indica que o artigo 8.º do RGPD se destina a ser aplicado a alguns, mas não todos, os serviços da sociedade da informação. A este respeito, se um prestador de serviços da sociedade da informação deixar bem claro aos potenciais utilizadores que só oferece os seus serviços a pessoas com 18 anos ou mais e se este facto não for refutado por outros elementos de prova (tais como o conteúdo do sítio ou planos de comercialização), então o serviço não será considerado como uma *oferta direta às crianças* e o artigo 8.º não é aplicável.

Por fim, no que diz respeito à autonomia do titular dos dados para dar consentimento para o tratamento dos seus dados pessoais e ter controlo total sobre o tratamento, o consentimento dado por um titular da responsabilidade parental ou autorizado por um titular da responsabilidade parental para o tratamento dos dados pessoais das crianças pode ser confirmado, modificado ou retirado, assim que o titular dos dados atinja a idade para dar consentimento digital.

No entender do GT29, significa isto que, se a criança ou o menor não agir, o consentimento dado pelo titular da responsabilidade parental ou autorizado por um titular da responsabilidade parental para o tratamento dos dados pessoais antes da idade para o consentimento digital continuará a ser um fundamento válido para o tratamento.

Não concordamos com o referido entendimento. Após alcançar a idade para dar consentimento digital, a criança deverá, consciente das finalidades e riscos desse tratamento, dar o seu consentimento diretamente (renovando-o perante o responsável pelo tratamento) e não apenas retirar o consentimento, em consonância com o artigo 7.º, n.º 3, do RGPD. A solução mais adequada seria a renovação do consentimento.

Por último, o RGPD determina que as regras relativas aos requisitos de autorização parental em relação a menores não interferem com "o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos do contrato em relação a uma criança". Por conseguinte, os requisitos para obter um consentimento válido para a utilização de dados acerca de crianças fazem parte de um quadro jurídico que deve ser considerado diferente do direito contratual nacional.

2.3 A retirada do consentimento

Antes de passarmos a problemas concretos do consentimento, e apesar de já termos adiantado alguns aspetos deste regime, cumpre analisar o artigo 7.º, n.º 3 do RGPD. Este normativo especifica que "o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento". Assim, por exemplo[48], se o consentimento for obtido por meios eletrónicos unicamente clicando no rato, deslizando o dedo ou pressionando uma tecla, os titulares dos dados devem, na prática, poder retirar esse consentimento de forma igualmente fácil.

Adicionalmente, a retirada do consentimento não deverá comportar qualquer prejuízo ou custo para o titular de dados, *i.e.*, o responsável pelo tratamento deve prever a possibilidade de retirar o consentimento de forma gratuita ou sem baixar os níveis do serviço[49].

O caráter gratuito da retirada do consentimento contraria o disposto no nosso regime civilista referente não apenas ao consentimento do lesado, previsto no artigo 340º do CC, e o qual determina o pagamento de uma indemnização aquando da retirada do consentimento, mas também quanto ao regime da limitação voluntária dos direitos de personalidade, prevista no artigo 81º, n.º 2 do CC, que estabelece

[48] Cf. GT29, Parecer WP259, cit., pp. 24-25.

[49] Cf. GT29, Parecer WP259, cit., p. 24-25, bem como, Parecer 4/2010 do GT29 sobre o código de conduta europeu da *Federation of European Direct and Interactive Marketing* (FEDMA) relativo ao uso de dados pessoais no marketing direto (WP 174) e o parecer sobre a utilização de dados de localização para criar serviços de valor acrescentado (WP 115).

que a limitação é sempre revogável, ainda que com obrigação de indemnizar os prejuízos causados às legítimas expectativas da outra parte.

Sempre se poderia colocar, contudo, a questão de saber se o titular dos dados, ao retirar o seu consentimento, não estará obrigado, em certos casos, e ao abrigo do instituto do enriquecimento sem causa, a restituir o montante correspondente ao sacrifício tido pelo responsável pelo tratamento e à vantagem que o titular dos dados obteve ao consentir o tratamento dos seus dados. A nossa posição é a de que este entendimento seria, em regra, questionável, porquanto a própria disponibilização dos dados pessoais do titular sempre consubstanciaria uma contrapartida económica[50] pelos eventuais serviços prestados ou sacrifícios tidos pelo responsável pelo tratamento e, portanto, a retirada do consentimento não geraria uma situação de manifesto desequilíbrio entre as partes, na medida em que o responsável já terá beneficiado com o prévio consentimento do titular dos dados.

Pelo contrário, temos dúvidas se a retirada do consentimento já não poderá despoletar prejuízos mais significativos no âmbito dos ensaios clínicos, por exemplo, porquanto o benefício que o responsável pelo tratamento retiraria do processamento de dados pressupõe, necessariamente, a manutenção do consentimento até à conclusão do ensaio clínico, sob pena de frustração da finalidade do ensaio.

Ademais, na nossa opinião, este direito à retirada livre do consentimento terá de ser conjugado com o instituto do abuso de direito – consagrado, no ordenamento jurídico português, no artigo 334.º do CC –, com vista a assegurar que o exercício do referido direito não extravasa, de modo inadmissível, os limites impostos pela boa-fé, nomeadamente na sua vertente de tutela da confiança, em virtude de se frustrarem, de modo objetivo, expectativas legítimas da outra parte.

Sem prejuízo do exposto supra, cumpre assinalar que a retirada do consentimento é concretizada, nos termos do RGPD, por via da consagração do direito ao esquecimento[51] (cf. artigo 17.º do RGPD), o qual atribui ao titular dos dados o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais. O responsável pelo tratamento tem, por sua vez, a obrigação de apagar os dados

---

[50] Veja-se, aliás, que os dados pessoais consubstanciam um importante ativo na denominada "economia de dados" ou *Data Economy*, pelo que existe sempre um benefício do responsável pelo tratamento ao lhe ser consentido, ainda que temporariamente, o tratamento de dados pessoais de um titular. Para uma maior compreensão do conceito de *Data Economy*, cf. ALBERT OPHER et. al, "The Rise of the Data Economy: Driving Value through *Internet* of Things Data Monetization", in *IBM Legal Book*, 2016, pp. 1-16.

[51] A consagração do direito ao esquecimento foi uma das grandes novidades do RGPD (artigo 17.º), especialmente atendendo ao famoso Acórdão *Google Spain SL vs Mário Costeja González* (Processo C-131/12, de 13 de maio de 2014).

pessoais, sem demora injustificada, nomeadamente quando o titular retire o consentimento em que se baseia o tratamento dos seus dados nos termos do artigo 6º, n.º 1, alínea a) ou do artigo 9º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento.

Assim, regra geral, se o consentimento for retirado, todas as operações de tratamento de dados baseadas nesse consentimento e que ocorreram antes da retirada do consentimento – e em conformidade com o RGPD – permanecem lícitas. Contudo, o responsável pelo tratamento deve parar as ações de tratamento em causa. Não obstante, a retirada do consentimento não significa que o responsável pelo tratamento tenha de apagar os dados tratados para uma finalidade que se baseia na execução do contrato celebrado com o titular dos dados, por exemplo. Por conseguinte, é essencial que os responsáveis pelo tratamento, desde o início, sejam muito claros quanto à finalidade a que corresponde cada elemento dos dados e em que fundamento legal assenta.

Como já fomos referindo anteriormente, o responsável pelo tratamento de dados deve garantir que a retirada do consentimento é tão fácil e rápida como foi dar o consentimento originalmente. A retirada do consentimento coloca, contudo, situações existentes e em curso, que tenham o consentimento como forma de licitude do tratamento de dados, numa situação precária, daí o problema da sua fragilidade, como se verá de seguida.

Por fim, coloca-se a questão da natureza jurídica e da qualificação dogmática desta retirada do consentimento no âmbito da cessação contratual, nomeadamente saber se estamos perante a figura da resolução, da denúncia, da revogação ou de outro modo de extinção da relação jurídica como, por exemplo, o direito ao arrependimento.

A nosso ver, trata-se de uma figura *sui generis* e que não se insere em nenhum dos modos de extinção acima referidos. Com efeito, a retirada do consentimento não carece de qualquer fundamentação ou justa causa, nem existe um prazo ou necessidade de pré-aviso para que o seu exercício seja legítimo. Por isso, qualificamos esta retirada do consentimento como um modo de desvinculação unilateral e imotivada da relação jurídica subjacente ao tratamento dos dados pessoais do titular.

2.4 A fragilidade do consentimento

Quando o consentimento está a ser utilizado como fundamento legal para o tratamento, deve existir, portanto, sempre a possibilidade de o titular dos dados o retirar facilmente. Nessa medida, o consentimento enquanto fundamento legal de tratamento de dados apresenta-se como um fundamento frágil e dependente da vontade, unilateral, do titular dos dados.

Esta fragilidade é particularmente notória em situações de investigação científica, na qual a retirada do consentimento pode prejudicar alguns projetos de investigação científica que exijam que os dados estejam associados a certas pessoas. Contudo, o RGPD é claro quanto a esta matéria: o consentimento pode ser retirado e os responsáveis pelo tratamento devem agir em conformidade. Não existe exceção a este requisito para fins científicos (ou outros). Portanto, se um responsável pelo tratamento de dados receber um pedido de retirada de consentimento, deve, em princípio, apagar imediatamente os dados pessoais se quiser continuar a utilizar os dados para fins de investigação (ou, diríamos, pelo menos, anonimizá-los).

A fragilidade do consentimento também é particularmente latente no caso do consentimento dos menores, onde a sua prova é particularmente difícil, em especial quando é dado pelos titulares de responsabilidades parentais.

Adicionalmente, o consentimento afigura-se como uma condição de licitude particularmente frágil nas situações em que não exista paridade entre as partes, ou seja, nas situações em que exista uma parte mais fraca, seja em virtude da assimetria informativa que carateriza a referida relação (*v.g.* no âmbito das relações de consumo), seja porque existe subordinação jurídica (v.g. nas relações laborais), seja, ainda, por se referirem a situações de especial vulnerabilidade do titular de dados (v.g. o caso dos menores, bem como no âmbito dos dados de saúde ou até da atividade seguradora).

Assim, e concluindo, o consentimento, apesar de ser uma forma de licitude comumente utilizada, é efetivamente frágil, na medida que não oferece a segurança jurídica que outros fundamentos de licitude oferecem como, por exemplo, a necessidade do tratamento para a execução de um contrato.

2.5 Articulação do RGPD com o consentimento prestado no âmbito da DPD

Analisadas as fontes com relevância para a análise do tema do consentimento do titular de dados, e o seu próprio conceito e concretização do mesmo, cumpre ainda analisar a questão prévia de saber o que acontece aos consentimentos obtidos nos termos da DPD, atendendo à entrada em vigor do RGPD, e atendendo à granularidade do consentimento.

Tem sido entendimento do GT29, quer do EDPB, que os responsáveis pelo tratamento de dados que procedem atualmente ao tratamento com base no consentimento em conformidade com as normas nacionais de proteção de dados não são automaticamente obrigados a renovar totalmente todas as relações de consentimento existentes com os titulares dos dados em preparação para o RGPD.

Portanto, o consentimento que foi obtido até à data de entrada em vigor do RGPD continua válido na medida em que esteja em consonância com as condições

do RGPD. Era importante, contudo, que antes da entrada em vigor do RGPD, os responsáveis pelo tratamento tivessem revisto pormenorizadamente os processos de trabalho e registos atuais, de modo a garantirem que os consentimentos existentes cumprem os critérios do RGPD – cf. Considerando 171.

Na prática, e como já referido, o RGPD eleva o nível de exigência no que toca à aplicação de mecanismos de consentimento e introduz vários novos requisitos que exigem que os responsáveis pelo tratamento alterem os mecanismos de consentimento, em vez de apenas reescreverem as políticas de privacidade.

De igual modo, uma vez que o RGPD exige uma "declaração ou ato positivo inequívoco", todos os presumíveis consentimentos que se tiverem baseado numa forma mais implícita de ação por parte do titular dos dados (*v.g.* uma opção pré-assinalada de aceitação, *i.e.*, um *opt-in* pré-definido) também não cumprem o disposto no RGPD em matéria de consentimento e terão, consequentemente, de ser renovados.

Além disso, por forma a ser possível demonstrar que o consentimento foi obtido ou permitir manifestações de vontade mais granulares por parte dos titulares dos dados, poderá haver necessidade de rever as operações e os sistemas informáticos. Também devem estar disponíveis mecanismos que permitam aos titulares dos dados retirar facilmente o seu consentimento e devem ser fornecidas informações sobre como fazê-lo. Se os procedimentos existentes para obtenção e gestão do consentimento não cumprirem as normas do RGPD, os responsáveis pelo tratamento terão de obter novos consentimentos que estejam em conformidade com o RGPD.

Por outro lado, uma vez que nem todos os elementos referidos nos artigos 13.º e 14.º do RGPD devem estar presentes como condição para um consentimento informado, os deveres de informação alargados previstos no RGPD não se opõem necessariamente à continuidade do consentimento que foi concedido antes da entrada em vigor do RGPD.

Nos termos da DPD, não existia requisito de informar os titulares dos dados acerca do fundamento para efetuar o tratamento. Se o responsável pelo tratamento verificar que o consentimento dado anteriormente nos termos da antiga legislação não cumpre as normas de consentimento do RGPD, os responsáveis pelo tratamento devem tomar medidas para cumprir essas normas, por exemplo, revalidando o consentimento de forma a cumprir o RGPD.

Note-se, ainda, que nos termos do RGPD, não é possível mudar de um fundamento legal para outro. Se o responsável pelo tratamento não conseguir renovar o consentimento em conformidade com as novas normas e também não conseguir – em situação excecional – fazer a transição para uma situação conforme com o RGPD, baseando o tratamento dos dados num fundamento legal diferente,

garantindo ao mesmo tempo que o tratamento continua a ser leal e responsável, as atividades de tratamento devem cessar. Em todo o caso, importa esclarecer que o responsável pelo tratamento deverá observar os princípios da licitude, lealdade e transparência aplicáveis ao tratamento de dados, previstos no artigo 5º do RGPD.

2.6 Articulação com o Direito Civil Português

Numa parte anterior do nosso estudo, já tivemos oportunidade de adiantar que, para alguns autores, o consentimento se afigura como uma manifestação de vontade que reconduz ao regime civilista dos negócios e dos atos jurídicos[52], e que essa recondução à dogmática civilística é possível na medida em que, no RGPD, não consta um completo regime negocial e, portanto, o Direito Civil, com as necessárias adaptações, é aplicável sempre que o RGPD não consagre uma solução especial – o que acontece com relativa frequência, atendendo às cláusulas de abertura que o próprio RGPD prevê para preenchimento pelos EM, sendo que esse preenchimento será, naturalmente, efetuado de acordo com o direito interno de cada EM, mais concretamente à luz das respetivas normas de Direito Civil.

Deste modo, e apesar de não ser uma posição unânime na doutrina, também acolhemos a posição de que cabe ao intérprete-aplicador recorrer às bases legais nacionais, nomeadamente do Direito Civil, para interpretar e aplicar as normas de direito da proteção de dados, garantindo que não contrariam o entendimento do RGPD enquanto lei supranacional e lei especial. Assim, e não obstante o conceito de consentimento consagrado no RGPD, questionamo-nos sobre a sua possível articulação com o Direito Civil português.

Nessa medida, e em primeiro lugar, questionamo-nos se podemos considerar o consentimento do titular de dados um direito subjetivo. Ora, se adotarmos a tese de Menezes Cordeiro[53], no direito subjetivo abdica-se de se dizer o que se

---

[52] Neste sentido, cf. António Barreto Menezes Cordeiro, "O Consentimento...", cit., p. 41.

[53] Comparativamente, Savigny defendia um conceito significativo-ideológico de direito subjetivo, na esteira da terceira sistemática, segundo o qual o direito subjetivo seria um poder da vontade da pessoa. Assim, poderia entender-se o consentimento como o poder da vontade do titular de dados em autorizar terceiros a tratar os seus dados? Entendemos que não. A teoria da vontade savignyana foi criticada por não prever as situações de pessoas privadas de vontade (menores ou incapazes, por exemplo). Assim sendo, e uma vez que a teoria de Savigny não previa essas situações, por entender a vontade relevante como a vontade da pessoa (e que ela estivesse presente no exercício dessa vontade), o consentimento não poderia, a nosso ver, ser considerado um direito subjetivo à luz desta teoria. Jhering, por sua vez, pega na teoria de Savigny e refuta-a, defendendo que o que releva é a tutela e o aproveitamento de um interesse juridicamente protegido. Defende, assim, uma noção técnica de

protege para relevar, apenas, como se faz essa proteção (escola jurídico-formal). Portanto, o direito subjetivo parte da norma jurídica, pelo que as concretas posições jurídicas das pessoas não podem ser determinadas através de regras objetivas, mas sim graças à atuação de vontades individuais. Nesse sentido, Menezes Cordeiro apresenta a sua solução para o debate em torno da natureza do direito subjetivo, defendendo que se trata de uma "permissão normativa específica de aproveitamento de um bem"[54].

No âmbito dos dados pessoais, e como já referido, tem vindo a ser defendida a existência de um direito à identidade informacional, num quadro mais alargado de direito geral de personalidade[55]. Com efeito, entendemos que, não obstante as dúvidas que tal conceção suscite, é defensável a existência de um direito à identidade informacional e que esse seja reconhecido como um direito de personalidade, nos termos do artigo 70º do CC que dispensa uma tutela geral, podendo dar azo a direitos subjetivos de personalidade em sentido próprio, sem qualquer tipicidade.

Portanto, o direito de personalidade típico analisa-se numa permissão de aproveitamento de um bem de personalidade. Mais, atendendo à existência de um direito de personalidade à identidade informacional, poderemos considerar que o consentimento é também um direito de personalidade? Quanto a nós, a resposta terá de ser negativa, *i.e.*, o consentimento não é um direito de personalidade, mas sim uma modalidade de direito subjetivo, de natureza distinta.

Assim, o consentimento, enquanto manifestação de vontade do titular, enquadra-se, quanto a nós, no conceito de direito potestativo, o qual consiste na faculdade conferida a alguém de, unilateralmente, alterar a esfera jurídica de outrem, independentemente da sua vontade[56]. Trata-se, contudo, de poderes atribuídos ao beneficiário através de normas permissivas, *i.e.*, cabe ao titular, segundo o seu livre-arbítrio, atuar ou não o poder que a norma lhe concede.

Por essa via, e atendendo à definição de direito subjetivo, o consentimento pode ser entendido como um bem – neste caso o bem é a pessoa, a sua personalidade e a sua identidade traduzida em dados pessoais identificáveis –, que o titular poderá aproveitar, ou não, como quiser.

---

direito subjetivo. Com efeito, para Jhering, não existem direitos sem interesse. Contudo, se formos a atender ao consentimento como direito subjetivo na ótica de Jhering, não seria defensável, na medida em que o consentimento não exige, necessariamente, um interesse por parte do titular de dados. Para mais desenvolvimentos, cf. António Menezes Cordeiro, *Tratado de Direito Civil*, I, 4ª edição, reimp. 2021, pp. 873-881.

[54] António Menezes Cordeiro, *Tratado de Direito Civil*, I, cit., pp. 892-895.

[55] Nesse sentido, cf. Alexandre Sousa Pinheiro, *Privacy*, cit., pp. 914 e ss.

[56] António Menezes Cordeiro, *Tratado de Direito Civil*, I, cit., p. 897.

Assim, poderá entender-se o consentimento como um direito potestativo de personalidade (de identidade informacional), na medida em que a sua atuação permite ao titular do bem o controlo da proteção e do tratamento dos seus dados pessoais.

Não obstante, poderia igualmente equacionar-se, antes, se estamos perante uma limitação voluntária ao direito de personalidade de identidade informacional do titular de dados.

No nosso entendimento, além de o consentimento do RGPD ser um direito potestativo, poderá tratar-se, também, de uma limitação voluntária de direitos de personalidade, embora atípica, no sentido em que o disposto no artigo 81º do CC não é aplicável *tout court* no âmbito do RGPD.

O consentimento pode, efetivamente, ser entendido como uma limitação lícita e voluntária ao direito à identidade informacional e à proteção de dados pessoais e até ao direito à privacidade. É, contudo, uma limitação voluntária atípica, na medida em que (i) decorre de um direito de personalidade atípico (originário da cláusula aberta do artigo 70º do CC) e (ii) a sua regulação obedece ao disposto no RGPD, como lei especial, ao abrigo do primado do Direito da União.

O artigo 81º do CC admite, em termos genéricos, essa limitação voluntária dos direitos de personalidade, desde que não se mostre atingida a ordem pública. Os direitos de personalidade representam, como quaisquer outros direitos subjetivos, posições de liberdade, reconhecidas ao seu beneficiário e, nessa qualidade, implicam disponibilidade por parte do seu titular.

Com efeito, o consentimento no RGPD pressupõe que o titular dos dados, previamente à autorização, tenha toda a informação necessária à tomada decisória de forma informada (princípio da transparência) e que o seu consentimento seja claro e inequívoco, garantindo a sua eficácia perante terceiros.

Contudo, a lei admite limitações temporárias, mas não alienações definitivas de direitos de personalidade. Daí que o artigo 81º fixe, igualmente, a regra de livre revogabilidade, ainda que com possível obrigação de indemnizar. No nosso entender, a obrigação de indemnizar, prevista no artigo 81º do CC, surge como forma de tutela da chamada "negociabilidade limitada" de direitos de personalidade de natureza creditícia, não impedindo, porém, que essa limitação se verifique perante direitos de personalidade de outra natureza.

Também no âmbito do RGPD, o consentimento, enquanto direito potestativo, prevê a possibilidade da sua retirada, mas não implica qualquer obrigação de indemnizar, ao contrário do previsto no artigo 81º, n.º 1 do CC. Concretizando, a obrigação de indemnizar não se aplica aos dados pessoais, na medida em que o titular de dados, ao consentir o seu tratamento por terceiros, não está a celebrar

um negócio jurídico com vista à "venda" dos seus dados e não recebe qualquer contrapartida pecuniária para o efeito. O direito à identidade informacional, a nosso ver, enquadra-se na modalidade de direitos de personalidade sociais, em paralelo com a reserva da vida privada e cujo núcleo essencial não tem natureza creditícia. Logo, não se poderá aplicar o mesmo raciocínio da indemnização do artigo 81º, n.º 1 do CC.

Adicionalmente, o RGPD, enquanto lei especial, afasta expressamente a obrigação de indemnização prevista na lei nacional sem, contudo, a nosso ver, retirar o conteúdo essencial associado ao regime da limitação voluntária de direitos de personalidade.

Em súmula, entendemos que o consentimento se pode caracterizar, simultaneamente, como um direito potestativo e como uma limitação voluntária atípica do direito de personalidade do titular de dados, ainda que a sua retirada não acarrete qualquer obrigação de indemnizar.

3 Problemas específicos do consentimento no contexto da *Internet*

3.1 Consentimento para transferências de dados para países terceiros ("*cross-border transfers*")

O tema da transferência de dados para países terceiros está regulada nos artigos 44º e ss do RGPD e no artigo 22.º da LEN.

O RGPD aplica-se, principalmente, aos controladores e subcontratantes localizados no EEE, com algumas exceções. Nessa base, o RGPD restringe as transferências de dados pessoais para fora do EEE, a menos que os direitos das pessoas singulares relativamente aos seus dados pessoais sejam protegidos de outra forma, ou que se aplique uma de um número limitado de derrogações.

Uma transferência de dados pessoais fora do âmbito da proteção do RGPD (que se pode designar por "transferência restrita") implica, na maioria dos casos, uma transferência do interior do EEE para um país fora do EEE.

Se se estiver a efetuar uma transferência restrita que não esteja abrangida por uma decisão de adequação, nem por uma salvaguarda adequada, só se pode efetuar essa transferência se estiver abrangida por uma das derrogações previstas no artigo 49º do RGPD.

Adicionalmente, nos termos do artigo 44º da RGPD, qualquer transferência de dados pessoais para países terceiros ou organizações internacionais deve, para além de cumprir com o Capítulo V do RGPD, satisfazer, também, os requisitos de outras disposições do RGPD. Nomeadamente, cada transferência deve respeitar os

princípios de proteção de dados previstos no artigo 5º do RGPD, ser lícita de acordo com o artigo 6º e cumprir com o disposto no artigo 9º, quando estejam em causa categorias especiais de dados. Por conseguinte, deve ser aplicado um teste em duas fases: primeiro, deve ser aplicada uma base jurídica ao processamento de dados enquanto tal, juntamente com todas as disposições relevantes do RGPD; e, como segundo passo, as disposições do Capítulo V do RGPD devem ser cumpridas.

O RGPD especifica no seu artigo 46º que, "na ausência de uma decisão nos termos do nº 3 do artigo 45º, um responsável pelo tratamento ou processador pode transferir dados pessoais para um país terceiro ou para uma organização internacional apenas se o controlador ou processador tiver fornecido garantias adequadas, e na condição de que estão disponíveis direitos executórios para os titulares dos dados e vias de recurso eficazes para os titulares dos dados". Podem ser previstas garantias adequadas por um instrumento juridicamente vinculativo e executório entre organismos públicos (Artigo 46.º, n.º 2, al. a) RGPD) ou, sujeito a autorização das autoridades de supervisão competentes, por disposições a inserir em acordos administrativos entre organismos públicos que incluam direitos executórios e efetivos do titular dos dados (Artigo 46.º, n.º 3, al. b) RGPD).

Mais recentemente, analisou-se o problema da transferência de dados para países terceiros a propósito da decisão do TJUE no âmbito do Caso *Schrems II*[57].

Em termos resumidos, o TJUE julgou que a Decisão *Privacy Shield*, relativa à transferência de dados pessoais entre a UE e os EUA, e através da qual a COM considerava que determinadas entidades norte-americanas asseguravam um nível de proteção substancialmente equivalente à europeia, é inválida, na medida em que a legislação nacional dos EUA e, em particular, certos programas que permitem

[57] Como antecedente, veja-se o caso Schrems I (Processo C-362/14). O caso Schrems remonta a 2015, quando Max Schrems contestou, junto da autoridade de controlo irlandesa, a validade do acordo de *Safe Harbor* – um dos mecanismos então utilizados para transferências internacionais de dados para os EUA. A queixa de Schrems fundava-se na alegada falta de garantias do mecanismo do *Safe Harbour* relativamente à utilização de sistemas de vigilância estatais, nos termos da legislação norte-americana. Na sequência dessa queixa, o TJUE viria a invalidar o *Safe Harbour*. Em sua substituição, foi criado outro mecanismo – o *Privacy Shield* – que constitui um esquema de autocertificação, ao qual as empresas sedeadas nos EUA aderem, atestando a adequação das medidas de segurança, por si implementadas, para a proteção dos dados pessoais e direitos dos titulares. Por sua vez, no acórdão do TJUE (Processo C-311/18), de 20 de julho de 2020, declarou-se igualmente inválida a decisão *Privacy Shield*. Veja-se ainda o comentário do próprio Max Schrems, a pedido da CNPD, ao acórdão Schrems II e traduzido para português – "Processo Schrems II: Do passado e o Futuro", in *Revista Forum CNPD – Em foco: O encarregado de proteção de dados*, n.º 07 (Dezembro) 2020, pp. 8-21, disponível *online* em www.cnpd.pt.

o acesso das respetivas autoridades públicas, para fins de segurança nacional, a dados pessoais transferidos da UE, resultam em limitações à proteção de dados pessoais que não estão enquadradas de forma a satisfazer requisitos substancialmente equivalentes aos exigidos pelo direito da UE.

Além disso, considerou o TJUE que a legislação dos EUA não oferece aos titulares dos dados qualquer via de recurso com garantias substancialmente equivalentes às exigidas na UE[58]. Consequentemente, as transferências baseadas neste quadro jurídico foram consideradas ilegais e assinalou-se a necessidade de analisar outros fundamentos de licitude como, eventualmente, o consentimento[59].

Sem prejuízo, além do disposto no artigo 46º do RGPD, na sua ausência o artigo 49º do RGPD também oferece um número limitado de situações específicas em que as transferências internacionais de dados podem ter lugar quando não há uma decisão de adequação por parte da COM. Em particular, uma isenção abrange as transferências necessárias por razões importantes de interesse público reconhecidas no direito da União ou no direito do EM ao qual o responsável pelo tratamento está sujeito, inclusive no âmbito do espírito de reciprocidade da cooperação internacional.

---

[58] O mesmo problema verificou-se com as transferências de dados para o Reino Unido após o término do período de transição do "Brexit" a 31.12.2020 (*i.e.*, a saída do Reino Unido da UE e a cessação do seu estatuto enquanto EM). Apesar de, à data do "Brexit" não existir decisão de adequação da UE a propósito do Reino Unido, a expectativa de adequação era praticamente total. Contudo, seria sempre necessária a decisão de adequação para que, doravante, pudesse haver transferência de dados de e para o Reino Unido, enquanto país terceiro. A 28 de junho de 2021, a COM adotou duas decisões de adequação visando o Reino Unido (C(2021) 4800): uma ao abrigo do RGPD e outra nos termos da Diretiva 2016/680, pelas quais reconhece que o Reino Unido assegura um nível de proteção adequado aos dados pessoais transferidos desde a União Europeia para aquele país. Nessa medida, os dados pessoais poderão continuar a ser livremente transferidos da União Europeia para o Reino Unido, sem necessidade de garantias ou autorizações adicionais, de acordo com o RGPD. Contudo, estas decisões foram alvo de críticas pelo Parlamento Europeu, na sua Resolução de 21 de maio de 2021 (disponível *online* em www.europarl.europa.eu), sobre a proteção adequada dos dados pessoais pelo Reino Unido (2021/2594(RSP)), "(...) por considerar que os projetos de decisão de execução não são compatíveis com o direito da UE.", exortando à retificação das duas decisões pela COM.

[59] Em termos práticos, verificou-se a tendência de as empresas adotarem as cláusulas contratuais tipo como meio de regular as transferências de dados pessoais para países terceiros. Esta foi a opção tomada, por exemplo, pela Google, mas também pela Microsoft, pelo Facebook e outros gigantes tecnológicos. Cumpre, todavia, averiguar que requisitos ou garantias deverão ser implementados para validar tais opções. Mais recentemente, a 25 de março de 2022, a COM e os EUA anunciaram, em conjunto, que chegaram a um acordo de princípio sobre transferência de dados pessoais entre UE e EUA que responderá às preocupações levantadas pelo TJUE na decisão *Schrems II* de julho de 2020.

Contudo, as derrogações previstas no artigo 49º do RGPD devem ser interpretadas de forma restritiva e dizem principalmente respeito a atividades de processamento que são ocasionais e não repetitivos[60].

Ora, uma das derrogações previstas no artigo 49º do RGPD é o *consentimento [explícito]*. Uma vez que o consentimento deve ser explícito (e específico), por vezes é impossível obter o consentimento prévio da pessoa em causa para uma transferência futura no momento da recolha dos dados. Com efeito, para que esta transferência seja válida com fundamento na derrogação do consentimento, a pessoa em causa deve dar o seu explícito consentimento para esta transferência específica no momento em que está prevista a transferência.

Deste modo, o consentimento fornecido no momento da recolha dos dados pela empresa da UE para fins de entrega não é suficiente para justificar a utilização desta derrogação para a transferência de dados pessoais para fora da UE que está prevista para mais tarde. Por conseguinte, o exportador de dados deve certificar-se de que obtém o consentimento específico antes de a transferência ser efetuada, mesmo que tal ocorra após a recolha dos dados.

Este requisito está também relacionado com a necessidade de o consentimento ser informado. O consentimento "informado" exige, no caso de o consentimento ser uma base legal nos termos do artigo 6.º, n.º 1, alínea a), para uma transferência de dados, que a pessoa seja devidamente informada antecipadamente e de forma adequada da situação específica em que se encontra, das circunstâncias da transferência – *v.g.*, identidade do responsável pelo tratamento dos dados, finalidade da transferência, tipo de dados, direito de retirada do consentimento, identidade ou categorias de destinatários, riscos específicos resultantes da transferência de dados para um país que não assegura uma proteção adequada e que não aplica salvaguardas adequadas destinadas a garantir a proteção dos dados.

O fornecimento desta informação é essencial para permitir que a pessoa em causa dê o seu consentimento com pleno conhecimento destes factos específicos da transferência e, por conseguinte, se não for fornecida, a derrogação não será aplicável.

No caso específico de uma transferência ser efetuada após a recolha de dados pessoais, o exportador de dados deve informar a pessoa em causa da transferência e dos seus riscos antes que ela ocorra, a fim de obter o seu consentimento explícito para a transferência "proposta".

---

[60] Neste sentido, cf. EDPB "Guidelines on derogations of Article 49 under Regulation 2016/679", p. 5 e "Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies", pp. 4-5, disponível *online* em www. edpb.europa.eu.

Como demonstrado pela análise acima, o RGPD estabelece um limiar elevado para a utilização da derrogação de consentimento. Dado esse elevado padrão de exigência para obtenção de um consentimento válido e o facto de o consentimento poder ser retirado, unilateralmente, pelo titular de dados, tal pode significar que a utilização do consentimento não será a solução mais viável para a transferência de dados.

3.2 Consentimento no âmbito de cláusulas contratuais gerais

Outro problema específico do consentimento verifica-se no âmbito do chamado "tráfego negocial de massas" e das cláusulas contratuais gerais (*allgemeine Geschäftsbedingungen*) que são comummente tratados no âmbito dos contratos de adesão[61]. Os contratos de adesão, por sua vez, são muito comuns no âmbito de contratos de consumo ou, em particular, no comércio eletrónico[62], dos contratos celebrados à distância ou através da *Internet*.

Ora, estes tipos contratuais foram surgindo em virtude de necessidades de rapidez e maior eficiência contratual, em especial com o crescimento da sociedade de informação que promoveu, de forma significativa, o crescimento destas modalidades contratuais.

As cláusulas contratuais gerais, em termos simples, são proposições pré-elaboradas que proponentes ou destinatários indeterminados se limitam a propor ou aceitar. Têm como requisitos essenciais a (i) generalidade, (ii) a rigidez, (iii) a desigualdade entre partes, (iv) a complexidade das cláusulas e (v) a natureza formulária[63].

---

[61] Ou também denominados como "contratos-standard" ou padronizados, "contratos-tipo" ou contratos "pré-redigidos". Para mais desenvolvimentos sobre os contratos de adesão e cláusulas contratuais gerais, cf. Carlos Ferreira de Almeida, *Contratos – Conceitos, Fontes, Formação*, vol. I, 6.ª edição, 2020, reimp., pp. 193 e ss.

[62] Note-se que os consumidores são, tradicionalmente, considerados como sendo a parte contratual mais fraca, atendendo, designadamente, à sua falta de informação (quer quanto aos produtos a adquirir, quer quanto aos seus direitos), ao seu baixo poder económico, ao menor ou até nulo poder negocial, à utilização de técnicas de vendas pouco leais, etc., sendo que a utilização da *Internet* na celebração de contratos com consumidores poderá potenciar um maior desequilíbrio entre as partes contratantes. Neste sentido, e para mais desenvolvimentos, cf. Elsa Dias Oliveira, "Tutela do consumidor na *internet*" in *Direito da sociedade da informação*, vol. 5., Coimbra, Coimbra Editora, 2004, pp. 335-358. No âmbito da contratação eletrónica, em particular, cf. Elsa Dias Oliveira, *A Proteção dos Consumidores nos Contratos Celebrados Através da Internet*, Almedina, Coimbra, 2002, pp. 17 e ss.; Sebastião Nóbrega Pizarro, *Comércio Electrónico – Contratos Electrónicos e Informáticos*, Almedina, Coimbra, 2005, pp. 11 e ss..

[63] Sobre esta definição, cf. António Menezes Cordeiro, *Tratado de Direito Civil,* II, Almedina, 4.ª edição, Coimbra, 2020, reimp., pp. 357 e ss. Em sentido contrário, cf. Carlos Ferreira de Almeida, *Contratos* I, cit., pp. 197 e ss., sendo que este autor sustenta, como mais rigoroso, atribuir apenas as características seguintes: predisposição unilateral e generalidade.

Desde sempre que a doutrina tem sido crítica sobre se podemos entender que às cláusulas contratuais gerais se aplica o regime geral do negócio jurídico, previsto no CC, em particular no que concerne à formação do contrato. Assim, os negócios de adesão formam-se e executam-se a um ritmo incompatível com um esquema negocial típico, que faculte aos seus intervenientes um consciente exercício das suas liberdades de celebração e estipulação.

Com efeito, as cláusulas contratuais gerais vieram promover a erosão dos esquemas negociais, na medida em que (i) a liberdade de estipulação é posta em causa, pois as pessoas desenvolvem uma atividade jurídica em que se limitam a aceitar ou recusar certos esquemas que lhes são propostos, onde não há negociação, nem contrapropostas; e (ii) a própria liberdade de celebração é puramente teórica, na medida em que as pessoas utilizam esquemas jurídicos de tipo negocial sem que, verdadeiramente, chegue a haver qualquer manifestação de vontade[64].

Portanto, este modo particular de circulação jurídica que prescinde de uma efetiva liberdade de estipulação, através de adesões maciças a esquemas pré-elaborados, corresponde à técnica negocial *standard* das cláusulas contratuais gerais. São designados por alguns autores, como *contratos não negociais*, visto que não se caracterizam por haver liberdade de estipulação.

Além disso, defende-se que, ao não haver uma efetiva manifestação de vontade contratual, a contratação, ao abrigo da adesão a cláusulas contratuais gerais, é feita através dos chamados comportamentos concludentes[65]. Ora, em termos simples, os comportamentos concludentes não exprimem qualquer vontade, mas apenas uma rotina ou um comportamento padrão e que, ainda assim, é admitido pelo Direito como válido. São, portanto, relações contratuais de facto.

No caso do consentimento no âmbito do problema das cláusulas contratuais, a nosso ver, o maior desafio coloca-se no contexto das comunicações comerciais.

Ora, a DCE regula as chamadas "comunicações publicitárias em rede "ou publicidade em rede e aqui surge a problemática das comunicações não solicitadas, que a diretiva deixa, em grande medida, em aberto. A DCE faz ainda referência à DEP, cujo artigo 13.º diz respeito às comunicações não solicitadas, estabelecendo que as comunicações para fins de marketing direto[66] apenas podem ser autorizadas em relação a destinatários que tenham dado o seu consentimento prévio.

---

[64] Carlos Ferreira de Almeida, *Contratos* I, cit., pp. 197 e ss.

[65] Para mais desenvolvimentos sobre este tema, cf. Paulo Mota Pinto, *Declaração tácita e comportamento concludente no negócio jurídico*, cit., pp. 18 e ss.

[66] Para mais desenvolvimentos, cf. Pedro Miguel Asensio, *Derecho Privado de Internet*, cit. pp. 299-308.

Assim, o sistema que está consagrado na DCE inspirou-se diretamente na DEP. Esta, por sua vez, refere que "(...) o consentimento por parte do utilizador ou assinante, independentemente de este ser uma pessoa singular ou colectiva, deve ter a mesma acepção que o consentimento da pessoa a quem os dados dizem respeito conforme definido e especificado na Directiva 95/46/CE. O consentimento do utilizador pode ser dado por qualquer forma adequada que permita obter uma indicação comunicada de livre vontade, específica e informada sobre os seus desejos, incluindo por via informática ao visitar um sítio na *internet*".

Como já referido na parte introdutória do nosso estudo, a DEP encontra-se, atualmente, desatualizada na parte do consentimento, face à entrada do RGPD. Contudo, o EDPB, o GT29 e as autoridades de controlo nacionais dos EM já se pronunciaram sobre se se deve entender que a remissão da DEP para os requisitos do consentimento deve ser entendida à luz dos atuais requisitos (mais exigentes) do RGPD.

Por conseguinte, coloca-se a questão adicional de saber se o consentimento dado no âmbito das comunicações comerciais e de celebração de contratos de adesão com recurso a cláusulas contratuais gerais cumpre os requisitos do RGPD.

Ora, o consentimento, ao abrigo do RGPD, deve ser livre, na medida em que, como já explicámos, pressupõe uma escolha genuína pela pessoa e respetivo controlo sobre como terceiros utilizam e tratam os seus dados. Se o indivíduo não tiver uma escolha real, o consentimento não é dado livremente e será inválido. Isto significa que as pessoas devem poder recusar o consentimento sem qualquer prejuízo, e devem poder retirá-lo facilmente a qualquer momento. Além disso, o consentimento não deve ser agrupado como uma condição à prestação de um serviço, exceto se for necessário para esse serviço.

Contudo, o RGPD indica, no Considerando 42 que "(...) 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 (...)".

Por sua vez, o EDPB esclarece[67] que "[e]m conformidade com as suas obrigações de transparência, os responsáveis pelo tratamento deverão evitar qualquer confusão quanto ao fundamento jurídico aplicável. Isto é particularmente relevante quando o fundamento jurídico adequado é o artigo 6.º, n.º 1, alínea b), e os titulares dos dados celebram um contrato relativo a serviços em linha. Consoante as circunstâncias, os titulares dos dados podem ter a impressão errada de que estão a dar o seu con-

[67] Na Orientação do EDPB n.º 2/2019 sobre o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha aos titulares dos dados, de 16 de outubro de 2019 – disponível *online* em www.edpb.europa.eu.

sentimento nos termos do artigo 6.º, n.º 1, alínea a), ao assinarem um contrato ou ao aceitarem as condições de serviço".

Assim, para que o consentimento seja válido, ao abrigo de contratos de consumo na *Internet*, cláusulas contratuais gerais ou publicidade, e sem prejuízo de se discutir se estamos perante um verdadeiro negócio jurídico, devem cumprir-se os deveres de informação exigidos no RGPD, em consonância com as disposições específicas das demais legislações aplicáveis, nomeadamente os artigos 5º e 6º da LCCG que obriga a um *dever de informação qualificado*[68].

Portanto, no âmbito das cláusulas contratuais gerais, exige-se, essencialmente, um consentimento informado do consumidor, ainda que, a nosso ver, seja menos exigente que noutras situações previstas no RGPD, como, *v.g.*, no caso da transferência de dados para países terceiros ou no caso do consentimento das crianças.

Ou seja, ao passo que a transferência de dados para países terceiros, por exemplo, exige um consentimento explícito e mais rigoroso, no âmbito das cláusulas contratuais gerais, o consentimento, regra geral, já se encontra pré-formulado pelo responsável pelo tratamento de dados, bastando ao titular "aderir" a um formulário pré-definido que servirá, ao abrigo do RGPD, como consentimento lícito.

Esta maior "flexibilidade" justifica-se, a nosso ver, como uma forma de adequar os requisitos do consentimento e proteção do titular de dados ao comércio eletrónico que se pretende rápido e eficaz, sem prejudicar a tutela do consumidor e a proteção dos dados pessoais.

Sem prejuízo do exposto *supra*, poderia equacionar-se se, porventura, o regime previsto na LCCG já acautela algumas das preocupações do RGPD ao nível do consentimento, em particular no artigo 19º referente às cláusulas proibidas.

Ora, o artigo 19º da LCCG consagra um elenco meramente exemplificativo de cláusulas relativamente proibidas no âmbito das relações entre empresários e entidades equiparadas, bem como entre aqueles e os consumidores (cf. artigo 20.º da LCCG), podendo ser aumentado sempre que se verificar uma ofensa ao princípio da boa-fé.

A proibição de utilização destas cláusulas pressupõe um juízo valorativo associado ao tipo de contrato em causa ou ao "quadro negocial padronizado"[69].

---

[68] O artigo 5º da LCCG começa por reafirmar a obrigação de comunicação que já decorre do artigo 227.º do CC. Para mais desenvolvimentos sobre o dever de informação no âmbito da LCCG, cf. Ana Prata, *Contratos de Adesão e Cláusulas Contratuais Gerais*, Almedina, 2.ª edição, Coimbra, 2021, pp. 278-287.

[69] Ana Filipa Morais Antunes, *Comentário à Lei das Cláusulas Contratuais Gerais*, Coimbra Editora, 1ª edição, Coimbra, 2013, p. 295.

Com efeito, consideramos que a própria LCCG já acautela algumas preocupações do RGPD, nomeadamente ao impor certas restrições, tais como, quando estejamos perante cláusulas que consagrem "ficções de receção, de aceitação ou de outras manifestações da vontade com base em factos insuficientes" (cf. artigo 19.º, alínea d), da LCCG)[70]. Esta previsão tem de ser, necessariamente, articulada com os artigos 217º e 218º do CC, o que indica que esta proibição permite justificar a inadmissibilidade de cláusulas que imponham unilateralmente a relevância do silêncio como manifestação da vontade, o que, igualmente, é proibido à luz da interpretação das características típicas do consentimento à luz do RGPD.

Adicionalmente, importa proceder a uma breve nota a propósito do artigo 23º da LCCG, que corresponde a uma norma autolimitada[71] ou internacionalmente imperativa. Tal preceito consagra a aplicação imperativa das normas da LCCG sobre cláusulas contratuais gerais proibidas, independentemente da lei escolhida pelas partes para regular o contrato, "sempre que o mesmo apresente uma conexão estreita com o território português". Ou seja, a validade do consentimento no âmbito dos contratos de adesão terá de ser, necessariamente, analisada à luz do disposto na LCCG, a qual, em conjugação com o disposto no artigo 9.º do Regulamento Roma I[72], poderá impor a sua aplicação territorialmente.

3.3 *Cookies* e outras tecnologias de rastreio

Para análise do problema do consentimento no âmbito dos *cookies*, cumpre esclarecer que, segundo a DEP, *cookies* são entendidos como testemunhos de conexão (cf. Considerando 25). Contudo, na prática, as autoridades de controlo têm avançado com definições mais concretas de *cookies* como pequenos ficheiros de dados enviados para o computador ou telemóvel de um utilizador a partir de um *site* e que são armazenados no disco rígido do dispositivo do utilizador.

Além disso, os *cookies* não se verificam apenas na página inicialmente visitada pelo *user*, mas em todas as páginas que o *user* queira visitar em determinado *site*. Assim, os *cookies* são geralmente classificados, pelas autoridades de controlo e pelos responsáveis pelo tratamento de dados, de acordo com as seguintes características: (i) período de duração, (ii) proveniência, bem como (iii) finalidade.

---

[70] Ana Prata, *Contratos de Adesão e Cláusulas Contratuais Gerais*, cit. pp. 443 e ss.

[71] Luís de Lima Pinheiro, *Direito Internacional Privado*, vol I, AAFDL Editora, Lisboa, 2019, pp. 270 e ss.

[72] Regulamento (CE) n.º 593/2008, do Parlamento Europeu e do Conselho, de 17 de Junho de 2008, sobre a lei aplicável às obrigações contratuais.

De facto, o tratamento dos *cookies* analíticos são os mais controversos, pois podem partir de um operador ou terceiro que esteja ou não vinculado por acordo com o operador e que, consequentemente, podem (ou não) estar sujeitos a consentimento nos termos do RGPD[73].

Além disso, coloca-se questões quanto aos *cookies* de publicidade, sendo que, regra geral, estão sujeitos a consentimento nos termos do RGPD. Contudo, são o tipo de *cookies* que, historicamente, têm suscitado mais preocupações por parte do GT29 e autoridades de controlo, na medida em que podem ser *pop-ups*, como veremos.

3.3.1 Disposições legais aplicáveis

Quanto às disposições aplicáveis, além do RGPD, referimos a DEP, bem como, no plano nacional, o Decreto-Lei n.º 7/2004, de 7 de janeiro, que transpôs a DCE para a ordem jurídica interna, e ainda a Lei n.º 41/2004, de 18 de agosto, referente à proteção de dados pessoais e privacidade nas telecomunicações.

No âmbito do RGPD, o artigo 95.º não impõe obrigações suplementares face às que decorrem da DEP (artigo 13º). O que é que isso significa? Segundo o EDPB, na sua *Opinion 5/2019*[74], é referido que: *(i)* os artigos 5.º, n.º 3, e 13.º da DEP se aplicam a prestadores de serviços de comunicações eletrónicas, assim como a operadores de *websites* (*v.g.*, no âmbito dos *cookies* ou testemunhos de conexão); (ii) é possível que o mesmo tratamento de dados se integre tanto no âmbito de aplicação da DEP, como do RGPD[75]; e que (iii) a DEP é *lex specialis* face ao RGPD – entendimento que já foi reforçado pelo EDPB nas suas *Guidelines 05/20 on consent*.

Contudo, quanto ao *tratamento subsequente* dessa informação, terá de se verificar um fundamento de licitude do artigo 6.º (e, possivelmente, do artigo 9.º) do RGPD, como *v.g.*, o consentimento. Portanto, as regras do RGPD e da DEP devem ser aplicadas em consonância. Contudo, dado que a DEP é *lex specialis,* a recolha de informação dos computadores está prevista no âmbito do seu artigo 5.º, n.º 3.

---

[73] Problema idêntico já se tinha colocado a propósito da identificação dos *users* através do endereço IP ou até do acesso via *login* e nome de domínio do *user*. Para mais desenvolvimentos, cf. Pedro Miguel Asensio, *Derecho Privado de Internet*, cit., pp. 294-296.

[74] Opinion 5/2019, on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities" – disponível *online* em www.edpb.europa.eu/.

[75] Cf. Acórdão *Wirtschaftsakademie Schleswig-Holsteine* (Processo C-210/16 de 5 de junho de 2018) e Acórdão *Fashion ID* (Processo C-40/17 de 29 de julho de 2019) ambos do TJUE, bem como o Considerando 30 do RGPD.

Mais, se a DEP é *lex specialis*, nos casos em que dispõe que é necessário o consentimento, não podemos, no nosso entender, recorrer a outros fundamentos de licitude. O legislador pretendeu limitar o fundamento de licitude dos *cookies* ao consentimento, o que não prejudica, porém, que os tratamentos posteriores possam ser baseados noutros fundamentos ao abrigo do RGPD.

Nestes casos, devemos recorrer ao artigo 6.º, n.º 4 do RGPD, para se efetuar o denominado *teste de compatibilidade*. Por um lado, as regras aplicáveis aos *cookies* aplicam-se independentemente de as informações recolhidas serem ou não dados pessoais, pois o que está em causa é a tutela da privacidade. Por outro lado, nos casos em que se recolhe dados pessoais, não há dúvida de que estão sujeitos a consentimento, exceto se caírem no âmbito do regime de isenção (ou seja, têm de ser absolutamente necessários)[76].

Ainda, se não se recolhem dados pessoais, em princípio o RGPD não tem aplicação. No entanto, recolhendo ou não dados pessoais, e aplicando-se as regras acima descritas, o consentimento tem de ser obtido através de uma aplicação analógica do RGPD. Este ponto é, contudo, controverso, mas entende-se que a posição mais cautelosa é a de que o consentimento deverá ser obtido nos termos melhor definidos no artigo 4.º, n.º 11, do RGPD.

Já ao abrigo da lei nacional, a regra é a de que é sempre necessário *consentimento prévio* e que este consentimento preencha os critérios da lei, ou seja, os requisitos de validade previstos no RGPD. Contudo, a lei nacional não esclarece sobre a que *cookies* é que se exige consentimento prévio, nem a CNPD dá resposta a esta questão.

3.3.2 Orientações do GTA29: o Parecer 4/2012

O GT29, no seu Parecer 4/2012[77], identifica exemplos de *cookies* que não carecem da obtenção do consentimento, tais como: (i) *cookies* alimentados pelo utilizador (identificador de sessão) para a duração de uma sessão ou *cookies* persistentes

---

[76] O EDPB observa também que, em conformidade com os requisitos de privacidade eletrónica e com o atual parecer do GT29 sobre publicidade comportamental (Parecer 2/2010 do GT29 sobre a publicidade comportamental em linha (WP171)), bem como com o Documento de Trabalho 02/2013 que fornece orientações sobre a obtenção de consentimento para os *cookies* (Documento de Trabalho 02/2013 do GT29 que fornece orientações sobre a obtenção do consentimento para os *cookies* (WP208)), os responsáveis pelo tratamento devem obter o consentimento prévio dos titulares dos dados para colocar os *cookies* necessários para a realização de publicidade comportamental.

[77] Parecer 4/2012 sobre a isenção de consentimento para a utilização de testemunhos de conexão, disponível *online* em www.ec.europa.eu.

limitados a algumas horas em certos casos; (ii) *cookies* de autenticação, utilizados para prestar serviços autenticados, para a duração de uma sessão; (iii) *cookies* de segurança centrados no utilizador, utilizador para detetar abusos de autenticação, para uma duração limitada e persistente; (iv) *cookies* de sessão criados por um leitor multimédia, designadamente os *cookies* de leitor *flash*, para a duração de uma sessão; (v) *cookies* de sessão para equilibrar a carga para a duração de uma sessão; (vi) *cookies* persistentes de personalização da interface do utilizador para a duração de uma sessão (ou ligeiramente mais); e (vii) *cookies* de terceiros para partilha de conteúdos para os membros ligados a uma rede social.

O GT29 entende, ainda, que, para os *cookies* estarem dentro do âmbito da isenção, têm de ser *absolutamente necessários*, pelo que a finalidade de melhorar o *site* não é um fundamento e é preciso, por exemplo, que o *site* não consiga funcionar sem os *cookies*. Deste modo, são muito residuais os casos em que *cookies* possam beneficiar desta isenção.

Neste sentido, se um *cookie* tiver mais do que uma finalidade, ou estão todos isentos ou o consentimento é necessário para todos.

3.3.3 Soluções jurisprudenciais: Casos *Fashion ID* e *Planet 49*

O TJUE, por sua vez, pronunciou-se sobre a temática do consentimento no âmbito dos *cookies* em dois acórdãos: Acórdão *Fashion ID*[78] e Acórdão *Planet 49*[79].

No Acórdão *Fashion ID*, o TJUE entendeu que o facto de haver um "botão *like*" no *site* de vestuário de moda (*Fashion ID*), permitindo ao Facebook "instalar" essa tecnologia, torna tanto o gestor do *site*, como o Facebook, responsáveis conjuntos por essa atividade em particular.

Para tal, entendeu o TJUE que não é necessário alguém clicar no botão, bastando aceder ao *site*. A partir do momento em que comunicam os dados, o Facebook já é responsável autónomo. Entendeu-se, ainda, que houve violação de dados pessoais, na medida em que o consentimento para o tratamento de dados deve ser obtido pelo administrador unicamente no que diz respeito à operação ou ao conjunto de operações de tratamento de dados pessoais cujas finalidades e meios são efetivamente determinados por esse administrador.

Ora, este acórdão não versa especificamente sobre *cookies*, mas mostra que o simples facto de haver um "botão de *like*" ou de partilha é o suficiente para que,

[78] Acórdão *Fashion ID* (Processo C-40/17 de 29 de julho de 2019).
[79] Acórdão *Planet 49* (Processo C-673/17 de 1 de outubro de 2019).

verificadas certas condições, as duas partes sejam consideradas responsáveis conjuntos pelo tratamento de dados.

Já no Acórdão *Planet 49* discute-se se a utilização de uma *pre-ticked box* é compatível com o consentimento nos termos dos artigos 5.º, n.º 3 e 2.º, alínea f) da DEP, em conjugação com o artigo 2.º, alínea h) da DPD e artigo 6.º, n.º 1 do RGPD, nos casos em que o consentimento do *user* era presumido, exceto se este, proactivamente, retirasse esse consentimento ao desmarcar a *checkbox*. Para o Advogado-Geral Szpunar, a resposta foi que não existia um consentimento válido[80], porquanto o consentimento para o armazenamento e utilização de *cookies* tem de ser específico e, como tal, não é compatível com seleções mediante *pre-ticked box*, ou seja, através de caixas ou opções pré-selecionadas.

Além disso, o entendimento de que "se continuar a navegar no site, está a concordar" não é uma opção válida, pelo que o "consentimento" obtido por utilizadores que continuam a navegar no *website*, não cumpre os requisitos elencados no RGPD[81].

Informação relativa à periodicidade dos *cookies*, assim como a partilha de informação com terceiros, deve ser prestada ao utilizador no momento de recolha do consentimento e prestadores de serviços devem indicar a duração dos *cookies* e a possibilidade de terceiros acederem aos mesmos. Estas regras são transversais a todos os *cookies*, independentemente de recolherem dados pessoais ou não.

3.3.4 Soluções das autoridades de controlo (ICO, CNIL, AEPD, CNPD)

No que concerne às autoridades de controlo, e ainda que as suas *guidelines* sejam instrumentos de *soft law*, têm sido essenciais para melhor interpretar o RGPD e guiar o intérprete-aplicador nacional no cumprimento da legislação supranacional. Contudo, e no que concerne aos *cookies*, em particular, as autoridades de controlo europeias nem sempre estão de acordo.

---

[80] Considerou-se que, nestes casos, "é praticamente impossível determinar objetivamente se um utilizador deu o seu consentimento com base numa decisão livre e informada", acrescentando-se ainda que "(des)marcar a opção relativa aos *cookies* configura um ato preparatório do ato final e juridicamente vinculativo de «acionar» o botão de participação. O utilizador não está, nesta situação, em condições de dar o seu consentimento de forma livre e em separado para o armazenamento ou a possibilidade de acesso a informações já armazenadas no seu equipamento terminal" – cf. Conclusões do Advogado-Geral Spzunar, de 21 de março de 2019, pp. 88-90.

[81] Ao contrário do anteriormente defendido pela autoridade de controlo espanhola AEPD no seu guião de *cookies* de novembro de 2019 e que, entretanto, foi alterado em julho de 2020, no seguimento das Orientações do EDPB sobre consentimento datado de 4 de maio de 2020, disponível *online* em www.edpb.europa.eu.

A autoridade de controlo francesa CNIL reviu, recentemente, as suas posições quanto aos *cookies*. Ora, quanto aos *cookies* analíticos necessitarem de consentimento, a CNIL entende agora que nem sempre. De facto, a autoridade de controlo francesa anteriormente (i) exigia o consentimento para os *cookies* analíticos e (ii) por derrogação tinha previsto um regime de *opt out* para certos tipos de *cookies* analíticos se as condições cumulativas fossem cumpridas. Contudo, ao abrigo das novas regras de outubro de 2020, a CNIL passou a (i) exigir o consentimento para os *cookies* analíticos e (ii) por derrogação, passou a aceitar que certos tipos de *cookies* analíticos possam ser considerados "estritamente necessários" (para o qual não é necessário prever um *opt-out*), se cumulativamente as condições eram cumpridas (por exemplo, tempo de vida de *cookies* analíticos não deve exceder 13 meses, etc.).

Esta abordagem da CNIL parece antecipar uma possível isenção dos *cookies* analíticos, sugerido em rascunhos da proposta de Regulamento *E-Privacy*, ao contrário do que antes defendia e que comprovava a sua natureza conservadora, porque admitiam que os *cookies* analíticos poderiam cair numa das isenções para efeitos do artigo 5.º, n.º 3 da DEP, se se garantisse que a intrusão na esfera privada fosse reduzida, designadamente: nas estatísticas de *performance*, nos *cookies* que tivessem sido implementados pelo operador do *site* ou por entidade subcontratada, ou ainda nos casos em que os *cookies* não permitissem que o *user* navegasse por várias páginas, que a duração não excedesse sete meses e nunca permitisse a entidade que o colocasse identificasse mais do que a cidade do *user*[82].

A CNIL reviu, igualmente, a sua posição sobre as *cookie walls* após a anulação parcial das suas diretrizes de julho de 2019 pelo mais alto tribunal administrativo francês (*i.e*, *Conseil d'Etat*) em junho de 2020. As diretrizes revistas de outubro de 2020 já não preveem uma proibição geral das *cookie walls*. Em vez disso, a CNIL observa que é pouco provável que as *cookie walls* cumpram o limiar de consentimento válido ao abrigo do RGPD. No entanto, tais *cookie walls* devem ser revistas e analisadas numa base casuística. Se estiver em causa um endereço de *IP* estático, seria demasiado intrusivo, mas se for dinâmico depende do esforço que o operador tenha de fazer para a descoberta da identificação.

Já a autoridade de controlo espanhola AEPD, numa primeira fase, defendia a regra das "duas camadas informativas", *i.e.*, que, numa primeira camada estaria

[82] A 7 de dezembro de 2020, a CNIL sancionou a empresa *Amazon Europe Core* com uma multa de 35 milhões de euros por ter colocado *cookies* de publicidade nos computadores dos utilizadores do *website* amazon.fr sem consentimento prévio e sem informação satisfatória. Para mais informações, vide a Declaração da CNIL, disponível *online* em www.cnil.fr.

disponível informação mais premente (*v.g.* finalidades, tipos de dados, painel de configuração), enquanto, numa segunda camada, estaria disponível informação mais detalhada (*v.g.* entidades que utilizam os *cookies,* prazo de conservação, transferências internacionais, lógica da perfilagem). Nessa primeira fase, a AEPD admitia a continuação da navegação no *site* como prestação de consentimento inequívoco, ao contrário do entendimento de consentimento do RGPD e do Acórdão *Planet 49*.

Esta posição bastante liberal – pois admitia que, caso o *user* continuasse a navegar num *site*, ignorando o *banner*, estaríamos perante consentimento válido – foi, entretanto, abandonada. Ora, o EDPB, em maio de 2020, emitiu as suas orientações sobre o consentimento e referiu, expressamente, que o facto de um utilizador continuar a navegar num determinado *site* não constitui, em nenhuma circunstância, consentimento[83]. Este entendimento obrigou a autoridade de controlo espanhola a atualizar o seu guião sobre a utilização de *cookies*, retratando-se do seu entendimento inicial[84] sobre as duas camadas informativas e a possibilidade de consentimento pela continuação de navegação no *site*.

A autoridade de controlo inglesa, ICO, por sua vez, defende que os *cookies* analíticos carecem sempre do consentimento do utilizador. Esclarecem que o consentimento é a única fonte de licitude para o tratamento de dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos. A ICO apenas admite que o operador do *site* trate para outras finalidades quando exista consentimento, no entanto a autoridade de controlo francesa admite que existam outros fundamentos para tratar, tal como interesses legítimos.

Por fim, a autoridade de controlo nacional CNPD não se pronunciou sobre estas divergências, sendo que entendemos que, à luz da legislação nacional, e como referido, prevalece o entendimento que é sempre necessário requerer consentimento para *cookies*, articulando-se a *ratio* da DEP, RGPD e leis nacionais.

---

[83] Cf. EDPB "Guidelines on Consent", p. 19, onde refere que: "actions such as scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action: such actions may be difficult to distinguish from other activity or interaction by a user and therefore determining that an unambiguous consent has been obtained will also not be possible. Furthermore, in such a case, it will be difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it.".

[84] No guião de *cookies* na versão de julho de 2020, posteriormente atualizada em janeiro de 2021, disponíveis online em www.aepd.es.

3.4 Categorias especiais de dados

3.4.1 Distinção entre dados genéticos, dados biométricos e dados relativos à saúde

Outro desafio que a *Internet* coloca aos titulares de dados verifica-se no contexto do consentimento em temas relacionados com categorias especiais de dados, em particular os dados de saúde. Nos termos do artigo 4º, números 13, 14 e 15, e do artigo 9º do RGPD, podemos distinguir entre dados genéticos, dados biométricos e dados relativos à saúde[85].

Note-se que, ainda que se trate de dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados, caso seja possível serem utilizados para re-identificar uma pessoa, continuam a ser dados pessoais e, portanto, são abrangidos pelo âmbito de aplicação do RGPD. No entanto, excluem-se da sua aplicação os dados que tenham sido tornados anónimos de modo que a pessoa não seja ou deixe de ser identificável – pelo que tais dados deixam de ser considerados dados pessoais (ainda que seja necessário, contudo, que a anonimização seja irreversível) –, assim como os dados de pessoas falecidas, de acordo com o Considerando 27, sendo que este remete para os EM o estabelecimento das "regras para o tratamento dos dados pessoais de pessoas falecidas". Quanto a nós, entendemos que deverão ser adotadas, nesta matéria, as medidas previstas na LEN, no seu artigo 17º.

De acordo com o artigo 9.º, n.º 1, do RGPD, a regra é da proibição do tratamento deste tipo de dados para identificar uma pessoa de forma inequívoca. Contudo, existem exceções à regra, sendo uma delas o consentimento.

Assim, de acordo com o artigo 9.º, n.º 2, alínea a) do RGPD: "Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados

---

[85] O conceito de «dados de saúde», ao contrário dos dados genéticos e biométricos, encontrava-se já prevista no artigo 8.º, n.º 1, da DPD, apesar de tal preceito não apresentar nenhuma definição. No âmbito da jurisprudência europeia, o TJUE adotou uma interpretação ampla do conceito de dados de saúde, nos termos da DPD. No Caso *Lindqvist* (Processo C-101/01), o TJUE decidiu que o conceito de dados de saúde inclui informação relativa a todos os aspetos da saúde do titular de dados, quer a nível de saúde física, quer a nível de saúde mental. Adicionalmente, o TJUE considerou que o conceito de dados pessoais devia ser entendido em sentido amplo, na medida em que abrangia dados que fossem incluídos numa página da *Internet* e a sua difusão através desses meios (como a inserção de palavras-chave ou *metatags* ou através das redes sociais). Para mais desenvolvimentos, cf. Pedro Miguel Asensio, *Derecho Privado de Internet*, cit., pp. 309 e ss. No mesmo sentido, o TJUE pronunciou-se no Caso T-343/13, *CN v European Parliament*, de 3 de dezembro de 2015.

pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.º 1 não pode ser anulada pelo titular dos dados".

Além disso, e de modo a reforçar essa tutela especial, o artigo 9.º, n.º 4, do RGPD, enquanto cláusula aberta, permite que os EM possam manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde. Deste modo, a LEN, no seu artigo 29.º, exige a concretização do *princípio da necessidade*[86] de conhecer a informação para efeitos de tratamento de dados genéticos, biométricos e relativos à saúde. Além disso, exige que o tratamento de dados seja feito, em exclusivo (i) por profissionais de saúde (ii) sujeitos a sigilo profissional e (iii) através de forma eletrónica, não admitindo a sua publicação ou divulgação.

De facto, para efeito de tratamento desta categoria especial de dados, exige-se um *consentimento explícito e informado* do titular de dados. No entanto, existem especificidades atendendo ao contexto em que esses dados especiais são tratados, como veremos de seguida.

3.4.2 A questão do consentimento para tratamento de dados no âmbito da investigação científica e dos ensaios clínicos

No âmbito da investigação científica[87] existem problemas concretos relacionados com o tema dos ensaios clínicos.

---

[86] Também o princípio da finalidade se afigura relevante nesta sede, nomeadamente como forma de proteção dos direitos humanos do titular de dados. A esse propósito, cf. o Acórdão do TEDH de 27 de agosto de 1997, *M.S. vs Suède* sobre o tratamento de dados médicos de uma paciente sem o seu consentimento. Para mais desenvolvimentos, cf. Cecile de Terwagne, "*Internet* et la Protection de La Vie Privée et des données à caractère personnel", cit. pp. 345-347.

[87] O artigo 4.º do RGPD não inclui uma definição explícita da expressão "tratamento para efeitos de investigação científica". Como indicado no Considerando 159, "o tratamento de dados pessoais para fins de investigação científica deverá ser entendido em sentido lato, abrangendo, por exemplo, o desenvolvimento tecnológico e a demonstração, a investigação fundamental, a investigação aplicada e a investigação financiada pelo setor privado. Deverá, além disso, ter em conta o objetivo da União mencionado no artigo 179.º, n.º 1, do TFUE, que consiste na realização de um espaço europeu de investigação. Os fins de investigação científica deverão também incluir os estudos de interesse público realizados no domínio da saúde pública". De notar, aliás, que o GT29 já tinha salientado que a noção de investigação científica não se pode estender para além do seu significado comum e entendia que "investigação científica" neste contexto significa "um projeto de investigação criado de acordo com as normas metodológicas e éticas aplicáveis em cada setor, em conformidade com as boas práticas" – cf. Orientações relativas ao consentimento na aceção do Regulamento 2016/679 do GT29 de 10.04.2018, WP259 rev.01, 17PT, p. 27 (aprovadas pelo EDPB).

Qualquer tratamento de dados pessoais de saúde deve respeitar os princípios relativos ao tratamento estabelecidos no artigo 5.º do RGPD e estar abrangido por uma das bases jurídicas e derrogações específicas enumeradas, respetivamente, no artigo 6.º e no artigo 9.º do RGPD, para efeitos do tratamento lícito desta categoria especial de dados pessoais[88].

O consentimento do titular dos dados, recolhido nos termos do artigo 6.º, n.º 1, alínea a), e do artigo 9.º, n.º 2, alínea a), do RGPD, poderá constituir a base jurídica para o tratamento de dados relativos à saúde. O RGPD exige, porém, para o tratamento de dados especiais, incluindo dados de saúde para investigação científica[89], um *consentimento explícito*, nomeadamente as estabelecidas no artigo 4.º, n.º 11, no artigo 6.º, n.º 1, alínea a), no artigo 7.º e no artigo 9.º, n.º 2, alínea a), do RGPD. Designadamente, o consentimento deve corresponder a uma manifestação de vontade livre, específica, informada e explícita e deve ser dado mediante declaração ou "ato positivo inequívoco"[90].

Mais recentemente, o EDPB publicou as suas respostas ao pedido de esclarecimentos da COM a propósito do tratamento de dados pessoais no contexto dos ensaios clínicos. Nesses esclarecimentos, e no que concerne ao consentimento em particular, o EDPB afirma que, tendo em conta que as declarações éticas e as

---

[88] Cf. Acórdão do TJUE *Google Spain*, de 13 de maio de 2014, processo C-131/12, n.º 71.

[89] Note-se que quando se fala de "tratamento de dados de saúde para efeitos de investigação científica", existem dois tipos de utilizações de dados: (i) investigação sobre dados pessoais (de saúde) que consiste na utilização de dados recolhidos diretamente para fins de estudos científicos ("utilização primária") e (ii) investigação sobre dados pessoais (de saúde) que consiste no tratamento posterior de dados recolhidos inicialmente para outro fim ("utilização secundária"). Esta distinção entre investigação científica baseada na utilização primária ou secundária de dados de saúde é particularmente importante quando se discute a base jurídica para os tratamentos, as obrigações de informação e o princípio da limitação das finalidades – cf. artigo 5.º, n.º 1, alínea b), do RGPD.

[90] Tal como referido no Considerando 43 do RGPD, o consentimento não pode ser considerado livre se existir um desequilíbrio manifesto entre o titular dos dados e o responsável pelo tratamento. Por conseguinte, é importante que o titular dos dados não seja pressionado e que não seja penalizado se decidir não dar o seu consentimento. O EDPB já abordou a questão do consentimento no contexto dos ensaios clínicos – cf. Parecer 3/2019, de 23.1.2019, relativo às Perguntas e Respostas sobre a relação entre o Regulamento Ensaios Clínicos (CTR) e o Regulamento Geral sobre a Proteção de Dados (RGPD). No âmbito do tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19, em particular, o EDPB emitiu a Orientação do EDPB n.º 03/2020, de 21 de abril de 2020, na qual assinala a importância de os titulares dos dados não se encontrarem numa situação de qualquer dependência relativamente aos investigadores que seja suscetível de influenciar indevidamente o exercício da sua livre vontade. Os investigadores devem estar ainda cientes de que, caso o consentimento seja utilizado como base jurídica para o tratamento, o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento, nos termos do artigo 7.º, n.º 3, do RGPD.

convenções de bioética visam, principalmente, proteger os indivíduos contra serem incluídos em projetos de investigação médica contra a sua vontade e/ou sem o seu conhecimento, isso significa que o consentimento informado para participar no projeto de investigação médica é um requisito necessário, salvo algumas exceções para situações em que o consentimento não pode ser dado – *v.g.,* indivíduos incapacitados, situações de emergência, entre outras. Contudo, tal consentimento pode e deve ser distinguido do consentimento como uma base jurídica para o tratamento de dados pessoais, nos termos do artigo 6.º, n.º 1, alínea a) do RGPD[91].

Ademais, e tendo em consideração que o artigo 6.º, n.º 1 do RGPD prevê outros fundamentos jurídicos além do consentimento e o artigo 9.º, n.º 2, prevê isenções para além do consentimento explícito, o EDPB defende que é previsível e não incompatível (com as normas éticas) que outros fundamentos jurídicos possam ser invocados para fins de processamento de dados de saúde para investigação científica.

No entanto, ao basear-se noutro fundamento jurídico previsto no artigo 6.º, para além do consentimento, e numa das outras isenções do artigo 9.º, n.º 2 do RGPD, o requisito "ético" do consentimento informado para a participação no projeto de investigação médica terá ainda de ser cumprido. No quadro do RGPD, isto pode ser visto como uma das salvaguardas adicionais previstas no artigo 89.º, n.º 1 do RGPD, que devem estar em vigor aquando do tratamento de dados pessoais para fins de investigação científica.

Ainda, no caso dos ensaios clínicos, em particular, entendemos relevante que a análise do RGPD seja feita em conjunto com o novo Regulamento de Ensaios Clínicos[92], que substitui a Diretiva 2001/20/CE, relativa aos ensaios clínicos.

Este Regulamento promoveu a criação e manutenção de uma base de dados europeia, acessível através de um portal da UE, sobre informação dos ensaios clínicos realizados na UE. Essa base de dados da UE deverá conter: (i) todas as informações pertinentes para o ensaio clínico; (ii) deverá ser acessível ao público; (iii) e os dados nela contidos apresentados num formato facilmente acessível. Na base de dados da UE não deverão ser registados dados pessoais dos sujeitos que

---

[91] Cf. EDPB "Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research", de 2 de fevereiro de 2021.
[92] Regulamento (UE) n.º 536/2014, o qual entrou em aplicação a 31 de janeiro de 2022, mas prevê um período de transição para o Sistema de Informação de Ensaios Clínicos ("CTIS") de três anos. Assim, de 31 de janeiro de 2022 a 31 de janeiro de 2023, os promotores de ensaios clínicos podem optar por submeter os seus pedidos de ensaios clínicos ao abrigo da Diretiva dos ensaios clínicos (Diretiva 2001/20/CE), através da submissão de processos a nível nacional, ou ao abrigo do Regulamento dos Ensaios Clínicos, através do CTIS.

participem em ensaios clínicos. As informações da base de dados da UE deverão ser públicas, salvo se, por razões específicas, uma determinada informação não deva ser publicada, a fim de proteger o direito das pessoas à vida privada e o direito à proteção dos dados pessoais, reconhecidos nos artigos 7º e 8º da CDFUE, bem como no RGPD.

Tratando-se de informação que vai ser disponibilizada em plataformas digitais[93], coloca-se a questão de analisar como vai ser regulado o consentimento dos pacientes/participantes, enquanto titulares dos dados médicos que constarão dessa plataforma digital pública.

Conforme referido, o RGPD, no seu artigo 9.º, considera os dados médicos dados especiais e que, por isso, merecem uma tutela mais protetora, exigindo, para o seu tratamento, um *consentimento explícito*.

Já o Regulamento de Ensaios Clínicos, a nosso ver, vai mais longe, ao prever nos seus artigos 28º a 35º, a obrigação de se obter um consentimento informado para efeito de promoção de ensaios clínicos. Este consentimento informado obriga a requisitos específicos consoante a situação concreta do titular dos dados em causa, *i.e.*, se se trata de uma pessoa singular plenamente capaz ou não, se estamos perante grávida ou pessoa lactante, entre outros.

Assim, o consentimento informado, para efeitos do artigo 2.º, n.º 2, alínea 21), do Regulamento de Ensaios Clínicos, afigura-se como "a expressão livre e voluntária por parte de um sujeito do ensaio da sua vontade de participar num ensaio clínico específico, depois de ter sido informado de todos os aspetos do

---

[93] No âmbito das plataformas digitais, é de assinalar que, a 15 de dezembro de 2020, a COM lançou duas novas propostas para o Regulamento sobre Serviços Digitais (*Digital Services Act*) e o Regulamento dos Mercados Digitais (*Digital Markets Act*). Este pacote legislativo constitui uma reforma ambiciosa da regulação sobre o ecossistema digital, que visa aumentar a segurança e a proteção dos direitos fundamentais neste espaço, bem como fomentar a concorrência e a inovação. Como novas medidas em matéria de privacidade e proteção de dados, destacam-se, a título exemplificativo: (i) obrigação de prestar informação aos utilizadores sobre as restrições à utilização dos dados fornecidos (v.*g.,* mecanismos de moderação de conteúdos ou algoritmos utilizados para tomar decisões); (ii) transparência quanto aos algoritmos utilizados para ordenar os conteúdos de plataformas *online* muito amplas; (iii) permitir ao utilizador desativar o uso de perfis, entre outras. Mais recentemente, a 10 de fevereiro de 2021, o EDPS emitiu dois pareceres relativos às duas propostas mencionadas *supra*, nos quais reiterou a necessidade de os diplomas se conjugarem com o RGPD em matéria de *privacy by design*, definição de perfis e de gestão do consentimento dos utilizadores, devendo esta última ser efetuada mediante uma solução *user-friendly*. Neste sentido, e para um maior aprofundamento, cf. Opinion 1/2021 on the Proposal for a Digital Services Act e Opinion 2/2021 on the Proposal for a Digital Markets Act. Finalmente, a 23 de abril de 2022 obteve-se o acordo político provisório entre o Conselho e o Parlamento Europeu sobre o Regulamento Serviços Digitais.

ensaio clínico que sejam relevantes para a sua decisão de participar, ou, no caso de um menor ou de um sujeito incapaz, uma autorização ou a concordância do seu representante legalmente autorizado sobre a sua inclusão no ensaio clínico".

O artigo 28.º do Regulamento estabelece as regras gerais de obtenção do consentimento informado e como não deve ser exercida qualquer influência indevida; esclarece que o paciente tem direito de se retirar do estudo a qualquer momento e sem necessidade de qualquer justificação; e garante os deveres de informação exigíveis para obtenção do consentimento.

O artigo 29.º, por sua vez, define as condições específicas para o consentimento esclarecido e informado. O consentimento esclarecido e informado deve ser escrito e documentado – contrariamente ao RGPD, que não exige qualquer forma especial –, e o paciente deve receber uma cópia do documento ou registo. Além disso, o paciente deve ter tempo suficiente para considerar a decisão. O número 2 do referido preceito elenca quais as informações que devem ser prestadas e de que forma. Em concreto, a informação deve permitir à pessoa compreender, nomeadamente, a finalidade do ensaio, as implicações e riscos do ensaio, bem como os seus inconvenientes; as condições, duração e alternativas de tratamento, entre outras informações entendidas como essenciais ao abrigo do Regulamento.

Para o EDPB, o consentimento esclarecido previsto no Regulamento de Ensaios Clínicos não deve ser confundido com a noção de consentimento como fundamento jurídico para o tratamento de dados pessoais nos termos do RGPD[94].

As disposições do Capítulo V do Regulamento de Ensaios Clínicos sobre consentimento esclarecido, particularmente o artigo 28.º, dão resposta, sobretudo, aos principais requisitos éticos de projetos de investigação que envolvem seres humanos derivados da Declaração de Helsínquia[95]. A obrigação de obtenção do consentimento esclarecido dos participantes num ensaio clínico é principalmente

---

[94] O EDPB alerta, ainda, para se ter em consideração que, ainda que sejam reunidas as condições para um consentimento esclarecido em conformidade com o Regulamento de Ensaios Clínicos, poderá haver situações de desequilíbrio de poderes. Uma situação clara de desequilíbrio de poderes entre o participante e o promotor/investigador implica que o consentimento não é "livre" na aceção do RGPD – *v.g.*, quando um participante não se encontra em boas condições de saúde, ou quando os participantes pertencem a um grupo desfavorecido do ponto de vista económico ou social ou ainda quando estes se encontram em qualquer situação de dependência institucional ou hierárquica. Nesses casos, o consentimento não constitui um fundamento jurídico adequado – cf. "Parecer 3/2019 relativo às Perguntas e Respostas sobre a relação entre o Regulamento Ensaios Clínicos (CTR) e o Regulamento Geral sobre a Proteção de Dados (GDPR) (art. 70.º, n.º 1, alínea b))", pp. 6-7.

[95] Declaração de Helsínquia da Associação Médica Mundial que promove Princípios Éticos para a Investigação Médica em Seres Humanos, adotada em junho de 1964.

uma medida destinada a assegurar a proteção do direito à dignidade humana e o direito à integridade dos indivíduos nos termos dos artigos 1.º e 3.º da CDFUE, mas não é concebida como um instrumento para o cumprimento da proteção de dados.

Adicionalmente, o EDPB, no seu Parecer 3/2019 (sobre a interação entre o Regulamento dos Ensaios Clínicos e o RGPD), declarou que, para efeitos de proteção de dados, o consentimento não é uma base jurídica adequada na investigação de atividades onde existe um claro desequilíbrio de poder entre a pessoa em causa e o responsável pelo tratamento dos dados. E reconheceu que, nos ensaios clínicos, tal desequilíbrio pode existir, dependendo das circunstâncias, por exemplo, quando a pessoa em causa não se encontra em boas condições de saúde e não há disponibilidade terapêutica ou de tratamento fora do ensaio clínico[96].

Com efeito, no que concerne à relevante legislação da União, até agora, apenas o Regulamento de Ensaios Clínicos pode ser identificado como legislação da União na qual uma base jurídica uniforme para os controladores pode ser encontrada, nomeadamente a obrigação legal dos controladores (artigos 41.º e 43 do Regulamento) de processar dados pessoais em ensaios clínicos para fins relacionados com a fiabilidade e segurança.

No entanto, esta obrigação legal dos responsáveis pelo tratamento não cobre todos os (outros) fins para os quais os dados pessoais são tratados num ensaio clínico. Por conseguinte, o responsável pelo tratamento terá de se basear noutro fundamento jurídico previsto no artigo 6º do RGPD para o tratamento de dados pessoais para tais outros fins de investigação[97].

Outro problema que se coloca é saber em que medida os dados de saúde recolhidos para um determinado projeto/ensaio de investigação com o consentimento dos titulares dos dados poderão ser "reutilizados" em diferentes projetos de

---

[96] Note-se, contudo, que o Parecer 3/2019 se limita ao contexto específico de – alguns – ensaios clínicos, pelo que há espaço para uma abordagem diferente em função das circunstâncias e do equilíbrio de poder entre o sujeito dos dados e o controlador noutros tipos de investigação científica. Por conseguinte, o Parecer 3/2019 não exclui a possibilidade de o responsável pelo tratamento de dados confiar no consentimento explícito como base jurídica para o tratamento de dados dos pacientes (hospitalizados ou não). Nesse sentido, o próprio EDPB nas respostas aos esclarecimentos solicitados pela COM, cit., p. 4.

[97] Neste sentido pronunciou-se o EDPB, esclarecendo, ainda que a COM está atualmente a trabalhar na criação de um Espaço Europeu de Dados de Saúde (EHDS), com o objetivo de melhorar o acesso e a qualidade dos cuidados de saúde, ajudando as autoridades competentes a adotar uma política de apoio à investigação científica. Cf. EDPB, *Esclarecimentos*, cit., p. 6 e proposta da COM para um Regulamento para criar o Espaço Europeu de Dados de Saúde (COM(2022) 197/2).

investigação da mesma natureza por outro responsável sem o consentimento dos titulares dos dados ou, ainda, em que medida pode o consentimento inicial ser invocado para o processamento posterior em tais casos.

Ora, de acordo com o artigo 5.º, n.º 1, alínea b) do RGPD, para o tratamento de dados pessoais para fins de investigação científica em diferentes projetos de investigação, deve ser tido em conta que a presunção de compatibilidade só pode ser utilizada sob a condição de que em tratamento posterior para fins de investigação científica são asseguradas as salvaguardas adequadas, tal como exigido pelo artigo 89.º, n.º 1 do RGPD, que as mesmas são respeitadas. Por conseguinte, a aplicação desta exceção está dependente de clarificação do que tais salvaguardas devem implicar.

Adicionalmente, a este propósito, a COM questionou se poderíamos estar perante um conceito de consentimento "alargado" (*broad consent*). Em resposta, o EDPB assumiu que, ao se utilizar a expressão "consentimento alargado", a COM estaria a referir-se ao Considerando 33 do RGPD e considera que há necessidade de clarificar o respetivo significado e alcance.

Sucede que o Considerando 33 do RGPD abre, no entender do EDPB, em certas circunstâncias, uma possibilidade de atenuar a exigência de especificidade do consentimento, a fim de ser válida como fundamento jurídico para o tratamento de dados pessoais. Assim, pode ser entendido que no mesmo se encontra prevista uma certa válvula de escape, que confere alguma flexibilidade para situações em que os objetivos do tratamento de dados no projeto de investigação científica não podem ser especificados no momento da recolha de dados, mas só pode ser descrita de forma *high level*, ou seja, em termos de (tipos de) investigação ou questões e/ou campos de investigação a explorar[98].

---

[98] Neste sentido, EDPB, *Esclarecimentos*, cit. pp. 7-8. Contudo, o EDPB esclarece que, por enquanto, tal como afirma nas Orientações EDPB 05/2020 sobre a autorização ao abrigo do Regulamento 2016/679 (§153 e ss), ainda que, para os casos em que os objetivos do tratamento de dados no âmbito de um projeto de investigação científica não possam ser especificados à partida, ainda que o Considerando 33 permita, como exceção, que a finalidade possa ser descrita a um nível mais geral, não pode ser interpretado de modo a permitir que um responsável pelo tratamento navegue em torno do princípio-chave da especificação das finalidades para as quais é solicitado o consentimento da pessoa em causa. No seu parecer preliminar sobre proteção de dados e investigação científica, a *European Data Protection Supervisor* (EDPS) indicou, igualmente, que o Considerando 33 não prevalece sobre as condições de consentimento estabelecidas no RGPD. Por conseguinte, não se pode pedir e contar com o consentimento "alargado" para o tratamento de dados de saúde para qualquer tipo – não especificado – de fins de investigação futura. Esse consentimento "alargado" pode, no entanto, ser invocado para diferentes projetos de investigação que satisfaçam determinadas salvaguardas adicionais, as quais serão elaboradas nas futuras orientações da EDPB sobre o tratamento de dados pessoais para fins de investigação científica – cf. EDPB "Guidelines 05/2020 on consent under Regulation 2016/679".

Por fim, e no que concerne ao consentimento no âmbito dos ensaios clínicos, poderá entender-se, a nosso ver, que o consentimento informado ao abrigo do Regulamento de ensaios clínicos é um consentimento especial, mas complementar, face ao do RGPD e que, portanto, se torna mais abrangente, específico e garantístico dos direitos dos indivíduos.

Por conseguinte, poderá entender-se, igualmente, que o consentimento informado do Regulamento dos ensaios clínicos deverá cumprir com os requisitos do consentimento explícito previsto no RGPD para dados especiais, sendo *lex specialis* face ao RGPD.

Portanto, o Regulamento de Ensaios Clínicos vem impor um consentimento mais abrangente do que o consentimento previsto no RGPD, incluindo, nesse consentimento informado, a proteção dos dados pessoais, em particular, por obrigar à sua não divulgação na base de dados europeia ou pela obrigação de anonimização dos dados.

Assim, e conforme referido *supra*, será necessário um consentimento explícito nos termos do artigo 9.º do RGPD, o qual se afigura, todavia, como menos protecionista que a estatuída no Regulamento de Ensaios Clínicos.

3.4.3 Problemas suscitados no âmbito do *E-Health*

Ainda no âmbito do tratamento de dados de saúde, coloca-se o problema recente das plataformas *E-Health*: uma rede voluntária, promovida por autoridades responsáveis pela saúde em linha designadas pelos EM, prevista no artigo 14.º da Diretiva 2011/24/UE, relativa aos direitos dos doentes em matéria de cuidados de saúde transfronteiriços.

A Decisão da COM n.º 2011/890/UE2 estabelece as regras e a criação, gestão e funcionamento da *E-Health*. Entre outros, um dos principais objetivos é reforçar a interoperabilidade entre os sistemas nacionais de saúde digitais no intercâmbio de dados dos doentes contidos nas receitas eletrónicas, nos resumos dos doentes e nos registos de saúde eletrónicos.

Neste contexto, e a fim de facilitar essa interoperabilidade, a rede de saúde em linha e a COM desenvolveram uma ferramenta informática, nomeadamente a infraestrutura de serviços digitais de saúde em linha (*eHealth Digital Service Infrastructure* ou *eHDSI*), a fim de proceder ao intercâmbio de dados relativos à saúde no âmbito do programa desenvolvido pela COM.

Na sua comunicação de 25 de Abril de 2018, a COM sublinhou a necessidade de clarificar o funcionamento do *eHDSI*, bem como o papel da rede de saúde em linha no que respeita à sua governação e à compatibilização com o RGPD.

Nesta medida, o EDPB publicou um parecer[99], no qual entende que (i) o sistema *eHDSI* permite o intercâmbio de dados de saúde eletrónicos dos doentes europeus, em especial receitas eletrónicas e resumos dos registos médicos dos doentes, entre pontos de contacto nacionais, utilizando uma rede privada segura (a seguir designada "TESTA"), criada pela COM; (ii) por conseguinte, se os dados pessoais forem disponibilizados através de uma rede privada, tal significa que estão a ser tratados, independentemente do facto de a COM poder ou não ter acesso aos mesmos, ou de serem aplicadas garantias adequadas para a sua transmissão (por exemplo, uma ligação segura e encriptada); (iii) assim, o facto de os dados pessoais dos pacientes estarem encriptados não prejudica o facto de continuarem a ser dados pessoais e, por isso, de se aplicar o disposto no RGPD.

Discute-se, então, se os cidadãos da UE deverão prestar consentimento como forma de licitude do tratamento dos seus dados médicos ao abrigo da plataforma europeia *E-Health*.

O consentimento, neste caso, deverá cumprir os requisitos previstos para os dados especiais, ou seja, deverá ser um consentimento explícito ou, tratando-se de informação disponibilizada através de ensaios clínicos, deverá ser um consentimento informado, nos termos do Regulamento dos ensaios clínicos, quando este entrar em vigor, como já referido.

Adicionalmente, e por fim, cumpre mencionar, muito brevemente, alguns desafios das aplicações móveis no âmbito da saúde e bem-estar (*Mobile Health*), que compreende práticas médicas e de saúde pública suportadas por dispositivos móveis – *v.g.,* telemóveis, dispositivos de monitorização de doentes, assistentes digitais pessoais e outros dispositivos sem fios. Existem vários tipos de utilização para dispositivos *mHealth* como tecnologias para medir os sinais vitais da frequência cardíaca, o nível de glicose no sangue, a pressão, temperatura corporal e atividades cerebrais; ferramentas de comunicação, informação e motivação (lembrete de medicação/aconselhamento dietético); ou sistemas de orientação pessoal.

Nestes casos, podem colocar-se problemas sobre como o consentimento dos titulares de dados é obtido no âmbito destes serviços. Imagine-se: quando o utilizador descarrega uma aplicação móvel que lhe permite saber (i) quantas horas dormiu num dia, (ii) quantos passos deu por dia, (iii) a média de batimentos cardíacos, (iv) hábitos alimentares, (v) medicação que toma regularmente, com lembretes para o efeito, está a dar o seu consentimento explícito e informado ao

[99] Parecer conjunto EDPB-AEPD 1/2019 sobre tratamento de dados de doentes e o papel da COM no âmbito da infraestrutura de serviços digitais de saúde em linha (*eHDSI*).

descarregar a *app* e permitir o acesso pela mesma aos seus dados pessoais de saúde?

A resposta recai, uma vez mais, nos requisitos específicos do consentimento explícito do RGPD, nomeadamente no artigo. 5.º (verificação das finalidades do tratamento de dados) e 9º (verificação de consentimento explícito).

Adicionalmente, no âmbito da pandemia Covid-19, suscitou-se a questão relacionada com o consentimento do titular de dados no âmbito da utilização de *app*s de rastreio da doença COVID-19, como a *app* "*Stay Away COVID*". Nestes casos, coloca-se a questão de saber se o consentimento do RGPD poderá ser considerado um fundamento de licitude necessário[100]. Entendemos que os requisitos exigidos para o consentimento no âmbito das aplicações *E-Health* aplicam-se, igualmente, no contexto da COVID-19, não podendo ser exigido ao titular dos dados que ceda dos seus dados sem um consentimento prévio e devidamente informado.

Em suma, os dados especiais dos titulares de dados são tão suscetíveis de serem utilizados no âmbito da *Internet* como outras categorias de dados. Contudo, o nível de proteção desta categoria especial de dados, ainda que esteja expressamente prevista no RGPD, deixa inúmeras dúvidas sobre a sua aplicabilidade prática, em especial em contextos informáticos e da sociedade de informação.

4 Síntese Conclusiva

Face ao exposto, conclui-se, desde logo, que a *Internet* é um "palco" propício a potenciais invasões de privacidade dos seus *users*, principalmente no que concerne aos seus dados pessoais, e cuja proteção ainda se encontra, de certa forma, desprotegida, devido à sua a-territorialidade. O consentimento revela-se, deste modo, como um importante fundamento de licitude do tratamento de dados pessoais do respetivo titular.

No contexto europeu, com a aprovação e entrada em vigor do RGPD estabeleceu-se um padrão elevado para o consentimento, que carece dos seguintes requisitos cumulativos para ser legítimo: (i) *manifestação de vontade*, (ii) *livre*, (iii) *específica*, (iv) *informada* e (v) *explícita*. O consentimento surge, portanto, como um conceito de exigente configuração e aplicação e que visa garantir a autonomia pessoal e privacidade do seu titular.

---

[100] A CNPD manifestou uma postura defensiva relativamente ao tratamento de dados pessoais pela *app* "STAYAWAY COVID". Para mais desenvolvimentos cf. Deliberação/2020/277.

Sucede que o RGPD não dá resposta a todos os desafios impostos pelo consentimento, em especial no âmbito da *Internet*, relevando, desde logo, o contributo da dogmática civilista nacional no que diz respeito ao regime sobre a formação dos atos e dos negócios jurídicos. Portanto, e conforme tivemos oportunidade de assinalar ao longo da presente investigação, caberá ao intérprete-aplicador recorrer às bases legais nacionais, nomeadamente do Direito Civil, para interpretar e aplicar as normas sobre proteção de dados, garantindo que estas não contrariam o entendimento do RGPD enquanto lei supranacional e especial.

Outro problema do consentimento tem a ver com a sua fragilidade, em virtude da possibilidade da sua retirada, a qualquer momento, sem necessidade de fundamento, pelo titular dos dados pessoais. Esta fragilidade é particularmente notória em situações de investigação científica, na qual a retirada do consentimento pode prejudicar alguns projetos de investigação científica que exijam que os dados estejam associados a certas pessoas, mas também é particularmente latente no caso do consentimento dos menores, onde a sua prova é particularmente difícil, em especial quando é dado pelos titulares de responsabilidades parentais ou, ainda, nas situações em que não exista paridade entre as partes, ou seja, nas situações em que exista uma parte mais fraca (*v.g.*, relações de consumo, relações laborais ou com seguradoras).

Quanto ao consentimento do titular dos dados no contexto da *Internet*, colocam-se diversos problemas, nomeadamente quando existam transferências de dados para países terceiros, ou no âmbito do chamado "tráfego negocial de massas" e das cláusulas contratuais gerais.

Em particular, afigura-se como particularmente problemática a articulação entre a DEP e o RGPD no que diz respeito à definição dos requisitos de validade do consentimento no contexto das comunicações comerciais e dos *cookies* ou testemunhos de conexão. Neste contexto, concluímos que a DEP opera como lei especial face ao RGPD, mas que, quanto ao *tratamento subsequente* da informação recolhida, ambos os instrumentos normativos deverão ser aplicados em consonância para se aferir a validade do consentimento do titular dos dados.

Por fim, quanto aos dados especiais dos titulares de dados – *v.g.,* dados de saúde –, concluímos que os mesmos são tão suscetíveis de serem utilizados no âmbito da *Internet* como outras categorias de dados. Contudo, o nível de proteção desta categoria especial de dados, ainda que esteja expressamente prevista no RGPD, deixa inúmeras dúvidas sobre a sua aplicabilidade prática, em especial em contextos informáticos e da sociedade de informação.

Face ao exposto, quanto a nós, resulta óbvio que o tema do consentimento do titular de dados é, por si só, um tema complexo. Mais ainda, os problemas

específicos que o contexto especial da *Internet* colocam a este regime são, ainda, particularmente desafiantes para o intérprete-aplicador, atendendo aos diversos interesses e direitos em confronto, mas, principalmente, atendendo à diversidade de temas nos quais o consentimento tem impacto relevante, dificultando uma desejada harmonização de soluções.

Assim, a nosso ver, o consentimento do titular de dados deve ser entendido e interpretado à luz dos princípios e requisitos exigidos no RGPD, servindo este conceito como a base primordial. Contudo, verifica-se, igualmente, que perante determinadas situações concretas, ou perante determinadas categorias de dados pessoais, o conceito de consentimento apresenta-se suficientemente elástico, poroso, flexível e mutável, para se adaptar à realidade que visa proteger, permitindo, por conseguinte, densificações específicas do seu próprio "conceito-base". E sem prejuízo do papel primordial do RGPD e do Direito da União, poderá sempre o intérprete-aplicador recorrer, se necessário, aos princípios internos, nomeadamente de Direito Civil, para melhor interpretar e aplicar o regime do consentimento ao caso concreto, sem prejuízo da garantia de compatibilidade e respeito dessa interpretação para com o RGPD.