UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DIR 2 - DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL

Gabriel Candaten Escher

A DICOTOMIA ENTRE AS BASES LEGAIS PARA O TRATAMENTO DE DADOS SENSÍVEIS DISPONÍVEIS PUBLICAMENTE

PORTO ALEGRE
2022

GABRIEL CANDATEN ESCHER

A DICOTOMIA ENTRE AS BASES LEGAIS PARA O TRATAMENTO DE DADOS SENSÍVEIS DISPONÍVEIS PUBLICAMENTE

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Bacharel em Direito pela Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Porto Alegre
2022

GABRIEL CANDATEN ESCHER

A DICOTOMIA ENTRE AS BASES LEGAIS PARA O TRATAMENTO DE DADOS SENSÍVEIS DISPONÍVEIS PUBLICAMENTE

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Bacharel em Direito pela Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Aprovado em 11 de maio de 2022.

BANCA EXAMINADORA

_____

Prof. Dr. Fabiano Menke

Orientador

_____

Prof. Dr. Gerson Luiz Carlos Branco

_____

Prof. Dr. Luis Renato Ferreira da Silva

RESUMO

O objetivo do presente trabalho é, através de revisão bibliográfica nacional e internacional, pesquisar acerca da possibilidade de enquadramento do tratamento de dados sensíveis nas disposições que regulam dados disponíveis publicamente, quando os dados possuírem ambos os atributos. Será estudado como a evolução das legislações de proteção de dados passou a dotar de maior flexibilidade o tratamento de dados, a ponto de dispensar o consentimento do titular, mas permitindo sua operacionalização com igual ou maior proteção quando comparado ao tratamento fundamentado no consentimento. Assim, constata-se a viabilidade da aplicação das hipóteses autorizativas dos parágrafos 3º, 4º e 7º do artigo 7º da Lei Geral de Proteção de Dados brasileira para dados pessoais sensíveis que estejam disponíveis publicamente, em detrimento das bases legais do art. 11 do mesmo diploma.

Palavras-chave: Proteção de dados; dados sensíveis; dados disponíveis publicamente.

ABSTRACT

The aim of the present work is to, through national and international bibliographical research, look into the possibility of adapting the processing of sensitive data to the dispositions regulating publicly available data, when the data have both attributes. It will be studied how the evolution of data protection laws have relaxed data processing rules to the point of exempting it from the data subject's consent. Thus, it indicates the feasibility of the application of the legal hypotheses of paragraphs 3º, 4º and 7º of article 7º of the Brazilian General Data Protection Law to sensitive personal data that are publicly available, to the detriment of the legal bases of article 11 of the same regulation.

Keywords: Data protection; sensitive data; publicly available data.

LISTA DE SIGLAS E ABREVIATURAS

ANPD – Autoridade Nacional de Proteção de Dados
CEPD – Comité Europeu de Proteção de Dados
DOD – *United States Department of Defense*
DPD – *Directive of Data Protection*
GPS – *Global Positioning System*
ICO – *Information Commissioner's Office*
IP – *Internet Protocol*
LAI – Lei de Acesso à Informação
LGPD – Lei Geral de Proteção de Dados
MCI – Marco Civil da Internet
NSA – *National Security Agency*
PEC – Proposta de Emenda à Constituição
PL – Projeto de Lei
RGPD – Regulamento Geral de Proteção de Dados

SUMÁRIO

1. INTRODUÇÃO

A Lei nº 13.709, de 14 de agosto de 2018, também denominada Lei Geral de Proteção de Dados Pessoais (LGPD), é a legislação brasileira que fornece as diretrizes de como os dados pessoais dos cidadãos podem ser coletados e tratados, regulando tais atividades. Aprovada em agosto de 2018 e com vigência a partir de setembro de 2020, a Lei representou um avanço na segurança de dados pessoais no Brasil, na medida em que criou um cenário de segurança jurídica com uma padronização elevada de normas e práticas para a proteção dos dados pessoais dos cidadãos. Por consequência, suas transformações resultaram na necessidade de revisão dos processos de administração e segurança das informações não somente por parte de empresas privadas, mas também pela administração pública.

Isso em razão de que se pode dizer que o consentimento se tornou a hipótese mais comum para o tratamento de dados, ou seja, o titular dos dados pessoais, a pessoa a quem se referem os dados, deve autorizar, de forma livre, informada e inequívoca, o uso de suas informações para determinados fins. No entanto, para garantir um fluxo mais livre e ininterrupto de dados, o legislador também previu diversas outras bases legais que dispensam a exigência do consentimento, bem como excetuou hipóteses que, em tese, configurariam tratamento ilegítimo de dados, pois sem a anuência do titular.

Uma dessas situações envolve os denominados dados pessoais disponíveis publicamente, para cujo tratamento não há exigência de consentimento, conforme os §§ 3º e 4º do art. 7º da LGPD, mas deve considerar seus propósitos legítimos, os direitos do titular, bem como os fundamentos e princípios previstos na Lei. Isso porque, dentre dados de acesso público e dados tornados manifestamente públicos pelo titular, há dados denominados sensíveis, quais sejam, os que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical ou a organização de caráter religioso, filosófico ou político, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa, cujas bases legais para tratamento encontram-se previstas em separado, no art. 11 da LGPD, justamente pela natureza potencialmente danosa desses dados demandar uma restrição maior ao seu uso.

Ocorre que tanto a administração pública quanto organizações privadas dispõem de uma infinidade de dados pessoais sensíveis, estejam eles armazenados em bancos de dados ou somente disponíveis na internet, sendo recorrente e essencial seu tratamento e até seu compartilhamento no âmbito do Poder Público e de pessoas jurídicas de direito privado, visando ao regular exercício de diversas políticas públicas e atividades privadas. Daí decorre a problemática da não exigência do consentimento do titular para o tratamento de seus dados apenas pelo fato de serem públicos, possivelmente compartilhando tais informações sensíveis sem a devida comunicação ao seu titular e, não raras vezes, prejudicando-o, ainda que a decorrente discriminação possa não ser intencional.

Ante o exposto, impõe-se o estabelecimento de uma relação entre a sensibilidade e a publicidade de dados sensíveis disponíveis publicamente, que parecem ser duas faces de uma mesma moeda, e a análise de possíveis soluções para a dicotomia de seu tratamento. Especificamente, este trabalho visa a analisar como dados sensíveis disponíveis publicamente são tratados e como as hipóteses autorizativas do tratamento de dados disponíveis publicamente, previstas nos §§ 3º, 4º e 7º do art. 7º da LGPD, podem ser operacionalizadas para o tratamento inclusive de dados pessoais sensíveis, viabilizando o regular exercício de atividades públicas e privadas sem comprometer sua segurança jurídica.

Para tanto, procedeu-se à realização de revisão bibliográfica nacional e internacional, especialmente europeia, haja vista que a LGPD sofreu influência direta do marco regulatório europeu. Recorreu-se, ainda, à teoria da privacidade contextual, elaborada por Helen Nissenbaum, como referencial teórico para embasar a ideia do contexto de publicização de dados pessoais como ponto de partida para a análise da viabilidade do tratamento.

O trabalho é dividido em três capítulos. O primeiro capítulo trata da evolução das legislações ao redor do mundo em matéria de proteção de dados, antes com o consentimento como elemento essencial para o tratamento de dados, mas que agora é muitas vezes dispensado, abrindo caminho para o surgimento de fundamentos legais que se baseiam em outros aspectos da relação entre o titular e o controlador de dados, como no caso de dados pessoais disponíveis publicamente.

A partir disso, explorar-se-á, no segundo capítulo, os reflexos da ausência de consentimento para o tratamento de dados pessoais disponíveis publicamente, diferenciando-os entre dados pessoais de acesso público e dados pessoais tornados manifestamente públicos pelo titular. Ainda, caracterizar-se-á dados pessoais sensíveis e se verificará como, frequentemente, estes são disponibilizados publicamente pelo titular ou por terceiros sem a devida ponderação de consequências.

Por fim, no terceiro capítulo, conclui-se como os requisitos específicos presentes nos §§ 3º, 4º e 7º do art. 7º da LGPD podem desempenhar o papel de parâmetros legais também para o tratamento de dados sensíveis, quando disponíveis publicamente, em detrimento das bases legais do art. 11.

2. O CONSENTIMENTO COMO BALIZADOR DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

2.1 EVOLUÇÃO HISTÓRICA DA PROTEÇÃO DE DADOS

A emergência da busca normativa pela proteção de dados pessoais se deu de maneira intrínseca ao reconhecimento da relevância contemporânea dos dados pessoais, hoje insumo principal da atividade econômica em todos os setores da chamada sociedade da informação.

Sob uma perspectiva genérica, o impacto social da tecnologia, ao mesmo tempo que propicia maior conveniência e benefícios para o cidadão, reflete-se também na coleta de dados acerca da privacidade de cada indivíduo e no seu tratamento de modo a atender aos interesses econômicos de uma sociedade deles dependente. O parecer do então Senador Ricardo Ferraço, relator do projeto de lei da Lei Geral de Proteção de Dados Pessoais, bem descreve a redução do indivíduo a dados economicamente úteis:

> Vivemos hoje uma economia maciçamente baseada em dados (*data driven economy*), em que informações sobre todos os aspectos das relações humanas, inclusive da personalidade dos indivíduos, estão sendo coletados, armazenados e processados como nunca fora possível. A todo momento, pessoas, conscientemente ou não, oferecem a um número crescente de empresas – com tecnologia adequada – dados sobre quem são, o que estão fazendo, onde estão, sobre o que falam ou com quem interagem.[1]

Em uma perspectiva específica, entretanto, a vulnerabilidade do indivíduo que decorre da livre circulação de seus dados gera uma tensão entre esses interesses econômicos e a tutela do direito à proteção de dados pessoais, fazendo-se necessária a imposição de limites para garantir os direitos fundamentais de liberdade, de privacidade e de livre desenvolvimento da personalidade.

O marco inicial para a consolidação do direito à privacidade foi a publicação, na revista *Harvard Law Review*, do artigo *"The Right to Privacy"*[2], dos americanos Samuel

---

[1] OLIVEIRA, Ricardo. A importância da LGPD e seu papel no ordenamento jurídico brasileiro. *In*: OLIVEIRA, Ricardo (coord.); COTS, Márcio (coord.). **O Legítimo interesse e a LGPDP**. 2. ed. São Paulo: Thomson Reuters Brasil, 2021. *E-book*. RB-1.1.

[2] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, Boston, v. IV,

D. Warren e Louis D. Brandeis, no ano de 1890. A partir da constatação do vínculo da tutela da privacidade ao progresso tecnológico e de uma necessidade cada vez maior daquela frente às novas formas de obtenção de informações pessoais, os autores construíram a abstração do *right to be let alone* como uma definição primitiva de privacidade[3]. Brandeis, como Juiz Associado da Suprema Corte dos Estados Unidos no caso *Olmstead v. United States* (1928), qualificou-o como o mais abrangente dos direitos e o direito mais valorizado pelos homens civilizados ("the most comprehensive of rights and the right most valued by civilized men")[4].

Apesar da vagueza do conceito legal não permitir a definição de privacidade de modo suficiente a facilitar a estruturação de um arcabouço normativo protetivo para informações pessoais, a atuação de Louis Brandeis na Suprema Corte dos Estados Unidos fortaleceu a noção do direito à privacidade e deixou um legado de intensa discussão acerca desse direito nos Estados Unidos da América, culminando na consolidação do direito à privacidade em diversos ordenamentos jurídicos desde então, inclusive no rol de direitos fundamentais da Declaração Universal dos Direitos Humanos, adotada pela Organização das Nações Unidas em 1948[5]. Porém, foi com o advento da informática na década de 1960 que o direito à privacidade ganhou, também, a tônica atual de direito à proteção de dados pessoais, sobretudo com o crescente processamento automatizado de dados e a preocupação com a falta de transparência ao seu uso na seara das tecnologias da informação e da comunicação.

O caso *Katz v. United States* (1967)[6] foi emblemático pela posição da Corte em redefinir o alcance da Quarta Emenda à Constituição dos Estados Unidos diante de

---

n. 5, pp. 193-220, dez. 1890. Disponível em: <https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 28 fev. 2022.

[3] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.); BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. *E-book*. p. 24.

[4] TAFT, William Howard, and Supreme Court Of The United States. U.S. Reports: **Olmstead v. United States**, 277 U.S. 438. 1927. Disponível em: <https://www.loc.gov/item/usrep277438>. Acesso em: 28 fev. 2022.

[5] Article 12 No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em: <https://www.un.org/sites/un2.un.org/files/udhr.pdf>. Acesso em: 28 fev. 2022.

[6] STEWART, Potter, and Supreme Court Of The United States. U.S. Reports: **Katz v. United States**, 389 U.S. 347. 1967. Disponível em: <https://www.loc.gov/item/usrep389347/>. Acesso em: 28 fev. 2022.

ameaças tecnológicas, com o voto vencido (*dissent*) de Louis Brandeis no caso *Olmstead v. United States* (1928) fundamentando o julgamento desse caso posterior. O voto do Juiz Associado John Marshall Harlan II ganhou notoriedade por elaborar o chamado *Katz Test* para a verificação objetiva de uma constitucionalmente protegida "expectativa razoável de privacidade". A título de exemplo, na situação do caso, se uma pessoa razoável poderia esperar que sua conversa em uma cabine telefônica fosse particular, entendendo a Suprema Corte que sim.[7]

Não obstante a doutrina e jurisprudência americanas, o fato é que, no ano de 1970, o Estado de Hesse, na Alemanha, foi pioneiro e promulgou a primeira legislação no mundo, ainda que em âmbito estadual, a regular o tema específico da "proteção de dados" (*Datenschutz*), a Lei de Proteção de Dados de Hesse (*Hessiches Datenschutzgesetz*). Embora genérica, a Lei estabeleceu princípios básicos da proteção de dados que mantêm sua relevância até hoje, como direitos dos titulares[8], servindo de modelo aos outros estados alemães e à Lei Federal de Proteção de Dados alemã (*Bundesdatenschutzgesetz*), em vigor a partir de 1978.[9]

A primeira legislação nacional sobre o tema, entretanto, surgiu na Suécia em 1973, exigindo a Lei de Dados sueca (*Datalagen*) uma autorização prévia e individualizada da agência de proteção de dados do país, embora não dos indivíduos, para cada registro computadorizado de dados pessoais, garantindo, inclusive, a liberdade de acesso dos titulares aos seus dados, sob pena de indenização no caso de prejuízo advindo do uso de informações incorretas.[10]

Com o relativo sucesso de tais legislações primitivas, no final da década de 1970 diversos países europeus já haviam se juntado à Suécia e à Alemanha com leis próprias para a utilização e exportação de informações de seus cidadãos, chegando

---

[7] SCHNEIDER, Harvey A. ***Katz v. United States***: The Untold Story. Sacramento: McGeorge L. Rev., 2016. Disponível em: <https://scholarlycommons.pacific.edu/mlr/vol40/iss1/2>. Acesso em: 28 fev. 2022.

[8] MENKE, Fabiano. Spiros Simitis e a primeira lei de proteção de dados do mundo. **Migalhas**. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-protecao-de-dados-do-mundo>. Acesso em: 26 fev. 2022.

[9] CORDEIRO, A. Barreto Menezes. **Direito da proteção de dados**: à luz do RGPD e da Lei n.º 58/2019. Coimbra: Almedina, 2020, p. 64.

[10] Ibid., p. 65.

ao ponto de o uso da informática ser regulado nas constituições de Portugal[11] e da Espanha[12].

Posto esse cenário de regulamentação multilateral da proteção de dados, e visando a unificar as normas para o tratamento automatizado de dados pessoais, o Conselho da Europa elaborou, no ano de 1981, a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, marco internacional que serviu de base para que diversas nações regulamentassem localmente regimes de governança para a proteção de dados pessoais. Isso porque, ao contrário das legislações anteriores, a Convenção não tratou apenas de princípios gerais da proteção de dados, mas instituiu dispositivos legais efetivos[13], como regras específicas para a transferência internacional de dados e mecanismos de assistência mútua entre os signatários, e até mesmo a vedação à coleta e ao tratamento de dados pessoais denominados sensíveis na ausência de proteção legal[14].

Na esteira da convenção universal europeia, o Tribunal Constitucional Federal alemão (*Bundesverfassungsgericht*), em um caso emblemático no ano de 1983, confirmou que dados pessoais são constitucionalmente protegidos e que o indivíduo possui um direito constitucional de "autodeterminação informacional" (*informationelle*

---

[11] Artigo 35.º Utilização da informática 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

[12] Artículo 18.4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

[13] CORDEIRO, op. cit., pp. 65-66.

[14] "In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards." COUNCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)**. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 28 fev. 2022.

Selbstbestimmung), ou seja, que indivíduos possuem a prerrogativa de decidir quando e até que ponto suas informações pessoais podem ser publicadas[15]. Foi a primeira vez que se atribuiu à proteção de dados uma dimensão relacionada ao direito constitucional e aos direitos humanos, reconhecendo-se que a liberdade e a autonomia do indivíduo exigiam uma proteção das condições informacionais gerais sob as quais pudessem se desenvolver. A decisão inspirou, inclusive, a vinculação da proteção de dados aos direitos fundamentais previstos no art. 8.º[16] da Carta dos Direitos Fundamentais da União Europeia e no art. 16.º[17] do Tratado sobre o Funcionamento da União Europeia.[18]

Em 1995, ainda nos primeiros anos do bloco, o Parlamento Europeu e o Conselho promulgaram a Diretiva 95/46/CE (*Directive of Data Protection* – DPD), que trata da proteção de indivíduos em relação ao tratamento de dados pessoais e à livre circulação desses dados, regulamentando a intepretação de seus propósitos de maneira muito mais desenvolvida e próxima das legislações atuais.[19]

A Diretiva determinava que cada país tivesse um órgão responsável pela implementação e supervisão da aplicação das leis regionais, que deveriam ser adequadas para estar em conformidade com a Diretiva. Mas, além de unificar o tratamento de dados e o direito dos usuários em todos os países do bloco, a Diretiva

---

[15] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, Gilmar Ferreira (coord.); SARLET, Ingo Wolfgang (coord.); COELHO, Alexandre Zavaglia P. (coord.). **Direito, inovação e tecnologia**. São Paulo, Saraiva, 2015. *E-book*. p. 211.

[16] Artigo 8.º Proteção de dados pessoais 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

[17] Artigo 16.º (ex-artigo 286.º TCE) 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.º do Tratado da União Europeia.

[18] DÖHMANN, Indra Spiecker gen. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. *In*: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.); BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. *E-book*. p. 115.

[19] Ibid., p. 116.

também trouxe medidas específicas sobre o tema e princípios que deveriam ser seguidos em tais circunstâncias, como o princípio da adequação, por meio da coleta e do tratamento de dados com uma finalidade específica e informada ao titular, e o princípio da transparência, operacionalizado pelo direito de acesso aos dados e de informações acerca do tratamento e de seus agentes, entre outras disposições.[20]

Ainda que tenha sido elaborada para uniformizar o direito europeu, suas disposições não podiam ser aplicadas diretamente, ou seja, havia a necessidade de recepção da DPD em cada país, abrindo espaço para discricionariedades na aplicação de suas normas e, consequentemente, enfraquecendo o padrão europeu de proteção de dados. Considerando essa deficiência na efetivação dos diplomas legais anteriores, percebeu-se a necessidade de um alargamento e aprofundamento das legislações nacionais e supranacionais em matéria de proteção de dados, ensejando a elaboração da primeira proposta do futuro Regulamento Geral de Proteção de Dados (RGPD) europeu, em 2012.

A tramitação da proposta ganhou fôlego no ano seguinte, quando o *whistleblower* Edward Snowden, então analista e administrador de sistemas na Agência Nacional de Segurança americana (*National Security Agency – NSA*), expôs o esquema de espionagem e vigilância global realizado pelo órgão, vinculado ao Departamento de Defesa dos Estados Unidos (*United States Department of Defense – DOD*), denunciando uma série de irregularidades e práticas ilegais de uso de dados pessoais, não somente de cidadãos americanos, mas também de governantes e diplomatas europeus e de indivíduos ao redor do globo.[21]

Assim, com a aprovação do Regulamento pelo *Trialogue* da União Europeia em dezembro de 2015 e a sua adoção pelo Conselho da União Europeia e pelo Parlamento Europeu em abril de 2016, em 4 de maio do mesmo ano seu texto foi publicado no Jornal Oficial da União Europeia, iniciando sua vigência na data de 24 de maio de 2016, 20 dias após a publicação, embora suas disposições, inclusive

---

[20] CORDEIRO, op. cit., pp. 67-68.

[21] GELLMAN, Barton; BLAKE, Aaron; MILLER, Greg. Edward Snowden comes forward as source of NSA leaks. **The Washington Post**. Washington, 9 jun. 2013. Disponível em: <https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html>. Acesso em: 28 fev. 2022.

efeitos e penalidades, somente fossem entrar em vigor passados dois anos[22]. Curiosamente, o único país-membro a votar contra o projeto foi a Áustria, justificando que o nível de proteção de dados, em alguns aspectos, era inferior ao verificado na Diretiva de 1995[23].

O RGPD reposicionou o direito à proteção de dados de modo a dotá-lo de maior efetividade, resolvendo seu problema histórico de dificuldade de implementação e cumprimento e obrigando empresas dentro do continente e para além da Europa a modificar radicalmente suas práticas de coleta e tratamento de dados, o que demandou um intervalo de adaptação de 24 meses entre o início da vigência e a entrada em vigor do Regulamento. Na data de 25 de maio de 2018, passado esse período de *vacatio legis*, as suas disposições entraram em vigor e se tornaram diretamente aplicáveis a todos os Estados-membros da União, inclusive para os países do Espaço Econômico Europeu (Islândia, Noruega e Liechtenstein) pouco tempo depois.

Como visto, embora as primeiras legislações regionais e nacionais acerca da proteção de dados tenham surgido na Europa a partir da década de 1970, inclusive com a criação de uma convenção universal em 1981 e de uma diretiva supranacional para a União Europeia em 1995, não foi até a aprovação em 2016 do RGPD e sua entrada em vigor em 2018 que a difusão do direito à proteção de dados pessoais atingiu uma magnitude global, muito em razão do denominado “Efeito Bruxelas”, ou seja, mediante a externalização de regulações europeias através dos mecanismos de globalização do mercado.

Tal fenômeno se apresentou com ainda mais força no que tange à proteção de dados pessoais, haja vista que, após os dois anos do prazo de adequação, países que mantivessem relações comerciais com a União Europeia também deveriam adotar uma legislação de proteção de dados com um padrão regulatório semelhante ao do RGPD, sob pena de imposição de barreiras econômicas ou de dificuldade de fazer

---

[22] The History of the General Data Protection Regulation. **European Data Protection Supervisor**. Disponível em: <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en>. Acesso em: 27 fev. 2022.

[23] EUROPEAN PARLIAMENT. **CM 2213/16**. Disponível em: <https://www.europarl.europa.eu/cmsdata/99614/Procedure_ecrite_GDPR_EN.docx>. Acesso em: 28 fev. 2022.

negócios com os países do bloco. Isso porque o alcance territorial do RGPD foi estendido não somente para o tratamento de dados por controladores ou operadores dentro da União, mas também para o tratamento de dados de pessoas que se encontrem nela, quando o tratamento é relacionado à oferta de bens ou serviços ou ao monitoramento do comportamento do indivíduo.[24]

A inovação da extraterritorialidade do RGPD partiu do entendimento de que, assim como o ambiente virtual não tem fronteiras, assim também o deve ser a lei, de modo que possa transpor os limites nacionais e alcançar toda e qualquer conduta de empresas e organizações que manipulem dados pessoais de cidadãos europeus, seja em parte ou em totalidade, fora do território comum do bloco.[25]

Não obstante, impõe-se tecer a consideração de que a aplicabilidade do Regulamento não é tão irrestrita quanto possa parecer quando da análise de seu âmbito de aplicação extraterritorial. A título exemplificativo, um site de uma marca brasileira que é frequentado majoritariamente por brasileiros não precisaria se adaptar ao RGPD caso percebesse, durante a análise estatística de visitas, que um único cidadão português visualizou o site e teve suas informações coletadas e incluídas em relatórios para tratamento. No entanto, se o mesmo site publicasse um anúncio oferecendo seus produtos ou serviços com preços em euros, anúncio esse que, por sua vez, atraísse o cidadão português, é indiscutível que tal conduta ensejaria a aplicação do disposto no RGPD.

Portanto, no âmbito da União Europeia e do Espaço Econômico Europeu, o Regulamento Geral sobre a Proteção de Dados, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, estabelece as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na União Europeia (artigo 1.º, números 1 e 2, artigo 2.º, e considerandos 1, 2, e 14).[26]

---

[24] WALFORD, Ben. Does the GDPR apply to companies outside of the EU? **GDPR.EU**. Disponível em: <https://gdpr.eu/companies-outside-of-europe/>. Acesso em: 12 fev. 2022.

[25] CAETANO, João Victor Lima. O Regulamento Geral de Proteção de Dados (GDPR): Uma análise do *extraterritorial scope* à luz da jurisdição internacional. **Cadernos Eletrônicos Direito Internacional sem Fronteiras**, v. 2, n. 1, jan-jun 2020, e:11.

[26] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção**

O RGPD, em seu art. 4.º, n.º 1, ainda define dados pessoais como “informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular”.

Tratamento, por seu turno, é definido no n.º 2 do mesmo artigo como “uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição”.

Mais do que apenas informações básicas como nome e número de identificação, o conceito de dados pessoais delineado pela lei europeia engloba toda e qualquer informação relativa a uma pessoa identificada ou identificável, protegendo até mesmo informações acerca de hábitos, gostos e interesses pessoais. A norma institui um modelo preventivo de proteção de dados, baseado na ideia de que todo dado pessoal possui relevância e valor, por representar projeção da pessoa humana[27].

Com inspiração na lei europeia, no Brasil a Lei Geral de Proteção de Dados Pessoais dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º).[28]

---

de Dados). Jornal Oficial da União Europeia, Luxemburgo, L 119, 2016. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1564-1-1>. Acesso em: 1 out. 2021.

[27] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.); BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. *E-book*. p. 131.

[28] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD).

Aqui, a evolução até a estruturação da proteção de dados em um conjunto normativo unitário foi recente[29], ainda que com uma tramitação legislativa demorada. Somente após a tramitação do RGPD nas instituições do Poder Legislativo da União Europeia (Parlamento Europeu e Conselho da União Europeia) é que a proposta ganhou contornos mais definidos no País, assemelhando-se, e muito, à legislação europeia, desde a definição de dados pessoais, direitos dos titulares e até a extraterritorialidade, embora com diferenças pontuais, especialmente quanto às bases legais para o tratamento e às multas[30].

A primeira menção acerca do direito à privacidade no ordenamento jurídico brasileiro é encontrada na Constituição Federal de 1988, em seu art. 5º, inc. X: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”, mas em outros incisos do próprio artigo se encontram disposições complementares acerca do direito à privacidade e do direito à informação, quais sejam, nos incisos XII[31], XIV[32], XXXIII[33] e LXXII[34].

Em 1993, o Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990) reservou uma seção específica para tratar sobre bancos de dados e cadastros de consumidores, normatizando direitos e princípios para conferir ao consumidor a capacidade de autodeterminação no que tange às suas informações pessoais. O art. 43, *caput*, garante o acesso do consumidor a toda e qualquer

---

Diário Oficial da União, Brasília, DF, v. 01, n. 157, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 1 out. 2021.

[29] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021. *E-book*. RB-4.1.

[30] KOCH, Richie. What is the LGPD? Brazil’s version of the GDPR. **GDPR.EU**. Disponível em: <https://gdpr.eu/gdpr-vs-lgpd/>. Acesso em: 12 fev. 2022.

[31] Art. 5º, XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

[32] Art. 5º, XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

[33] Art. 5º, XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

[34] Art. 5º, LXXII - conceder-se-á "*habeas-data*": a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

informação sobre ele, não se restringindo a informações negativas para fins de concessão de crédito. Já os parágrafos seguintes do mesmo artigo garantem a exatidão do banco de dados, bem como sua finalidade clara e verdadeira (§ 1º), a notificação prévia do consumidor da abertura de banco de dados por ele não solicitado (§ 2º), e, ainda, a imediata correção de informações incorretas quando solicitada pelo consumidor (§ 3º).[35]

Porém, somente em 2010 o Ministério da Justiça redigiu o anteprojeto de uma legislação de proteção de dados, promovendo uma consulta pública para incentivar o debate acerca de políticas públicas de proteção de dados pessoais[36]. A consulta pública deu origem ao Projeto de Lei (PL) nº 4060/2012, mas a relevância dada ao tema fomentou o surgimento de outras leis no período, como a Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011) e a Lei de Acesso à Informação (LAI – Lei nº 12.527, de 18 de novembro de 2011)[37].

A LAI ganhou destaque no ordenamento jurídico porque teve como objetivo primordial garantir o direito fundamental de acesso à informação, indicando como diretrizes básicas a publicidade como princípio geral, o sigilo como exceção, a divulgação de informações de interesse público independentemente de solicitação, a cultura da transparência e o controle social da administração pública[38]. Posteriormente, na esteira das repercussões das denúncias de vigilância em massa, mas principalmente como reação da sociedade civil a um movimento legislativo para regulamentar a internet por meio de leis penais, foi acelerada a tramitação do projeto que criou o Marco Civil da Internet (MCI – Lei nº 12.965, de 23 de abril de 2014)[39], que assegurou os direitos e as garantias do cidadão no ambiente eletrônico, reforçando, assim o direito à privacidade no Brasil.

No entanto, em 2015, o Ministério da Justiça promoveu nova consulta pública sobre o tema, que retomou a pauta de proteção de dados e deu origem ao Projeto de

---

[35] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2021. p. 125.
[36] Ibid., p. 130.
[37] Ibid., p. 126.
[38] SENADO FEDERAL. **Acesso à Informação Pública:** Uma leitura da Lei nº 12.527, de 18 de novembro de 2011. p. 3. Disponível em: <https://www12.senado.leg.br/transparencia/arquivos/sobre/cartilha-lai/> Acesso em: 20 mar. 2022.
[39] Ibid., p. 128.

Lei nº 5276/2016, com texto mais completo do que o anterior, devido ao amplo debate que envolveu sua redação[40]. Novamente, a tramitação acelerou somente em março de 2018, quando veio à tona o escândalo de dados Facebook-Cambridge Analytica, durante o qual foi revelado que dados de mais de 87 milhões de usuários do Facebook foram coletados sem seu consentimento e utilizados como assistência analítica para publicidade política. O escândalo alcançou uma magnitude ainda maior quando foram disseminadas acusações de que a coleta e o tratamento ilícitos dos dados teriam influenciado as eleições presidenciais americanas de 2016, especificamente através de seu uso pelas campanhas dos republicanos Donald Trump e Ted Cruz[41], bem como poderiam ter interferido no referendo do mesmo ano referente à saída do Reino Unido da União Europeia (*Brexit*)[42].

Devido à repercussão das denúncias contra a Cambridge Analytica e à entrada em vigor do RGPD na Europa, o projeto de lei da LGPD foi, finalmente, aprovado. Após sua publicação em 14 de agosto de 2018, a Lei, inicialmente, passaria por um período de vacância de 18 meses, porém, tendo em vista que foi exposta a necessidade de um tempo maior para que empresas e instituições se adequassem às inovações trazidas pelo novel diploma, sua data de entrada em vigor foi objeto de constantes debates, até a entrada em vigor em 18 de setembro de 2020 e sua vigência integral em 1º de agosto de 2021, quando começaram a valer as sanções administrativas.

De qualquer sorte, a LGPD traz a premissa da boa-fé para o tratamento de dados pessoais, que, para ser permitido, passa a ter de cumprir, de um lado, uma série de princípios, e, de outro, itens de controles técnicos para governança da segurança das informações, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis[43]. Para tanto, a Lei facilita o controle dos dados tratados, impõe deveres e

---

[40] Ibid., p. 130.
[41] OVERLY, Steven. Report: Trump-linked firm exploited data on 50 million Facebook users. **Politico**. Washington, 17 de março de 2018. Disponível em: <https://www.politico.com/story/2018/03/17/facebook-trump-campaign-data-cambridge-analytica-423599>. Acesso em: 20 mar. 2022.
[42] SCOTT, Mark. Cambridge Analytica did work for Brexit groups, says ex-staffer. **Politico**. Londres, 30 de julho de 2019. Disponível em: <https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/>. Acesso em: 20 mar. 2022.
[43] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**. 3. ed. São Paulo: Saraiva, 2021. *E-book*. p. 21.

responsabilidades aos agentes de tratamento e proporciona segurança para que as informações circulem, visando a antecipar os riscos de violação à privacidade e também evitar tratamentos abusivos de informações e vazamentos de dados[44]. Para Mario Viola e Chiara Spadaccini de Teffé:

> Entende-se que o sistema desenvolvido tem como pilares centrais: a) amplo conceito de dado pessoal; b) necessidade de que qualquer tratamento de dados tenha uma base legal; c) rol taxativo de hipóteses legais para o tratamento de dados; d) caracterização detalhada do consentimento do titular e preocupação com sua manifestação; e) legítimo interesse como uma das hipóteses autorizativas e necessidade de realização de um teste de balanceamento de interesses para a sua regular aplicação; f) amplo rol de direitos do titular; e g) densa carga principiológica.[45]

Reforçando a nova cultura decorrente dos debates nos anteriores, a proteção de dados pessoais se tornou um direito fundamental, previsto na Constituição. Além de prevenir o surgimento de leis estaduais e municipais em conflito ou semelhantes à LGPD, a aprovação da Proposta de Emenda à Constituição (PEC) nº 17, de 2019, impõe a observação do direito à proteção de dados em todos os atos do Poder Público, sejam pelo Executivo, Legislativo ou Judiciário.[46]

2.2 FICÇÃO LEGAL DO CONSENTIMENTO

No rol de diretrizes do art. 2º da LGPD, encontra-se expressa uma dupla função das normas de proteção de dados, qual seja, não somente de garantir a privacidade e outros direitos fundamentais, mas também de fomentar o desenvolvimento econômico em uma sociedade cujos negócios e políticas públicas se sustentam no fluxo informativo dos indivíduos. Para tanto, a proteção de dados conciliaria a antinomia entre o poder econômico e a luta pelos direitos do homem, visando à facilitação de trocas econômicas sem lesar as liberdades dos cidadãos, apenas possível por meio da autodeterminação informativa.[47]

---

[44] VIOLA; TEFFÉ, op. cit., p. 159.
[45] Ibid.
[46] Senado Federal aprova Proposta de Emenda à Constituição 17 (PEC 17/2019) que inclui a proteção de dados pessoais no rol de direitos e garantias fundamentais. **Autoridade Nacional de Proteção de Dados**. Brasília, 21 out. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/senado-federal-aprova-proposta-de-emenda-a-constituicao-17-pec-17-2019-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-e-garantias-fundamentais>. Acesso em: 1 mar. 2022.
[47] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. p. 103.

Essa noção de autodeterminação informativa, prevista tanto no RGPD quanto na LGPD, traduz-se na figura do consentimento do titular como principal fundamento legal para o tratamento de dados. O RGPD, em seu artigo 4.º, número 11, dispõe que o consentimento é uma manifestação de vontade livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. Embora o consentimento escrito não esteja explícito no artigo 4º, número 11, o artigo 7.º/2 também define que o pedido deve ser apresentado de forma destacada e em linguagem clara.

De maneira semelhante, a LGPD, por sua vez, dispõe no inciso XII de seu artigo 5º que o consentimento deve ser livre, informado, inequívoco, bem como deve dizer respeito a uma finalidade determinada e geral — ressalvando-se hipóteses em que é exigido o consentimento específico, como no caso de tratamento de dados sensíveis ou de menores, vide arts. 11, inc. I, e 14, § 1º, respectivamente. Já o artigo 8º acrescenta exigências, privilegiando o consentimento escrito, que deve constar em cláusula contratual destacada (§ 1º), bem como nulificando autorizações genéricas de tratamento, em atenção ao princípio da finalidade (§ 4º).

O consentimento informado nada mais é do que a observância do dever-direito de informação e de transparência, devendo o controlador informar ao titular dos dados, de forma ostensiva, suficiente, clara e adequada (art. 9º, *caput* e incisos) as informações necessárias para dirimir a assimetria informacional entre eles. I.e., é preciso possibilitar ao titular dos dados acesso prévio, completo e detalhado sobre o tratamento dos dados, incluindo sua natureza, objetivos, métodos, duração, justificativa, finalidades, riscos e benefícios, garantindo, assim, um processo genuíno de tomada de decisão.[48]

Por consentimento livre, entende-se a anuência, livre de vícios, do titular dos dados ao tratamento, sendo garantida a liberdade para recusar ou interromper o tratamento de dados em qualquer momento[49]. Em outras palavras, o consentimento

[48] BIONI, 2021. pp. 183-186.
[49] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado:** Lei Geral de Proteção de Dados Pessoais, n. 144, pp. 47-53, nov. 2019. Disponível em:

deve ser uma ação espontânea, caracterizada pelo livre-arbítrio e pelo poder de barganha do titular na escolha de quais funcionalidades ofertadas ele quer fazer uso, e, consequentemente, como compartilhará diferentes tipos de dados[50], atendendo à granularidade do consentimento, ou seja, a possibilidade de seu fatiamento de acordo com os interesses do titular (art. 9º, § 3º).

Por sua vez, o consentimento inequívoco e para finalidades determinadas se relaciona ao princípio da finalidade do tratamento de dados, que impõe que somente será legítima a declaração inequívoca de vontade que estiver ligada a um propósito específico e explícito para seu tratamento[51]. A inequivocidade deve ser depreendida da possibilidade de o titular dos dados configurar a utilização de seus dados de forma a efetivamente controlá-los, sem ser manipulado pelo *design* do um ambiente (art. 6º, *caput*)[52].

Por fim, para que o consentimento seja específico e explícito, há de ser manifestado para um fim concreto, por meio da delimitação do objeto do tratamento dos dados. Mais do que isso, deve haver uma carga participativa maior do titular dos dados, de modo que a manifestação de vontade seja destacada no instrumento de declaração autorizativa para o tratamento de dados e ofereça uma camada a mais de segurança para a efetiva compreensão do titular acerca de seus próprios dados.[53]

Por ser a principal base de legitimidade e de licitude do tratamento de dados pessoais, o consentimento do titular protege os interesses individuais de cada sujeito na medida em que garante ao seu titular o direito de controlar o fluxo de informações para determinada finalidade específica que lhe é informada, assegurando suas legítimas expectativas e preservando o livre desenvolvimento de sua personalidade[54]. Contudo, tal instituto não é imune de críticas por parte da doutrina.

Embora não seja a única base legal da proteção de dados, o protagonismo do titular dos dados pessoais e, consequentemente, do consentimento, ao mesmo tempo

---

<https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html>. Acesso em: 21 mar. 2022.

[50] BIONI, 2021, pp. 188-189.

[51] MULHOLLAND, op. cit., p. 51.

[52] BIONI, 2021, pp. 190-191.

[53] Ibid., pp 192-193.

[54] CORDEIRO, op. cit., p. 167.

que empodera o indivíduo, não pode deixar apenas sobre os ombros deste a proteção de suas informações pessoais. A redução do conteúdo da autodeterminação informativa apenas ao elemento volitivo fragiliza a proteção dos dados na medida em que expõe a incapacidade dos indivíduos de efetivamente controlarem suas informações[55] haja vista que, segundo Spiros Simitis[56], na maioria das vezes, o titular consente apenas formalmente em razão de não poder recusar, como quando os dados são solicitados por um supervisor hierárquico, ou mesmo quando o consentimento é necessário para utilizar serviços essenciais como saúde, emprego, comunicações, contas bancárias, etc[57].

Bert-Japp Koops[58], por sua vez, argumenta que a maioria das pessoas limita-se a consentir sem o fazer conscientemente, quer por falta de paciência, quer porque os meios de avaliação sejam muito pesados e complexos. No mesmo sentido, Daniel J. Solove[59] complementa que os titulares não têm capacidade ou conhecimento para compreender o que leem e, se todos os usuários o decidissem fazer, os custos econômicos seriam elevadíssimos.[60]

Segundo António Barreto Menezes Cordeiro, ainda que se reconheça sua validade, as críticas não bastam para sustentar a concepção paternalista que advém da desconsideração do consentimento, qual seja, a de caber ao legislador determinar que dados podem ser utilizados e em que termos. Dado o caráter personalíssimo dos dados pessoais, o consentimento assume-se como indispensável, mas passível de discussão quanto aos seus limites e à proteção que efetivamente confere ao titular.[61]

Já Bruno Ricardo Bioni pondera se o consentimento, em sua atual hipertrofia, deve ser o elemento normativo central para a proteção de dados. Para o autor, o paradigma normativo da autodeterminação informacional não pode se basear apenas no consentimento específico para permitir o tratamento, o que ele considera como uma ficção legal, pois o reconhecimento do direito ao consentimento traduz apenas

---

[55] BIONI, 2020, pp. 130-131.
[56] SIMITIS apud CORDEIRO, op. cit., p. 168.
[57] CORDEIRO, ibid.
[58] KOOPS apud CORDEIRO, ibid., p. 169.
[59] SOLOVE apud CORDEIRO, ibid.
[60] CORDEIRO, ibid., p. 169.
[61] Ibid., p. 170.

uma falsa ideia de controle na esfera jurídica do titular, haja vista que o consentimento formal, sem possibilidade de recusa, não restringe o uso dos dados pessoais e, pelo contrário, possibilita o acesso ilimitado às informações pessoais.[62]

Portanto, haveria a necessidade de capacitar o cidadão com um maior controle de suas informações pessoais através do que o autor denomina consentimento contextual, ou seja, por meio da adequação do fluxo informacional ao livre desenvolvimento da personalidade e, ao mesmo tempo, ao uso dos dados de acordo com a expectativa legítima gerada no titular pelo contexto do tratamento. Assim, manter-se-ia o papel de protagonismo do consentimento, mas com a ressalva da vulnerabilidade do titular dos dados pessoais, impondo-se um novo roteiro normativo, considerando, *in verbis*: “a percepção de que o titular dos dados pessoais amarga uma (hiper)vulnerabilidade, o que demanda, respectivamente, o seu empoderamento para emancipá-lo e a sua intervenção para assisti-lo”.[63]

Como visto, a doutrina se mostra cética à utilização do consentimento como principal balizador do direito à proteção dos dados pessoais, em detrimento das outras bases legais apresentadas pela LGPD, tendo em vista que a mera manifestação formal não é suficiente para consagrar a proteção originalmente concebida pelas leis de proteção de dados. Por consequência, diversas teorias são defendidas para mitigar a vulnerabilidade do titular de dados, seja através da desconsideração do consentimento, situação na qual o legislador decidiria acerca do uso de dados individuais, seja através da aplicação de condicionantes como a expectativa legítima e o legítimo interesse, linha adotada pela maioria dos autores.

Em suma, é nesse sentido que se pode afirmar que, a despeito dos requisitos objetivos formais, a subjetividade material na qual a declaração de consentimento é pautada pode ensejar um elevado grau de insegurança jurídica quanto à validade da declaração, especialmente em abordagens de consentimento forçado, conhecidas como *take it or leave it*, nas quais o usuário é obrigado a aceitar integralmente os termos para o tratamento de seus dados, sob pena de não poder utilizar um serviço. Frequentemente manejado, a título de exemplo, por *Big Techs* como Facebook, Inc e

[62] BIONI, 2021, p. xxix.
[63] Ibid., p. xxix.

Google LLC, esse tipo de abordagem já resultou em ações judiciais sob a égide do RGPD europeu, inclusive com a aplicação de multas pelo reconhecimento de tal prática como abusiva.[64]

Ademais, a própria LGPD abre margem para a discussão de conflitos normativos acerca do consentimento e de seu papel como elemento central da proteção de dados. Haja vista que o § 2º do artigo 18 garante ao titular de dados o direito de se opor a tratamento realizado mesmo em hipóteses de dispensa de consentimento, caso dos incisos II a X do artigo 7º, em razão da obrigação de observação dos direitos do titular e princípios gerais da LGPD, vide seu artigo 7º, § 6º, tem-se que, além do consentimento, a Lei também é expressa em minimizar a vulnerabilidade do indivíduo quando o tratamento é realizado sem sua anuência, trazendo dúvidas quanto à efetividade da manifestação de vontade *per se* nos casos em que esta é exigida.

Tal debate acompanhará a evolução das recentes leis de proteção de dados, sendo certo que o crescente número de responsabilizações por estas ensejará o aprofundamento da contraposição entre os requisitos objetivos do consentimento e a subjetividade da legitimidade de expectativas e interesses. Foi já com isso em mente que o legislador pátrio estabeleceu tanto requisitos a serem cumpridos quanto princípios gerais a serem observados para garantir eventual tratamento legítimo e adequado de dados. Requisitos e princípios esses que também viabilizam a previsão de outras bases legais para o tratamento de dados que não o consentimento, hipóteses que seriam inviáveis caso o consentimento expresso fosse a única exigência a ser observada, como no caso de dados disponíveis publicamente.

---

[64] SATARIANO, Adam. Facebook's WhatsApp is fined for breaking the E.U.'s data privacy law. **The New York Times**. Londres, 02 set. 2021. Disponível em: <https://www.nytimes.com/2021/09/02/business/facebook-whatsapp-privacy-fine.html>. Acesso em: 1 out. 2021.

3. ENTRE A FADIGA E A TRAVA DO CONSENTIMENTO

3.1 EXCEÇÃO DOS DADOS DISPONÍVEIS PUBLICAMENTE

Dados pessoais disponíveis publicamente podem ser definidos como dados relacionados a pessoa natural, identificada ou identificável, e que foram intencionalmente publicizados pelo titular ou por terceiro, estando acessíveis a qualquer cidadão.

Se livremente acessíveis, um poderia deduzir que também podem ser livremente tratados. *A contrario sensu*, dados disponíveis publicamente sujeitam-se a regimes de tratamento diferenciados que mantêm o domínio do titular sobre seus dados, ainda que não exijam o seu consentimento, mas desde que os dados sejam tratados de acordo com o referencial da privacidade contextual.[65]

Já no próprio texto legal, dados pessoais disponíveis publicamente são subdivididos em dados pessoais de acesso público e dados pessoais tornados manifestamente públicos pelo titular, sendo os primeiros regulados pela LGPD em seu art. 7º, §§ 3º e 7º, ao passo que se encontra a previsão de tratamento dos segundos nos §§ 4º e 7º do mesmo artigo, *in verbis*:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> (...)
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
> § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
> (...)
> § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

Os exemplos clássicos para o fim de diferenciar dados de acesso público de dados tornados manifestamente públicos são, para o primeiro, dados constantes de

[65] BIONI, 2021, p. 275.

portais de órgãos governamentais livremente acessíveis para o público, enquanto, para o segundo, são dados publicados e compartilhados pelo titular em redes sociais.

Entretanto, e conforme observa Giovanna Milanez Tavares[66], a LGPD não define nem dados pessoais disponíveis publicamente, nem dados pessoais de acesso público ou dados pessoais tornados manifestamente públicos pelo titular, fazendo-se necessária a busca por uma definição para os dois últimos tomando-se como base as terminologias encontradas no Decreto nº 8.777, de 11 de maio de 2016 (Política de Dados Abertos do Poder Executivo Federal) e na LAI.

Segundo a autora, o conceito de dados pessoais de acesso público pode ser comparado ao de dado aberto com qualificador pessoal, nos termos do art. 2º, II e III, do Decreto, ou seja, um dado relacionado a uma pessoa natural identificada ou identificável, gerado ou acumulado pelo Governo, que não esteja sob sigilo ou sob restrição de acesso nos termos da LAI, disponibilizado sob licença aberta que permita sua livre utilização, consumo ou cruzamento.[67]

Contudo, para não limitar a conceituação de dados pessoais de acesso público como somente aqueles dados dos quais dispõe a administração pública, também se mostra necessária a comparação com o conceito de informação pessoal de acesso público, presente nos arts. 3º, II, 4º, I, III e IV, e 8º, *caput*, da LAI, qual seja, qualquer dado de interesse coletivo ou geral, de acesso público, processado ou não, relacionado a uma pessoa natural identificada ou identificável, que pode ser utilizado para produção e transmissão de conhecimento, contido em qualquer meio, suporte ou formato.[68]

A partir dessa análise sistemática, a autora observa duas características para a qualificação de um dado como de acesso público: a publicidade ampla do dado, ou seja, seu livre acesso pelo público geral, e a divulgação intencional do dado por terceiros que não o próprio titular. Com isso em mente, conclui pela definição preliminar de dado pessoal de acesso público como qualquer dado pessoal que tenha

---

[66] TAVARES, Giovanna Milanez. **O tratamento de dados pessoais disponíveis publicamente e os limites impostos pela LGPD**. Rio de Janeiro: Processo, 2022. pp. 61-62.
[67] Ibid., pp. 63-64.
[68] Ibid.

sido divulgado intencionalmente por terceiro, com ampla publicidade e acessibilidade.[69]

Dados pessoais tornados manifestamente públicos pelo titular, por seu turno, também pressupõem duas condições para sua caracterização, quais sejam, a disponibilização dos dados ao público pelo próprio titular em um ato deliberado e intencional, bem como a manifesta publicidade e acessibilidade irrestrita dos dados.[70]

Quanto à primeira, trata-se da divulgação ativa de seus dados pessoais com a ciência, ou mesmo com a pretensão, de um possível tratamento posterior. Para que se possa validar a ciência, exige-se o manifesto conhecimento de que foi o próprio titular que os tornou públicos, pois a dispensa de consentimento do § 4º não acoberta o tratamento de dados que tenham sido tornados públicos por outros sujeitos, que não o próprio titular[71]. No entanto, ainda que a ciência possa ser aferida objetivamente, a investigação pretérita pelos controladores da intenção dos usuários quanto aos dados já tornados públicos por estes parece uma exigência inviável, de modo que a pretensão de um tratamento posterior pode ser extraída já do aspecto inegavelmente público que os dados atingiram pela divulgação feita pelo titular[72], como dados publicados pelo titular em seu perfil de uma rede social profissional, onde espera que sejam visualizados, compartilhados e também tratados por empresas da sua área.

Já quanto à segunda condição, exige-se o acesso indistinto pelo público em geral, não somente a divulgação, ainda que ampla, para grupos específicos. Utilizando-se do mesmo exemplo anterior, dados publicados pelo titular em uma rede social profissional, visando ao alcance de várias empresas, são dados tornados manifestamente públicos, porém, se os mesmos dados são publicados em uma rede social de cunho pessoal, limitando-se o acesso ao seu grupo de amigos, já não o são, pois os dados são públicos, mas não de acesso irrestrito.

---

[69] Ibid.,

[70] Ibid., pp. 74-77.

[71] MARCACINI, Augusto Tavares Rosa. As regras aplicadas ao tratamento de dados pessoais. *In*: LIMA, Cíntia Rosa Pereira de (coord.). **Comentários à Lei Geral de Proteção de Dados:** Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020. *E-book*. p. 147.

[72] MOREIRA, André de Oliveira Schenini. A exceção dos dados pessoais tornados manifestamente públicos pelo titular na LGPD. **Migalhas**. Disponível em: <https://www.migalhas.com.br/depeso/293745/a-excecao-dos-dados-pessoais-tornados-manifestamente-publicos-pelo-titular-na-lgpd>. Acesso em: 26 fev. 2022.

Em suma, pode-se diferenciar as espécies de dado pessoal de acesso público e dado pessoal tornado manifestamente público pelo titular através de critérios normativos de identificação prática, quais sejam: (i) o sujeito que tornou o dado acessível publicamente, pois dados de acesso público são publicizados por um terceiro, enquanto os tornados manifestamente públicos pelo titular, como diz o próprio nome, foram disponibilizados pelo próprio titular; (ii) a justificação da divulgação pública, haja vista que sempre há uma obrigação legal de publicidade de dados de acesso público, ao passo que dados tornados manifestamente públicos só o são a partir da vontade do titular; e (iii) a manifesta acessibilidade a um público irrestrito e incondicionado, a qual não é exigida para dados de acesso público, pois passíveis de limitação de visibilidade, mas obrigatórios para a caracterização de dados pessoais como tornados manifestamente públicos pelo titular, sob pena de serem considerados apenas dados pessoais e, consequentemente, sujeitarem-se às bases legais dos incisos do art. 7º da LGPD para tratamento, sem o benefício da dispensa de consentimento.[73]

Tal subdivisão do gênero dados disponíveis publicamente entre dados de acesso público e tornados manifestamente públicos não se deu por acaso, porquanto fruto de amplo debate público desde a consulta pública do Anteprojeto de Lei de 2010, haja vista que o espírito da LGPD é justamente transpor a dicotomia entre o público e o privado em matéria de dados, privilegiando o contexto no qual os dados são publicamente acessíveis em detrimento de sua natureza.[74] Isto é, dados públicos, oriundos de registros, atos ou documentos públicos de acesso público irrestrito, a título exemplificativo, não perdem seu caráter pessoal apenas por não conterem informações privadas ou sensíveis do indivíduo ao qual são relativos, superando o entendimento, antes comum, de que dados obtidos de fontes públicas, de livre circulação e acesso amplo, poderiam ser utilizados por qualquer um, de qualquer forma e para qualquer finalidade.

Assim, para o tratamento de dados pessoais de acesso público, o § 3º do art. 7º elenca a finalidade, a boa-fé e o interesse público que justificaram a disponibilização

[73] TAVARES, op. cit., p. 81.
[74] BIONI, 2021, p. 275.

dos dados como quesitos para permitir o controle da licitude ou não de seu tratamento. É justamente essa análise contextual que calibra os possíveis usos que podem ser feitos dos dados, de acordo com a compatibilidade com a finalidade e o interesse público pelo qual tais dados são de acesso público.[75]

A título de exemplo, dados pessoais de acesso público constantes de certidões judiciais emitidas especificamente para aferir a capacidade de solvência dos cidadãos poderiam ser utilizados para análise de crédito, considerando a finalidade e o interesse público que justificaram a disponibilização, mas não poderiam ser utilizados para a desclassificação de um candidato a uma vaga de emprego apenas pela existência de uma dívida, pois restaria desvirtuada a finalidade e configurado o uso abusivo das informações.[76]

Em contrapartida, parte da doutrina entende que referido parágrafo não poderia ser tratado como uma hipótese de dispensa de consentimento, pois não estaria redigido no formato de uma exceção. O enquadramento em uma das bases legais autorizativas se mostraria necessário para evitar que dados de acesso público, publicados, por exemplo, por força de uma obrigação legal, fossem uma carta branca para um tratamento posterior, com uma finalidade distinta, sem a demonstração da existência de uma base legal que autorizasse o tratamento de tal dado, especialmente quando ele não foi tornado público por seu titular.[77]

No entanto, o uso da base legal autônoma do § 3º somente pode acontecer com a observância do requisito da identidade da finalidade do tratamento, ou seja, se a finalidade desse novo tratamento for a mesma que justificou a disponibilização do dado, pois a Lei prevê outras bases legais para os casos de finalidades diversas. O próprio § 7º do art. 7º pode ser utilizado como hipótese autorizativa para o tratamento cuja finalidade não seja idêntica, mas compatível à original, enquanto as bases legais dos incisos do art. 7º podem ser utilizadas para finalidades diversas e não compatíveis.[78]

---

[75] Ibid., p. 267.
[76] TAVARES, op. cit., pp. 96-97.
[77] VIOLA; TEFFÉ, op. cit., p 138.
[78] TAVARES, op. cit., p. 156.

O mesmo entendimento pode ser aplicado à hipótese do § 4º, não havendo necessidade de uma nova base legal para o tratamento de dados tornados manifestamente públicos, já que se trata de verdadeira hipótese autorizativa para o tratamento de dados sem o consentimento de seu titular, ou, melhor dizendo, tratando-se de outra base legal autônoma.

Como introduzido, já no caso de dados pessoais tornados manifestamente públicos pelo titular, é expresso na Lei que, via de regra, não se exige o consentimento do titular para que sejam tratados, haja vista a exceção disposta no § 4º do art. 7º da LGPD. Conforme ensina Augusto Tavares Rosa Marcacini:

> Parece-nos, para utilizarmos corretamente as palavras e conceitos, que o que este parágrafo dispensa é a manifestação expressa de consentimento; presume a Lei que o ato de publicar os próprios dados, que é em si uma manifestação de vontade do titular, é uma autorização para que possam ser tratados.[79]

À primeira vista, a previsão legal de uma exceção de dispensa do consentimento do titular para o tratamento de seus dados disponíveis publicamente se justificaria na medida em que seria inerente à ideia de publicidade que os dados pudessem ser livremente acessados e tratados quando disponibilizados. Logo, não haveria falar, a princípio, de qualquer violação a direitos do titular, pois ilógico exigir sua anuência para o tratamento de toda e qualquer informação básica, tais como seu nome, quando constantes de bancos de dados públicos ou quando o próprio titular as disponibilizou.

Nessa lógica, a manifestação de vontade representada pela publicização de dados por seu titular poderia ser utilizada como uma alternativa para permitir um amplo tratamento de dados pessoais sem o enquadramento em qualquer das bases legais previstas na Lei. Isso porque o controlador que atuasse sob a regra excepcional do § 4º não precisaria justificar suas atividades em nenhuma das demais hipóteses autorizadoras do art. 7º da LGPD, configurando-se a dispensa do consentimento em razão da publicização dos dados como verdadeira base legal autônoma, ainda que não elencada com as demais.

---

[79] MARCACINI, op. cit., p. 147.

Quando a base legal para o tratamento é o consentimento, qualquer uso de dados com finalidade diversa da autorização conferida, ou a ausência de comprovação efetiva do recebimento do consentimento, torna os controladores passíveis de serem responsabilizados e de sofrerem as sanções legais previstas na LGPD, como o ressarcimento de danos causados ao titular dos dados pelo uso indevido destes.

Por sua vez, a amplitude da possibilidade de tratamento de dados apenas em razão da publicização pelo titular, e especialmente em substituição ao oneroso ônus de se exigir seu consentimento expresso, que é restrito a uma finalidade específica, a exceção da dispensa do consentimento para o tratamento de dados tornados manifestamente públicos por seu titular poderia se tornar uma válvula de escape para os controladores[80].

Entretanto, não é a mera disponibilização *on-line* do dado que enseja a possibilidade de utilização dessa base legal autônoma. Mais do que tornado público, o dado precisa ser manifestamente tornado público, ou seja, o titular, inequivocamente, deve desejar e esperar que o dado seja processado posteriormente, bem como o controlador deve demonstrar, quando do tratamento, que a finalidade deste não poderia ser atingida por outros meios.[81]

Ademais, o conteúdo principiológico da LGPD não é afastado apenas pela publicização pelo titular de seus dados pessoais, pois o próprio § 4º, em sua parte final, assevera a necessidade de observância aos direitos do titular e aos princípios previstos no art. 6º da Lei, em especial aos princípios da finalidade, da adequação, e da necessidade do tratamento.

Por mais que tais princípios sejam aplicáveis a toda atividade de tratamento de dados pessoais regulada pela LGPD, André de Oliveira Schenini Moreira também

---

[80] MOREIRA, op. cit.

[81] “On the other hand, such data would have to be made public by the data subject, and more than that, manifestly made public, so as to indicate that they wish and expect such data to be further processed. No need to mention that all other provisions, including the principles and the Article 6, still apply, and also the personal data may be processed only if the purpose of the processing could not reasonably be fulfilled by other means”. FOITZIK, Piotr. Publicly available data under the GDPR: Main considerations. **International Association of Privacy Professionals**. Disponível em: <https://iapp.org/news/a/publicly-available-data-under-gdpr-main-considerations/>. Acesso em: 20 mar. 2022.

enxerga uma maior limitação à exploração de dados pessoais a partir da hipótese de dispensa de consentimento comparativamente ao mecanismo do consentimento. Para o autor, a expressa autorização do usuário permite uma maior liberdade para o controlador fazer uso dos dados pessoais, enquanto a dispensa de consentimento não funciona com essa mesma amplitude, mormente levando em conta o ato e o contexto de publicização para fundamentar a análise de finalidade e adequação.[82]

Utilizando-se do exemplo ilustrado pelo autor, alguém que torna pública a informação de que já frequentou determinada pizzaria, através de uma postagem em uma rede social, pode vir a ter a informação utilizada para fins de oferecimento de um cupom exclusivo de desconto para quando retornar ao estabelecimento. Todavia, a inserção de tal pessoa em um cadastro de consumidores de pizza para acesso geral já não é aceitável sob o ponto de vista da finalidade e da adequação, pois, a partir do contexto do ato de publicação, infere-se que a intenção do indivíduo não é compatível com a finalidade do tratamento.[83]

Logo, vê-se que a análise do contexto da publicização pelo titular de seus dados pessoais é a chave para a verificação da possibilidade ou não do manejo da exceção do § 4º do art. 7º, tendo em vista, por um lado, sua amplitude reduzida em relação ao consentimento expresso, mas, por outro, a facilidade de coleta e tratamento dos dados. É evidente que a intenção do legislador foi proporcionar uma fluidez maior para o ambiente de tratamento de dados pessoais, ainda que para a maioria das situações, a obtenção do consentimento do titular para o tratamento de dados tornados manifestamente públicos permaneça indispensável.

Ainda segundo Moreira, a dúvida que resta diz respeito não aos princípios, mas ao exercício de direitos do titular, previstos, em sua maior parte, nos arts. 17 a 22 da LGPD, já que os dados são acessíveis a qualquer momento, sem necessidade de consentimento. No entanto, o próprio art. 18 já esclarece a questão quando dispõe, em seu § 2º, que “o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta lei”.[84]

---

[82] MOREIRA, op. cit.
[83] Ibid.
[84] Ibid.

Por conseguinte, mesmo que a hipótese autorizativa do § 4º do art. 7º não exija o consentimento do titular para o tratamento de seus dados tornados manifestamente públicos, é garantido ao titular o direito de se opor a tal tratamento e até mesmo de solicitar a eliminação de seus dados, mas desde que nas hipóteses de desrespeito à LGPD. Essa ressalva surge da leitura inversa do § 2º do art. 18, por meio da qual se extrai a conclusão de que o uso de dados dispensado de consentimento, dentro dos limites legais, não está sujeito à oposição de seu titular.[85]

Essa, porém, não parece ser a interpretação extraída do RGPD europeu, inspiração da LGPD, na hipótese de autorização do tratamento de dados pessoais de categorias especiais que tenham sido tornados manifestamente públicos pelo titular.[86]

3.2 ESPECIALIDADE DE DADOS PESSOAIS SENSÍVEIS

Em seu art. 5º, inc. II, a LGPD define dados pessoais sensíveis como aqueles “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”.

Os dados pessoais sensíveis são uma das duas exceções, junto aos dados pessoais de crianças e de adolescentes, cujas bases legais para tratamento não se encontram no art. 7º, estando as primeiras reguladas no art. 11 e, diga-se de passagem, de forma muito mais restritiva do que nas hipóteses autorizativas de tratamento de outros dados pessoais.

Essa disciplina especial para dados pessoais sensíveis se justifica na medida em que sua utilização se mostra indispensável em algumas situações, mas sua natureza e suas características importam em riscos significativos aos direitos e às liberdades fundamentais da pessoa no caso de violação ao disposto na Lei, i.e., através de seu uso de modo discriminatório, ilícito ou abusivo. Referidos riscos são potencializados pela constatação de que não há uma linha distintiva nítida entre dados

[85] Ibid.
[86] TAVARES, op. cit., p. 76.

pessoais e dados pessoais sensíveis, a despeito do rol supostamente taxativo do inciso II do art. 5º. Segundo Ana Frazão[87], a perspectiva de análise da sensibilidade de um dado deve ser dinâmica, e não estática, de sorte que, mesmo dados que, aprioristicamente, não se enquadrem nessa categoria podem ser considerados sensíveis quando permitirem que se chegue, como resultado final, a informações sensíveis do titular, sendo então denominados dados pessoais potencialmente sensíveis.

Inobstante a análise contextual, também se faz necessária uma análise principiológica, nomeadamente quanto à incidência do princípio da não discriminação, previsto no art. 6º da LGPD como a "impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos". Isso porque a essência da especialidade da proteção dos dados sensíveis é, justamente, permitir uma igualdade substancial no tratamento dos dados, vedando a discriminação de seus titulares e a abusividade de manipulação que dele podem surgir.

Portanto, tem-se que a determinação da sensibilidade ou não de um dado passa não somente pelo contexto de seu tratamento, mas também pelas inferências que dele podem ser extraídas, ainda que não haja outros dados disponíveis para corroborar tais relações, bem como pelo grau de potencialidade de sua utilização como instrumento de estigmatização ou discriminação[88]. Tal entendimento encontra respaldo na própria LGPD, haja vista que, no § 1º do art. 11, a aplicação do disposto para o tratamento de dados pessoais sensíveis se estende “a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular”. O exemplo mais recorrente na doutrina contempla a análise do histórico de compras de um indivíduo, seja através do registro de entradas e saídas do próprio comércio, como em um supermercado ou farmácia, seja através do acesso à fatura do seu cartão de crédito, haja vista que se torna possível a inferência de dados sensíveis, como sua orientação sexual ou seu estado de saúde.[89]

---

[87] FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. **Jota**. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018>. Acesso em: 16 mar. 2022.
[88] VIOLA; TEFFÉ, op. cit., p. 153.
[89] Ibid., p. 156.

O fato é que, embora a Lei permita o tratamento dos dados sensíveis e o uso das informações dele decorrentes, ela não regulamenta a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem, apenas referindo que tal prática pode ser objeto de vedação ou de regulamentação pela autoridade nacional, consoante seu § 3º. Entretanto, seu § 4º veda expressamente a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, especificamente quando com o objetivo de obtenção de vantagem econômica[90], excetuando hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º do mesmo artigo.

O mencionado § 5º refere que é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. À primeira vista, parece que o legislador proíbe qualquer utilização de dados do estado de saúde de um indivíduo por parte de operadoras de planos de saúde, o que terminantemente inviabilizaria essa atividade econômica.

No entanto, em análise detida da terminologia empregada, percebe-se que o sentido do dispositivo é o mesmo da Lei nº 9.656, de 3 junho de 1998, que versa sobre os planos e seguros privados de assistência à saúde, depreendendo-se que o que foi coibido é, na verdade, a obtenção de informações sensíveis para recusar o oferecimento de cobertura a determinado proponente em razão da sua idade ou de ele ser portador de deficiência. Essa seleção ilícita de riscos é diferente da análise de riscos, que nada mais é do que a precificação desses para fins de subscrição, por exemplo, com o agravo do prêmio em razão de doença preexistente, prática lícita e que autoriza o tratamento de dados sensíveis referentes à saúde do beneficiário ou do segurado para essa finalidade.[91]

---

[90] “Importante destacar, ainda, que nem toda comunicação ou uso compartilhado de dados sensíveis referentes à saúde será escopo de obter vantagem econômica. Um exemplo de uso compartilhado com finalidade não econômica é justamente o combate e a prevenção à fraude contra o seguro.” Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados pessoais. **CNseg**. p. 34. Disponível em: <https://cnseg.org.br/data/files/A6/25/A2/F2/9B22571029E24F473A8AA8A8/GBPMS_ONLINE_ok.pdf >. Acesso em: 19 mar. 2022.

[91] “Especificamente no que toca ao setor de saúde suplementar, deve-se dar destaque ao disposto no §5º do art. 11 da LGPD. Uma leitura isolada e não sistemática desse dispositivo poderia levar à interpretação de que estaria vedada a utilização de dados de saúde para a subscrição de seguros

Logo, o tratamento de dados que gere uma discriminação para fins lícitos, como a segmentação de riscos securitários, poderá ser admitido, ainda que envolva dados sensíveis, desde que presente alguma das hipóteses autorizativas previstas nos já citados artigos 7º e 11 e havendo pleno respeito às normas da LGPD.

Ademais, a proteção dos dados sensíveis referentes à saúde tem seu protagonismo reforçado no atual cenário pandêmico, pautado por uma coleta ostensiva de dados pessoais para abastecer sistemas de vigilância sob o pretexto de combate à doença e de proteção à saúde. A título de exemplo, dados de geolocalização e contatos físicos, mesmo a princípio não sensíveis, podem ser utilizados para a verificação de informações íntimas, inclusive podendo ser manipulados para usos lesivos, como para o rastreamento de pessoas infectadas e de seus contatos recentes para impor medidas restritivas de direitos, como o isolamento domiciliar. Nesse sentido, Viola e Teffé questionam:

> Até onde o interesse coletivo pode avançar sobre o individual? Quais mecanismos de rastreamento e coleta de dados serão aplicados e por quanto tempo? Quem terá acesso aos bancos de dados criados? Serão eles algum dia descartados? O que se mostra justificável diante de um cenário de pandemia global e qual legado isso deixará para o tema da proteção de dados? Perguntas apresentadas globalmente, mas ainda sem respostas.[92]

Stefano Rodotà bem esclarece que, em relação aos dados de saúde, "a proteção especial atribuída a estes dados não se justifica somente por se referirem a fatos íntimos, mas também, e às vezes sobretudo, pelo risco que seu conhecimento possa provocar discriminações"[93]. Não há dúvida de que, sejam empregadores, seguradoras e operadoras de planos de saúde, sejam governos, tanto os agentes privados quanto os públicos que tratarem informações pessoais deverão agir em

---

saúde. Esse dispositivo, porém, deve ser lido em consonância com o que dispõe a Lei nº 9.656/98 (que versa sobre os planos e seguros privados de assistência à saúde) e aqui merece ser feita uma distinção entre seleção de riscos e análise de risco para fins de subscrição e precificação. A Lei nº 9.656/98 veda a seleção de riscos, ou seja, a possibilidade de recusa de oferecimento de cobertura a determinado proponente, porém a mesma lei reconhece a possibilidade de precificação e de análise de riscos para fins de subscrição ao admitir que, na presença de doença preexistente, deverá ser ofertada ao proponente a cobertura parcial temporária ou o agravo do prêmio durante o período no qual seria aplicável a cobertura parcial temporária. Portanto, é nessa linha que deve ser interpretado esse dispositivo da LGPD. Logo, é fundamental que se ponha em perspectiva que nem toda discriminação é prejudicial e ilícita, como não é, por exemplo, aquela diretamente relacionada a subsidiar a contratação de um seguro." Ibid., p. 14.

[92] VIOLA; TEFFÉ, op. cit., p. 157.

[93] RODOTÀ apud VIOLA; TEFFÉ, ibid., p. 157.

conformidade com os limites fixados no ordenamento, evitando medidas arbitrárias que extrapolem a proporcionalidade na restrição de direitos individuais e causem discriminações, sob pena de responsabilidade[94].

Nesse diapasão, é evidente que dados sensíveis necessitam de uma tutela diferenciada e mais protetiva, visando a evitar que sejam vazados, usados indevidamente, comercializados ou utilizados para discriminar ilicitamente o titular. Não se pode simplesmente proibir o tratamento de dados sensíveis, pois tal proibição seria inviável na medida em que o uso desses dados pode ser legítimo e até mesmo necessário, tendo em vista o exposto nas hipóteses autorizativas do inc. II do art. 11, sob pena do comprometimento da razão de ser de diversos organismos. Instituições hospitalares, a título de exemplo, tratam alguns dos dados mais sensíveis definidos pela Lei, se é que é possível graduá-los assim, haja vista a potencial sensibilidade de qualquer dado pessoal, dependendo da conjuntura de sua coleta e tratamento.

Não obstante, não raras vezes dados sensíveis ou potencialmente sensíveis são coletados e tratados sem o amparo de uma base legal ou mesmo de maneira ilícita, como através de um consentimento genérico e não destacado para permitir a utilização de um serviço, ou seja, sem informar especificamente a finalidade da coleta e tratamento, de modo a possibilitar o acesso a dados do titular sem maiores restrições. O RGPD, por exemplo, explicita essa preocupação em seu artigo 9.º, afirmando que, embora o consentimento seja essencial no tratamento de dados sensíveis, há exceções cujos procedimentos devem respeitar, com a mesma seriedade e garantia da segurança ao tratamento, os direitos do titular[95].

Na LGPD, a situação não é diferente. O tratamento de dados sensíveis por parte de autônomos, empresas e governo depende do consentimento do titular de dados, consentimento, esse, específico, destacado e para um fim definido, conforme o inciso I do art. 11. No inciso, verifica-se uma exigência adicional em comparação ao consentimento para o tratamento de dados pessoais que não se enquadrem em categorias especiais, qual seja, a necessidade da especificidade e da explicitude da manifestação.

---

[94] Ibid., p. 158.
[95] PINHEIRO, p. 145.

A imposição de uma delimitação formal para a declaração de concordância, que deve se destacar das demais cláusulas contratuais, vai ao encontro do cerne da LGPD, que é proteger os direitos fundamentais de liberdade, de privacidade e de livre desenvolvimento da personalidade da pessoa natural. Sobretudo no que tange à proteção de dados pessoais sensíveis, o papel do destaque da manifestação se mostra necessário por reforçar a compreensão do titular dos dados acerca do significado da sua decisão e das possíveis consequências do compartilhamento dessas informações, tornando-o protagonista no controle do fluxo de seus dados sensíveis e impedindo que algoritmos sejam manejados para enganá-lo durante esse processo. Dessa maneira, o consentimento específico e explícito engloba tanto a protagonização do sujeito, em uma autodefesa contra a violação da privacidade de modo geral, quanto a regulação do controlador, dificultando o emprego de subterfúgios para a obtenção do consentimento. Regina Linden Ruaro e Gabrielle Bezerra Sales Sarlet bem sintetizam:

> Em outras palavras, o consentimento deve ser efetuado nos moldes de um ato jurídico pleno, respeitando a ampliação de uma perspectiva de validade e de perfectibilidade em um panorama em que novos atores, advindos da era informacional, passam a ser cada vez mais corresponsáveis pela criação de um ambiente livre seguro minimamente estável nas fronteiras estabelecidas por sistemas auditáveis, compreensíveis e acessíveis.[96]

Sem o consentimento do titular, em contrapartida, o inciso II do art. 11 dispõe que o tratamento somente será possível nas situações previstas em suas sete alíneas, quais sejam, quando for indispensável: ‘a)’ ao cumprimento de obrigação legal ou regulatória pelo controlador; ‘b)’ à execução de políticas públicas; ‘c)’ à realização de estudos via órgãos de pesquisa; ‘d)’ ao exercício regular de direitos em contratos ou processos; ‘e)’ à proteção da vida ou incolumidade física do titular ou de terceiro; ‘f)’ à tutela da saúde em procedimentos realizados por profissionais da área; ou ‘g)’ à garantia da prevenção à fraude e à segurança do titular.

---

[96] RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/2018. *In*: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.); BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. *E*-book. p. 204.

Nota-se que o termo empregado pelos legisladores em relação às hipóteses de possibilidade de tratamento sem consentimento foi ‘indispensável’, ou seja, resta demonstrada a priorização da obtenção do consentimento e, consequentemente, da participação do indivíduo no fluxo de seus dados sensíveis, ainda que parte da doutrina[97] critique a técnica legislativa e reconheça uma posição de igualdade entre as hipóteses, e não de prevalência do consentimento.

De qualquer sorte, vale lembrar da crítica doutrinária que, acertadamente, considera que a exigência do consentimento acaba por constituir um empecilho para o fluxo de informações entre o titular dos dados e o controlador, sendo insipiente privilegiá-lo a ponto de concentrar toda e qualquer possibilidade de tratamento à mera manifestação de vontade do titular, não raras vezes eminentemente formal e despida dos requisitos adjetivos do inc. XII do art. 5º da Lei. Ruaro e Sarlet[98] também refletem que o enfraquecimento do consentimento como instrumento para a reafirmação da autonomia se dá, acima de tudo, por consequência do grande volume e fluxo de informações no cotidiano, inclusive de rastros digitais gerados independentemente da anuência das pessoas, fatores que elevam a velocidade das transações a níveis exponenciais e comprometem o processo de formação da vontade consciente.

Tanto é assim que a LGPD permite o tratamento de dados sensíveis sem a necessidade de fornecimento de consentimento do titular de dados nas referidas hipóteses, que se referem a interesses públicos e a interesses do próprio titular de dados. No caso dos últimos, o consentimento do titular de dados é dispensado em decorrência de uma ponderação de interesses realizada pela Lei, que considera mais relevantes e preponderantes os interesses de natureza pública frente aos interesses do titular. Tal posicionamento legislativo, no entanto, merece críticas, haja vista que a proteção do conteúdo dos dados pessoais sensíveis é imprescindível justamente para o pleno exercício de direitos fundamentais, como os de igualdade, liberdade e privacidade.[99]

Sejam os dados sensíveis tratados com o consentimento do titular como alicerce, sejam tratados enquadrados nas referidas hipóteses de interesses públicos

[97] VIOLA; TEFFÉ, op. cit., p. 155.
[98] RUARO; SARLET, op. cit., p. 208.
[99] MULHOLLAND, op. cit., p. 52.

e do próprio titular, um ponto comum de análise é a disponibilização pública de tais dados, também podendo esta ser realizada tanto por um terceiro quanto pelo próprio titular.

Inerente à sociedade digital e à economia de dados, a crescente exposição de pessoas e informações na internet impõe o desafio de controlar o compartilhamento de dados pessoais sensíveis ou potencialmente sensíveis, tão essencial para o livre desenvolvimento da personalidade em uma realidade voltada para a vigilância em massa. Como já ressaltado em diversas ocasiões, não se trata de limitar o acesso e uso de dados para impedir o desenvolvimento tecnológico e, consequentemente, o socioeconômico, pois é irrefutável que a transformação digital é inexorável, mas o que cabe é a minimização de possíveis efeitos negativos da exposição indiscriminada de dados, a partir do arcabouço normativo da proteção de dados.

Há, por um lado, o papel da autonomia individual, assentada na noção de empoderamento do indivíduo através da autodeterminação informativa, que reclama uma participação mais ativa e responsável do sujeito de direito em relação à sua exposição virtual, em um exercício de cidadania para controlar a disponibilização de seus dados pessoais sensíveis. De outra parte, há um conjunto de ações a serem realizadas por controladores públicos ou privados de dados de modo a salvaguardar o direito fundamental à privacidade, seja atendendo ao dever de informação aos usuários, seja garantindo-lhes as condições temporais, circunstanciais e informacionais para uma deliberação livre e passível de retratação.

Contudo, tal fluxo ubíquo de dados evidencia a contraposição do direito à privacidade ao direito à informação, especialmente para dados de acesso público. É inconteste que, em razão da disponibilidade pública, nem sempre dados sensíveis são tratados de maneira a salvaguardar os interesses de seu titular, prática que atrai o interesse da proteção de dados, segundo Rafael Mafei Rabelo Queiroz:

> Por isso, mesmo a informação pública (e dificilmente caracterizável com informação protegida pelo direito à privacidade) interessa ao direito à proteção de dados, se relacionar-se a indivíduo identificado ou identificável e for armazenada em bancos de dados ou cadastros, sujeitos a tratamento automatizado ou não. Um exemplo: dados sobre processos judiciais não protegidos por sigilo, disponíveis em diários oficiais eletrônicos gratuitamente acessíveis na internet, não são facilmente enquadráveis sob o manto da

> privacidade. Mas é possível garimpar neles dados sensíveis sobre a saúde de pessoas determinadas, coletando e tratando informações sobre autores de ações contra secretarias de saúde para obtenção de medicamentos e tratamentos não custeados pelo sistema público de saúde. Não se pode dizer que o direito à proteção de dados se limita a 'um aspecto' do direito à privacidade.[100]

Ante todo o exposto, a dúvida que surge é: dados sensíveis ou potencialmente sensíveis que estejam disponíveis publicamente podem ser tratados com base nas hipóteses de dispensa de consentimento dos parágrafos 3º, 4º e 7º do art. 7º, ou o tratamento deve necessariamente se adequar às situações específicas do inciso II do art. 11?

[100] QUEIROZ, Rafael Mafei Rabelo. Direito à privacidade e proteção de dados pessoais: aproximações e distinções. **Revista do Advogado:** Lei Geral de Proteção de Dados Pessoais, n. 144, pp. 15-21, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html>. Acesso em: 21 mar. 2022.

4. A COMPATIBILIZAÇÃO NORMATIVA COMO PONTO DE EQUILÍBRIO PARA O FLUXO INFORMACIONAL

4.1 COMPATIBILIZAÇÃO DA LGPD AO RGPD

A princípio, as bases legais autônomas dos §§ 3º e 4º parecem ser aplicáveis tão somente para o tratamento de dados pessoais do art. 7º, excluindo-se os dados de categorias especiais, como os sensíveis, do alcance normativo das exceções de dispensa de consentimento para tratamento. Depreende-se tal entendimento pela escolha do legislador de desmembrar as hipóteses de tratamento de dados pessoais e as de tratamento de dados pessoais sensíveis em dois artigos (7º e 11), e mais, em seções diferentes do mesmo capítulo, inserindo referidos parágrafos excepcionadores apenas no art. 7º. Porém, vale ressaltar que essa suposta restrição da abrangência de aplicabilidade da dispensa do consentimento gera dúvidas na doutrina[101] e ainda será objeto de confirmação ou não pela Autoridade Nacional de Proteção de Dados (ANPD).

Ademais, verifica-se que, nesse aspecto, a LGPD se afastou da estrutura regulatória do RGPD, porquanto a legislação europeia não prevê em seu texto hipóteses de dispensa de consentimento para tratamento, mas, sim, uma hipótese autorizativa para dados sensíveis tornados manifestamente públicos pelo titular. Especificamente, o RGPD prescreve em seu artigo 9.º, número 2, alínea e), que a proibição ao tratamento de dados sensíveis não se aplica quando o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular.[102]

---

[101] "A despeito disso, restam dúvidas a respeito dos contornos desse dispositivo legal, como: (i) considerando que a regra a respeito da utilização de dados cujo acesso é público está localizada no art. 7º, ela poderá se estender aos dados pessoais sensíveis (cuja base legal de tratamento se encontra no art. 11)? Em caso de resposta negativa, bastaria tratar dados sensíveis com base nas hipóteses legais previstas no art. 11 da LGPD? (...) Essas e outras perguntas relacionadas deverão ser respondidas pela Autoridade de Proteção de Dados Pessoais após a sua efetiva instituição". LANGENEGGER, Natalia; GOBBATO, Andréa. Acesso à Informação com a Lei Geral de Proteção de Dados pessoais: desafios no âmbito do Poder Judiciário. **Revista do Advogado:** Lei Geral de Proteção de Dados Pessoais, n. 144, pp. 141-148, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html>. Acesso em: 21 mar. 2022.

[102] TAVARES, op. cit., pp. 158-159.

Haja vista que essa previsão não acoberta todos os dados sensíveis sob domínio público, apenas os que o próprio indivíduo tornou manifestamente públicos, faz-se necessário um cuidado ainda maior do controlador para não se fiar apenas ao fato de que os dados estão disponíveis publicamente. Ao invocar tal exceção, recai sobre os seus ombros o ônus de provar que os dados sensíveis foram deliberadamente divulgados pelo seu titular, excluindo-se, assim, dados vazados ou acessíveis após uma falha de segurança, ilegalmente tornados públicos, e até mesmo dados compartilhados não intencionalmente pelo titular.[103]

A princípio, a exceção parece lógica e razoável, muito em razão do ato de publicização dos dados possuir uma presunção de manifestação deliberada de consentimento para o tratamento por terceiros. Todavia, não se trata de uma presunção *juris tantum*, pois não se pode negligenciar o contexto da publicização dos dados para a verificação de sua manifesta intencionalidade ou não, e, por consequência, da legitimidade ou não do tratamento, mormente no que tange a dados sensíveis.

O *Information Commissioner's Office* (ICO), autoridade britânica responsável pela proteção de dados, apresenta algumas questões a serem respondidas para se verificar se determinado dado pessoal de categoria especial pode ser considerado como tendo sido tornado manifestamente público por seu titular: O dado de categoria especial já está sob domínio público – pode um membro do público realisticamente acessá-lo, na prática? Quem tornou o dado público – foi o próprio indivíduo ou foi outra pessoa? Em que contexto foi tornado público – por exemplo, foi por ele ter dado uma entrevista, por ter concorrido a um cargo público, por ter escrito um livro, blog ou uma publicação em rede social? O indivíduo deliberadamente seguiu os passos para tornar esse dado de categoria especial público, ou foi acidental ou não intencional? Ele tomou uma decisão clara? É provável que o indivíduo tenha entendido que sua ação significa que seu dado de categoria especial está sob domínio público?[104]

---

[103] GRATTON, Louis-Philippe. Article 9 GDPR. Processing of special categories of personal data. **GDPR Text**. Disponível em: <https://gdpr-text.com/read/article-9/>. Acesso em: 29 mar. 2022.

[104] "So to use this condition, you should consider some specific questions: Is the special category data already in the public domain – can a member of the public realistically access it in practice? Who made the data public – was it the individual themselves or was it someone else? In what context was it made public – for example was it due to them giving an interview, standing for public office, or writing a book, blog or social media post? Did the individual deliberately take the steps which made this special category data public, or was it accidental or unintentional? Did they make a clear decision? Is the individual likely

É notório que um autor que escreve um livro narrando suas experiências sexuais ou revelando detalhes sobre sua saúde voluntariamente dispõe de seus dados, assim como uma publicação sobre os mesmos assuntos em seu blog também pode ser considerada um compartilhamento com o público. Uma publicação em uma rede social, por outro lado, pode não ser tão fácil de qualificar como tornada pública, pois, se foi feita para ser compartilhada entre seu círculo de amigos e família, tais dados não são acessíveis ao público em geral e dificilmente serão considerados públicos na acepção estrita[105] que exige a exceção.[106]

As Diretrizes 8/2020 sobre o direcionamento para os utilizadores das redes sociais, adotadas em 2 de setembro de 2020 pelo Comité Europeu de Proteção de Dados (CEPD), elencam elementos para facilitar uma avaliação caso a caso, ressalvando que a observância de apenas um elemento nem sempre será suficiente para que os dados sejam considerados como tornados manifestamente públicos, pois a palavra 'manifestamente' estabelece um patamar elevado para o recurso à exceção[107]. Veja-se:

> i) as predefinições da plataforma de redes sociais (ou seja, se o titular dos dados efetuou uma ação específica para alterar estas predefinições de privadas para públicas), ou
> ii) a natureza da plataforma de redes sociais (ou seja, se esta plataforma está intrinsecamente associada ao conceito de ligação a pessoas próximas do titular dos dados ou de criação de relações íntimas [tais como as plataformas de encontros em linha], ou se se destina a proporcionar um âmbito mais vasto de relações interpessoais, como relações profissionais, ou microblogues, partilha de conteúdos multimédia, plataformas de redes sociais para a partilha de críticas em linha, etc.), ou

---

to have understood that their action means that their special category data is in the public domain?" INFORMATION COMMISSIONER'S OFFICE. What are the conditions for processing? Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/5>. Acesso em: 20 mar. 2022.

105 "No seu Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (WP 258, 29 de novembro de 2017, p. 11), o Grupo de Trabalho do Artigo 29.º clarificou que a expressão «manifestamente tornados públicos pelo seu titular» tem de ser interpretada de modo a implicar que o titular está ciente de que os seus dados serão disponibilizados ao público, o que significa a todos, incluindo às autoridades. Por conseguinte, «[e]m caso de dúvida, deve fazer-se uma interpretação restrita [...]»". COMITÉ EUROPEU DE PROTEÇÃO DE DADOS. **Diretrizes 8/2020 sobre o direcionamento para os utilizadores das redes sociais**. p. 29. Disponível em: <https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_pt_0.pdf> Acesso em: 30 mar. 2022.

106 GRATTON, op. cit.

107 COMITÉ EUROPEU DE PROTEÇÃO DE DADOS, op. cit., pp. 40-41.

> iii) a acessibilidade da página onde os dados sensíveis são publicados (ou seja, se a informação está acessível ao público ou se, por exemplo, é necessária a criação de uma conta antes de aceder às informações), ou
> iv) a visibilidade das informações através das quais o titular dos dados é informado da natureza pública das informações que publica (ou seja, se existe, por exemplo, uma faixa contínua na página, ou se o botão para confirmar a publicação informa o titular dos dados de que as informações serão tornadas públicas, etc.), ou
> v) se foi o próprio titular a publicar os dados sensíveis, ou se os dados foram publicados por terceiros (por exemplo, uma fotografia que revela dados sensíveis publicada por um amigo) ou inferidos.[108]

Para melhor compreensão da imprescindibilidade da ponderação das circunstâncias de cada caso específico ao avaliar se os dados foram manifestamente tornados públicos pelo seu titular, bem como da possível necessidade de combinação de mais de um elemento para que possa haver a aferição objetiva da intenção do indivíduo, lança-se mão do exemplo constante das próprias Diretrizes, qual seja:

> O Sr. Jansen criou uma conta numa plataforma de redes sociais dedicada a microblogues. Ao preencher o seu perfil, indicou que é homossexual. Por ser conservador, optou por aderir a grupos conservadores. Quando se registou, foi informado de que as mensagens que trocar na plataforma são públicas. Um partido político conservador pretende efetuar o direcionamento a pessoas que partilham a mesma filiação política e a mesma orientação sexual que o Sr. Jansen, utilizando as ferramentas de direcionamento das redes sociais.[109]

In casu, dois dados sensíveis do Sr. Jansen foram coletados pela plataforma de redes sociais: sua orientação sexual e sua filiação política. Como a orientação sexual dos usuários é privada por predefinição da plataforma e o Sr. Jansen nada fez para publicá-la, não se pode considerar que foi manifestamente tornada pública. *A contrario sensu*, a sua filiação política também não, a despeito da natureza da plataforma de rede sociais de microblogues, destinada a compartilhar informações com o público em geral, e do fato de ter sido informado da natureza pública das mensagens que publicasse. Isso porque, embora tenha entrado em fóruns públicos sobre conservadorismo, foi a plataforma que deduziu sua filiação política, e não o próprio Sr. Jansen a informá-la, carecendo a intenção específica do titular de tornar o dado manifestamente público, especialmente tendo em mente que a dedução pode se revelar falsa. Portanto, o Sr. Jansen não pode ser objeto de direcionamento com base em nenhum dos dois dados sensíveis coletados.[110]

---

[108] Ibid.
[109] Ibid.
[110] "Como a orientação sexual dos membros é «privada» por defeito e o Sr. Jansen não efetuou qualquer ação para a tornar pública, não pode considerar-se que foi manifestamente tornada pública. Além disso, os dados relativos à sua filiação política não foram manifestamente tornados públicos, apesar i) da

Indo além, e só a título exemplificativo, a autoridade de proteção de dados norueguesa (*Datatilsynet*) multou a empresa Grindr LLC em 6,5 milhões de euros após tomar conhecimento do compartilhamento indevido de dados dos usuários para fins de marketing[111]. A partir dos dados, que incluíam a localização via sistema de posicionamento global (*Global Positioning System – GPS*), endereço de protocolo da internet (*Internet Protocol – IP*), idade, gênero e o fato do usuário fazer uso do aplicativo, empresas de marketing eram capazes de identificar os usuários quando do tratamento, podendo, inclusive, compartilhar os dados com terceiros.

A autoridade considerou que o uso de um aplicativo de relacionamento gay não configura a ação de tornar manifestamente público o dado sensível sobre a orientação sexual do indivíduo, porquanto tal dado somente é visível para outros membros da comunidade, e mais, somente para usuários que também possuam uma conta no aplicativo, ainda que anônima, vide o elemento 'iii' das Diretrizes. Logo, a base legal teria de ser o consentimento, não a hipótese autorizativa para dados sensíveis tornados manifestamente públicos.[112]

Observa-se que a chave para a avaliação da legitimidade ou não do tratamento de dados pessoais de categorias especiais tornados manifestamente públicos encontra-se na finalidade da disponibilização de tais dados, ou, em outras palavras, na expectativa legítima de quem os publicizou, à luz do referencial da privacidade contextual. Não obstante a privacidade contextual se alicerce na confiança depositada na outra pessoa ou na relação, é, também, a partir do contexto da disponibilização dos dados que se extrai, de modo objetivo, que uso legítimo pode ser esperado por uma

---

natureza da plataforma de redes sociais dedicada a microblogues, que se destina a partilhar informações com o público em geral, e ii) do facto de ter sido informado da natureza pública das mensagens que publica nos fóruns. Além disso, embora tenha aderido a fóruns públicos relacionados com o conservadorismo, não pode ser objeto de direcionamento com base nestes dados sensíveis, uma vez que foi a plataforma de redes sociais a efetuar uma dedução sobre a filiação política do Sr. Janssen e que o titular dos dados não tinha a intenção específica de tornar estes dados manifestamente públicos, tanto mais que esta dedução pode revelar-se falsa. Por conseguinte, não pode ser objeto de direcionamento com base em dados relativos à filiação política. Por outras palavras, é necessário ter em conta as circunstâncias em cada caso específico ao avaliar se os dados foram manifestamente tornados públicos pelo seu titular". Ibid.

[111] Intention to issue € 10 million fine to Grindr LLC. **Datatilsynet**. Oslo, 26 jan. 2021. Disponível em: <https://www.datatilsynet.no/en/news/2021/intention-to-issue--10-million-fine-to-grindr-llc2/>. Acesso em: 29 mar. 2022.

[112] Article 9 GDPR. **GDPR Hub**. Disponível em: <https://gdprhub.eu/index.php?title=Article_9_GDPR>. Acesso em: 29 mar. 2022.

pessoa razoável na mesma situação, devendo a finalidade do tratamento corresponder a essa expectativa.

A partir de uma análise sistemática da LGPD brasileira, nota-se que também no País há uma preocupação com o respeito à privacidade contextual, consubstanciada, em alguns casos, em verdadeiras bases legais autônomas de tratamento, como as aplicáveis para dados pessoais disponíveis publicamente.

Cabe destacar, aqui, a diferenciação crucial entre os parágrafos 3º e 4º do art. 7º e o parágrafo 7º do mesmo artigo. Enquanto os primeiros disciplinam o tratamento equivalente dos dados, seja ele primário, seja secundário, o último dispõe sobre o tratamento posterior compatível dos dados.[113]

Denomina-se tratamento equivalente qualquer tratamento cuja finalidade seja idêntica àquela que justificou a disponibilização dos dados. Logo, quanto ao tratamento de dados de acesso público, vê-se que um terceiro coleta e posteriormente disponibiliza os dados, em virtude de uma obrigação legal de publicidade, mas somente após o tratamento primário pelo terceiro é que os dados são publicizados e se tornam disponíveis publicamente, tratando a hipótese do § 3º, portanto, de um tratamento secundário equivalente. Já no caso de dados tornados manifestamente públicos, não houve tratamento anterior porque o próprio titular os disponibilizou, então a hipótese do § 4º se refere a um tratamento primário equivalente.[114]

O tratamento posterior compatível, por sua vez, se dá para uma nova finalidade, diversa daquela que justificou a publicização das informações, mas ainda compatível à original, enquadrando-se no § 7º do art. 7º. Essa hipótese autorizativa de tratamento pode ser utilizada tanto para dados de acesso público quanto para dados tornados manifestamente públicos, quando não for caso de tratamento equivalente.

Para identificar a base legal autônoma mais adequada ao tratamento de dados pessoais disponíveis publicamente, Giovanna Milanez Tavares propõe uma análise de três níveis: (i) identidade de finalidades: se a finalidade do tratamento for a mesma

[113] TAVARES, op. cit., p. 93.
[114] Ibid., p. 93.

que justificou a disponibilização, bem como se os outros requisitos dos §§ forem cumpridos, o tratamento poderá ser enquadrado nas bases legais autônomas de tratamento equivalente dos §§ 3º ou 4º do art. 7º; (ii) compatibilidade de finalidades: se a finalidade for diversa, mas for compatível com a que justificou a disponibilização, bem como se os outros requisitos do § forem cumpridos, o tratamento poderá ser enquadrado na hipótese de tratamento posterior compatível do § 7º do art. 7º; (iii) possibilidade de enquadramento em outra base legal para o tratamento de dados pessoais: se a finalidade for diversa e não for compatível com a que justificou a disponibilização, o tratamento deverá ser enquadrado em uma das outras bases legais dispostas nos incisos do art. 7º, para que a finalidade seja verdadeiramente legítima à luz da LGPD[115]. Por fim, se o tratamento não puder ser enquadrado em nenhuma base legal, será incompatível com a finalidade da disponibilização e, consequentemente, ilegítimo.

Assim, conclui-se que as bases legais autônomas dos §§ 3º e 4º somente permitem o tratamento de dados pessoais sem a necessidade de amparo em outra base legal porque devem ser observados todos os requisitos presentes em ambos os parágrafos, mormente a identidade de finalidades do tratamento e da disponibilização, mas também, no caso de dados de acesso público, o tratamento à luz do princípio da boa-fé e do interesse público que justificou a disponibilização do dado pessoal publicamente, e, no caso de dados tornados manifestamente públicos, dos direitos do titular e dos princípios da LGPD.

Especificamente no que se refere a dados de acesso público, é fundamental extrair a finalidade que justificou a publicização do dado pessoal, que sempre está intrinsecamente ligada ao motivo de sua coleta, para que o controlador valore a razoabilidade e a licitude da finalidade específica de eventual tratamento. Quando este for viável, não há falar de dever de informação ao titular acerca do tratamento secundário do dado, pois a finalidade já foi explicitada pelo primeiro agente de tratamento, quando da coleta para posterior disponibilização. Vale lembrar que isso somente será possível quando o tratamento secundário for equivalente ao original, ou seja, a finalidade da disponibilização e do tratamento equivalente deve necessariamente ser a mesma, pois presume-se que dela o titular do dado já foi

[115] Ibid., pp. 156-157.

cientificado anteriormente, e, assim, já sabe o que esperar de tratamentos posteriores.[116]

Não é diferente o fundamento para o requisito da identidade de finalidades para o tratamento equivalente de dados tornados manifestamente públicos pelo titular. A dispensa da exigência do consentimento para o tratamento equivalente se justifica na manutenção da finalidade que levou o titular a publicizar seus dados, razão pela qual, novamente, impõe-se a análise do contexto, ainda que não haja como confirmar, de maneira segura, a finalidade específica que motivou a disponibilização[117]. Para tanto, faz-se necessário que o agente de tratamento delimite, interpretativamente, a esfera razoável de utilização dos dados, a partir da aparente finalidade da publicização que pode ser extraída do contexto, para que possa inferir a expectativa legítima do titular em relação a eventual tratamento dos dados[118].

A hipótese autorizativa do § 7º do art. 7º, de outra banda, impõe uma série ainda maior de requisitos para que o tratamento seja conferido de legitimidade, pois não mais restrito à identidade da finalidade da disponibilização. Para tanto, devem ser observados os propósitos legítimos e específicos do novo tratamento, os fundamentos e princípios da Lei e a preservação dos direitos do titular. Em outras palavras, impõe-se a avaliação de compatibilidade das finalidades e a manutenção das garantias legais.[119]

Os propósitos legítimos e específicos para o novo tratamento nada mais são do que finalidades de tratamento que estejam de acordo com a Lei e cujos objetivos sejam definidos. A legitimidade da finalidade decorre da conformidade não somente com a LGPD, mas com o ordenamento jurídico como um todo, podendo, também, atrair a incidência de outras normas protetivas, como a LAI ou o MCI. Já sua especificidade deve ser suficiente para delimitar quais dados serão tratados, bem como seu uso posterior, de modo que o agente de tratamento condiciona sua própria conformidade legal ao delimitar quais operações de tratamento podem ser realizadas. Além de garantir previsibilidade ao titular acerca do tratamento, a suficiente

[116] Ibid., pp. 113-115.
[117] Ibid., pp. 134-135.
[118] Ibid., pp. 145-146.
[119] Ibid., p. 194.

especificidade ainda facilita a própria avaliação de compatibilidade da finalidade do tratamento posterior.[120]

Assim, percebe-se a necessidade de observância de um terceiro requisito para que a finalidade seja passível de enquadramento no § 7º, ainda que tal requisito não esteja expressamente previsto no parágrafo. A compatibilidade da finalidade do tratamento posterior à finalidade original, que justificou a publicização dos dados, é o que assegura que a hipótese autorizativa não seja um cheque em branco para o tratamento para finalidades incompatíveis, permitindo, então, a reutilização dos dados sem que o titular perca o controle sobre os usos que lhes são dados, tal como já ocorre na Europa.

Consoante bem esclarece Indra Spiecker gen. Döhmann, através da leitura combinada do artigo 5.º, n.º 1, b)[121], e do artigo 6.º, n.º 4[122], ambos do RGPD, infere-se que nem toda nova finalidade de tratamento exige uma nova justificativa, permanecendo o tratamento de dados para uma nova finalidade coberto pela justificativa do tratamento original de dados se a nova finalidade for compatível (*compliant*) com a finalidade original[123]. Para a avaliação de compatibilidade, deve-se recorrer, entre outros, aos quatro fatores-chave enumerados no Parecer 3/2013 sobre limitação da finalidade, do Grupo de Trabalho de Protecção de Dados do Artigo 29.º: a) a relação entre as finalidades para as quais os dados foram recolhidos e as

---

[120] Ibid., pp. 195-197.

[121] Artigo 5.º Princípios relativos ao tratamento de dados pessoais 1. Os dados pessoais são: (...) b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»).

[122] Artigo 6.º Licitude do tratamento 4. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta: a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior; b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento; c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.o, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º; d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados; e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

[123] DÖHMANN, op. cit., p. 106.

finalidades do tratamento posterior; b) o contexto no qual os dados foram recolhidos e as expectativas razoáveis das pessoas em causa quanto à sua utilização posterior; c) a natureza dos dados e o impacto do tratamento posterior sobre as pessoas em causa; d) as garantias aplicadas pelo responsável pelo tratamento para assegurar um tratamento leal e para impedir quaisquer impactos indevidos sobre as pessoas em causa[124].

Ou seja, evidente que, nem na Europa, nem no Brasil, os princípios da limitação das finalidades e da minimização dos dados (adequação) são impeditivos para o fluxo informacional. Pelo contrário, a ponderação acerca da equivalência ou da compatibilidade das finalidades permite, inclusive, o tratamento de dados disponíveis publicamente sem o recurso a outra base legal elencada no artigo 6.º do RGPD ou no art. 7º da LGPD.

Constatando-se que o propósito específico do tratamento posterior já fora implicado na finalidade original, ou sendo um passo lógico seguinte em virtude de uma conexão entre eles, não cabe a fundamentação do tratamento em outra base legal. Logo, quanto maior o afastamento entre a finalidade da publicização e a finalidade do tratamento posterior, menores as chances de ser considerado legítimo o tratamento.

O mesmo raciocínio se aplica para a expectativa legítima do titular, uma vez que, quanto mais inesperada for a nova utilização, menor a probabilidade de que o titular tivesse consciência de tal possibilidade de uso de seus dados. Para que não se caia no subjetivismo de ter de conjecturar cada consequência que determinado indivíduo possa ter considerado ao publicar ou ter seus dados publicados, impõe-se uma ponderação objetiva do que poderia ser esperado em contextos idênticos ou semelhantes.

Não se pode olvidar, no entanto, da identificação dos riscos e da análise do impacto para os indivíduos a quem os dados se referem, bem como de eventuais garantias adotadas para prevenir consequências negativas. Isso porque diferentes

---

[124] GRUPO DE TRABALHO DE PROTECÇÃO DE DADOS DO ARTIGO 29.º. **Parecer 3/2013 sobre limitação da finalidade (WP 203, 2 de abril de 2013)**. Disponível em: <https://www.gpdp.gov.mo/uploadfile/2017/0127/20170127113421380.pdf>. Acesso em: 8 abr. 2022. pp. 29-34.

naturezas de dados, como os sensíveis, podem restringir ainda mais a possibilidade do tratamento ser considerado compatível.

Portanto, a solução encontrada pelos legisladores para proteger dados disponíveis publicamente foi a restrição de tratamento para as finalidades englobadas pelo contexto original, de maneira a proteger as expectativas legítimas do titular que publicizou ou teve publicizados seus dados. No Brasil, esse entendimento a favor da limitação da finalidade do tratamento de dados pessoais disponíveis publicamente pode e deve ser reproduzido no âmbito do tratamento de dados sensíveis disponíveis publicamente, mormente em razão da natureza dúplice e, à primeira vista, dicotômica de tais dados.

4.2 COMPATIBILIZAÇÃO DAS BASES LEGAIS DA LGPD

A exigência de maior proteção pela sensibilidade e pelo potencial danoso dos dados contrasta com a disponibilidade pública e a facilidade de deles fazer uso, e a solução não é privilegiar uma dessas características em detrimento da outra, mas buscar seu meio-termo. Isso porque é inegável a disponibilização pública em massa de dados pessoais sensíveis, e a ausência de uma regulamentação específica quanto à dispensa ou não do consentimento do titular para o tratamento desses dados expõe a necessidade de se conferir segurança jurídica tanto para o titular quanto para o controlador.

Considerando a potencial sensibilidade de qualquer dado pessoal, mostra-se temerário limitar a possibilidade de tratamento de todos os dados pessoais disponíveis publicamente à “trava do consentimento” do titular ou às restritivas hipóteses do inc. II do art. 11, especialmente considerando que seu § 1º dispõe que tais regras especiais se aplicam a qualquer tratamento que possa revelar dados sensíveis, ou seja, sendo uma norma aberta com potencial de albergar grande parte dos dados pessoais, facilmente relacionáveis entre si e ao seu titular. Segundo Bioni, a incumbência ao titular do ônus de seguir seus dados em todos os seus movimentos prejudica a dinamicidade das relações sociais e a própria economia dos dados, na medida em que a “trava do consentimento” bloqueia a todo momento o fluxo dos dados pessoais e ainda leva o cidadão à chamada “fadiga do consentimento”, que nada mais é do que

a sobrecarga de solicitações de consentimento para o tratamento de seus dados pessoais[125].

Tanto assim que essa foi a justificação para a inclusão do § 7º no art. 7º da LGPD. O então Deputado Eduardo Barbosa, através da Emenda Aditiva nº 112 à Medida Provisória nº 869/2018, argumentou que diversas atividades legítimas são baseadas no tratamento de dados oriundos de fontes publicamente acessíveis, em que os dados pessoais não foram coletados perante o titular, não podendo atividades essenciais ao desenvolvimento da sociedade serem inviabilizadas por uma restrição ao uso desses dados, *in verbis*:

> "Independentemente disso, é preciso compreender a importância de atividades de tratamento de dados que são realizadas a partir dessas fontes publicamente acessíveis. Na medida em que o dado tenha acesso irrestrito a qualquer pessoa, física ou jurídica, ou seja, quando ele é publicamente acessível, o dado pessoal passa a ser um importante elemento para a realização de análises e estudos que podem otimizar e desenvolver setores e atividades inteiros na sociedade, reduzindo custos, racionalizado o processo de tomada de decisões, maximizando resultados, e, assim, promovendo competitividade, inovação, empregabilidade, qualidade de vida e prosperidade. (...) No entanto, as situações em que o tratamento dos dados ocorra a partir de acesso público ou por ter sido tornado publicamente acessível pelo titular são muitas. São circunstâncias em que o dado pessoal não foi coletado junto ao titular, o que exige um olhar mais atento do legislador a fim de não inviabilizar atividades legítimas baseadas nesse tipo de tratamento".

Assim, a dispensa da exigência do consentimento do titular para o tratamento de dados que já estejam sob domínio público, consagrada nos §§ 3º, 4º e 7º do art. 7º da LGPD, surge como uma alternativa também para dados sensíveis disponíveis publicamente.

A elasticidade da privacidade contextual se mostra útil para governar usos que não podem ser previamente especificados e controlados de maneira rígida[126], haja vista que o próprio contexto e os critérios de aferição de integridade dele decorrentes restringem o fluxo de dados ao longo da vida útil destes. O consentimento, aqui, é substituído por uma proteção *ex ante* intrínseca aos dados, sem usurpar do titular a possibilidade do exercício *a posteriori* de seus direitos.

---

[125] BIONI, 2021, pp. 227-228.
[126] Ibid., p. 231.

Não é por outro motivo que a parte final de todos os parágrafos relaciona condições específicas a serem observadas pelo agente de tratamento. Como bases autônomas, os parágrafos foram desenhados especificamente para garantir a dados disponíveis publicamente, irrelevante se sensíveis ou não, o nível semelhante de proteção de dados tratados com fundamento no consentimento ou em outras bases legais.

Destarte, mostram-se os parágrafos mais adequados para salvaguardar dados disponíveis publicamente do que qualquer outra hipótese de tratamento[127] de dados pessoais ou de dados pessoais sensíveis, haja vista que as outras bases legais não foram idealizadas com a prévia publicização dos dados em mente, o que, ao mesmo tempo que inviabiliza muitos tratamentos, exacerba o risco dos restantes, que não se encaixam ao atributo público dos dados e podem ser explorados sem o cumprimento das garantias adicionais prescritas pelos parágrafos.

Embasando-se o tratamento nas hipóteses adequadas, o risco de uso discriminatório de dados sensíveis é mitigado porquanto os próprios parágrafos limitam o tratamento dos dados apenas às finalidades compatíveis com a sua disponibilização, seja por terceiros, seja pelo próprio titular. Em outras palavras, dados sensíveis disponíveis publicamente devem passar pela mesma avaliação de identidade ou compatibilidade de finalidades prevista para dados pessoais também disponíveis publicamente, fazendo-se necessário, para tanto, o reconhecimento da possibilidade de integração do regime normativo para o tratamento de dados sensíveis às disposições dos §§ 3º, 4º e 7º do art. 7º da LGPD.

A extensão do alcance normativo das bases legais autônomas para tratamento de dados pessoais disponíveis publicamente encontra respaldo na semelhança à já analisada hipótese autorizativa do artigo 9.º, n.º 2, alínea e) do RGPD, que estende a flexibilidade da disciplina do tratamento de dados pessoais disponíveis publicamente ao tratamento de dados pessoais de categorias especiais quando tornados manifestamente públicos. Porém, ainda que essa hipótese autorizativa genérica do RGPD não deixe de garantir a proteção dos dados pessoais sensíveis através da exigência da análise do contexto de disponibilização, também não abarca dados de

[127] TAVARES, op. cit., p. 155.

acesso público disponibilizados por terceiros, e nem restringe a finalidade do tratamento uma vez que se confirme que os dados sensíveis tenham sido manifestamente tornados públicos pelo titular.

Em contrapartida, a LGPD vai além da hipótese de tratamento de dados pessoais sensíveis tornados manifestamente públicos e permite que dados pessoais sensíveis de acesso público também sejam enquadrados nas bases legais autônomas dos referidos parágrafos. A aplicação desse diferencial em relação ao RGPD somente é possível pelo balizamento exercido pelos próprios §§ 3º, 4º e 7º no que tange à finalidade do tratamento, que deve ser, quando não idêntica, ao menos compatível à finalidade da disponibilização dos dados.

Desse modo, a inclusão de dados sensíveis de acesso público nas hipóteses autorizativas dos §§ 3º e 7º dinamiza ainda mais o fluxo de dados, especialmente para agentes de tratamento que legitimamente fazem uso de bancos de dados para tratamento em massa, pois diversas atividades econômicas dependem de dados obtidos de fontes públicas, razão pela qual não é razoável a inviabilização dessas atividades apenas pela constatação da presença de dados sensíveis nos bancos de dados. Vê-se, aqui, que não se trata de permitir o uso indiscriminado de dados sensíveis, pois a adstrição à finalidade da disponibilização dos dados sensíveis nada mais é do que um controle indireto exercido pelo titular ou pelo terceiro responsável pela publicização.

Tudo sem deixar de lado o controle direto, ou seja, os direitos do titular dos dados sensíveis, haja vista que, ainda que a determinação de sua observância não esteja expressamente prevista no § 3º, em decorrência da opção legislativa pela primazia do interesse público, os demais requisitos para tal hipótese de tratamento equivalente não deixam de ser considerados. Por outro lado, para o tratamento posterior do § 7º, é explícita e imperiosa a obediência aos direitos previstos entre os arts. 17 e 22 da LGPD, especialmente à possibilidade de exercício das prerrogativas dispostas no art. 18.

Vale recordar que, com fulcro no § 2º do art. 18, há a previsão do direito de oposição do titular a qualquer tratamento fundamentado em uma das hipóteses de

dispensa de consentimento, desde que realizado em descumprimento ao disposto na Lei. Trata-se de um dispositivo de proteção *ex post* que deve ser exercida pelo próprio titular, complementando a proteção *ex ante* da LGPD e reforçando a carga participativa do titular no fluxo de seus dados. Logo, estendendo-se o efeito normativo de tal disposição também para os dados sensíveis e potencialmente sensíveis, resta cristalino o fato de que pode haver a oposição do titular ao uso indevido desses dados ainda que não haja falar de consentimento ao tratamento, pois já disponíveis publicamente e protegidos pela privacidade contextual.

Entretanto, o controle direto viabilizado pelo direito de oposição não pode ser confundido com uma manifestação de consentimento *a posteriori*, ainda que seja uma forma de autodeterminação informativa do titular dos dados. Ocorre que a manifestação de oposição não possui o condão de fazer cessar o tratamento de dados, salvo se ilícito o tratamento, de sorte que cabe ao agente de tratamento sopesar os argumentos apresentados pelo titular por meio de uma nova avaliação dos interesses e dos direitos envolvidos, tendo em vista que a expectativa legítima do titular pode ter sido extrapolada. Em outras palavras, não há uma contradição entre a avaliação de compatibilidade do tratamento e o direito de oposição, mas, sim, uma complementação daquela com este.

Em suma, é inegável que o balizamento de finalidades desempenhado pelas bases legais autônomas dos §§ 3º, 4º e 7º do art. 7º não deixa de garantir a observância tanto dos direitos do titular quanto dos fundamentos e princípios da LGPD, razão pela qual se torna possível sua aplicação também para dados sensíveis, quando disponíveis publicamente. Quanto mais sensíveis os dados, mais restritas serão as finalidades, ressalvando-se que, incompatíveis as finalidades da disponibilização e do tratamento, este deve ser amparado por uma das bases legais próprias do art. 11, sob pena de carecer de legitimidade e incorrer nas sanções da LGPD.

Cai por terra o argumento de que referidas hipóteses autorizativas seriam um cheque em branco para o agente de tratamento, impondo-se o reconhecimento de que nada mais são do que uma válvula de escape tanto à “fadiga do consentimento” quanto à “trava do consentimento”, garantindo a LGPD flexibilidade e segurança em

uma sociedade cada vez mais baseada em dados, cuja velocidade o ordenamento jurídico não é capaz de acompanhar[128]. Por consequência, confirma-se a tese de que autodeterminação informacional vai além do consentimento, pois o cidadão também exerce domínio sobre seus dados se forem tratados de acordo com suas legítimas expectativas[129], evitando-se, de um lado, a elevação da privacidade a um valor intransacionável[130], e, de outro, que a disponibilização pública dos dados sensíveis seja uma carta branca para tratamentos discriminatórios.

Ante todo o exposto, no Brasil, tem-se que as bases legais autônomas dos §§ 3º e 4º do art. 7º podem ambas ser manejadas para o tratamento de dados pessoais sensíveis ou potencialmente sensíveis, em razão de sua restrição à idêntica finalidade da disponibilização, seja por terceiros, no caso de dados de acesso público, seja pelo titular, em relação a dados manifestamente tornados públicos. Na mesma lógica, pode-se cogitar a aplicação do § 7º para casos de finalidades que não são idênticas, mas compatíveis, de modo que resta mantida a vedação da LGPD a qualquer tratamento com finalidade incompatível à natureza dos dados sensíveis.

[128] TAVARES, op. cit., p. 212.
[129] BIONI, 2021, p. 276.
[130] AZEVEDO, Ricardo. O legítimo interesse e a legítima expectativa do titular dos dados pessoais. *In*: OLIVEIRA, Ricardo (coord.); COTS, Márcio (coord.). **O Legítimo interesse e a LGPDP**. 2. ed. São Paulo: Thomson Reuters Brasil, 2021. *E-book*. RB-3.1.

5. CONSIDERAÇÕES FINAIS

O presente trabalho buscou examinar a natureza dúplice de dados pessoais sensíveis disponíveis publicamente e a consequente possibilidade de enquadramento em mais de uma base legal de tratamento prevista na LGPD, aprofundando a pesquisa sobre as duas características para então ponderar qual seria a hipótese autorizativa mais adequada para essa categoria especial de dados.

Com uma economia cada vez mais neles baseada, é de suma importância que o Direito dote de segurança jurídica a matéria de proteção de dados, ainda que não seja capaz de acompanhar a velocidade das mudanças da sociedade da informação. Para tanto, não se pode dar-se ao luxo de impedir o tratamento de dados pessoais, nem mesmo de dados pessoais sensíveis, pois essenciais para viabilizar o regular exercício de diversas políticas públicas e atividades privadas. É dessa busca pelo equilíbrio regulatório que decorre o dilema entre flexibilizar e restringir o tratamento de dados em determinadas situações, e também a razão de ser da presente pesquisa.

Dicotômicos, à primeira vista, os atributos da sensibilidade e da publicidade possuem disciplinas próprias na LGPD, sendo as disposições acerca do tratamento de dados pessoais sensíveis no art. 11 mais restritivas do que as concernentes a dados pessoais disponíveis publicamente no art. 7º. Entretanto, de uma análise sistemática da Lei, percebe-se que os dispositivos são, na verdade, complementares.

Enquanto o tratamento de dados pessoais sensíveis é, *a priori*, restrito ao consentimento ou a uma das limitadas hipóteses do inc. II do art. 11, o tratamento de dados pessoais disponíveis publicamente é regido por três parágrafos abertos, não prevendo os §§ 3º, 4º e 7º do art. 7º situações específicas de autorização para o tratamento, mas, sim, fundamentos, princípios e direitos a serem observados, sendo o principal deles o princípio da finalidade, que veda o tratamento incompatível à finalidade da disponibilização dos dados.

Portanto, ao mesmo tempo que a maleabilidade dos referidos parágrafos permite a compatibilização de seus efeitos normativos com a mais restritiva disciplina de dados pessoais sensíveis, a limitação das finalidades do tratamento à identidade

ou à compatibilidade com a finalidade de disponibilização salvaguarda a contextualização da publicização dos dados pessoais sensíveis disponíveis publicamente e assegura que estes não serão tratados com a extrapolação da expectativa legítima que havia quando da publicização dos dados pelo titular ou por terceiros.

Tal observação é corroborada pela análise comparativa da LGPD com o RGPD, haja vista que, no diploma legal europeu, há uma exceção genérica que permite o tratamento de dados pessoais sensíveis quando manifestamente tornados públicos pelo titular. Entretanto, ainda que a carga principiológica do RGPD se aplique para qualquer tratamento abarcado pelo Regulamento, reconhece-se que não há uma limitação do tratamento à finalidade da disponibilização dos dados pessoais sensíveis pelo titular, como há na LGPD, deficiência que suscita dúvidas quanto à margem para um tratamento cuja finalidade não é compatível à expectativa legítima do titular quando da disponibilização, amparado apenas pelo fato de que o titular publicizou, conscientemente, seus dados pessoais sensíveis.

Considerando a possibilidade de compatibilização, no âmbito da LGPD, da ideia europeia da especialidade da publicidade em relação à sensibilidade, tem-se que, além de dados pessoais sensíveis tornados manifestamente públicos pelo titular, a limitação da finalidade presente na Lei brasileira garante a segurança do tratamento também de dados pessoais sensíveis de acesso público, ao contrário do RGPD, na medida em que a Lei restringe o tratamento à identidade ou à compatibilidade com a finalidade da publicização dos dados, caso dos §§ 3º e 4º ou § 7º do art. 7º da LGPD, respectivamente, salvaguardando a expectativa legítima do titular e vedando o tratamento incompatível de seus dados.

Conclui-se, então, que o arcabouço normativo do tratamento de dados pessoais disponíveis publicamente é mais protetivo para dados pessoais sensíveis, quando também disponíveis publicamente, em razão de sua construção com a publicização prévia dos dados em mente, em contraste com as hipóteses do art. 11, que não conferem semelhante proteção para dados pessoais sensíveis já ao alcance do público. Portanto, os §§ 3º, 4º e 7º do art. 7º da LGPD são aptos não somente para operacionalizar o tratamento de dados pessoais sensíveis disponíveis publicamente,

mas também para manter inalteradas as garantias do titular, que exerce um controle indireto de tratamentos futuros através do contexto da publicização, garantindo, assim, um dos principais objetivos da Lei, qual seja, o livre desenvolvimento da sua personalidade.

Ressalta-se que esse entendimento ainda será objeto de confirmação ou não pela ANPD, sendo certo que o futuro debate deverá ser observado com atenção para prevenir o engessamento do fluxo informacional de dados pessoais sensíveis disponíveis publicamente em detrimento da dinamização que sua natureza demanda.

REFERÊNCIAS BIBLIOGRÁFICAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Senado Federal aprova Proposta de Emenda à Constituição 17 (PEC 17/2019) que inclui a proteção de dados pessoais no rol de direitos e garantias fundamentais**. Brasília, 21 out. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/senado-federal-aprova-proposta-de-emenda-a-constituicao-17-pec-17-2019-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-e-garantias-fundamentais>. Acesso em: 1 mar. 2022.

AZEVEDO, Ricardo. O legítimo interesse e a legítima expectativa do titular dos dados pessoais. *In*: OLIVEIRA, Ricardo (coord.); COTS, Márcio (coord.). **O Legítimo interesse e a LGPDP**. 2. ed. São Paulo: Thomson Reuters Brasil, 2021. *E-book*.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, v. 01, n. 157, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 1 out. de 2021.

CAETANO, João Victor Lima. O Regulamento Geral de Proteção de Dados (GDPR): Uma análise do *extraterritorial scope* à luz da jurisdição internacional. **Cadernos Eletrônicos Direito Internacional sem Fronteiras**, v. 2, n. 1, jan-jun 2020, e:11.

CNSEG. **Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados pessoais**. p. 34. Disponível em: <https://cnseg.org.br/data/files/A6/25/A2/F2/9B22571029E24F473A8AA8A8/GBPMS_ONLINE_ok.pdf>. Acesso em: 19 mar. 2022.

COMITÉ EUROPEU DE PROTEÇÃO DE DADOS. **Diretrizes 8/2020 sobre o direcionamento para os utilizadores das redes sociais**. Disponível em: <https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_pt_0.pdf>. Acesso em: 30 mar. 2022.

CONGRESSO NACIONAL. **Emenda Aditiva nº 112 à Medida Provisória n° 869, de 2018**. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7913121&disposition=inline>. Acesso em: 9 abr. 2022.

CORDEIRO, A. Barreto Menezes. **Direito da proteção de dados:** à luz do RGPD e da Lei n.º 58/2019. Coimbra: Almedina, 2020.

COUNCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)**. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 28 fev. 2022.

DATATILSYNET. **Intention to issue € 10 million fine to Grindr LLC**. Oslo, 26 jan. 2021. Disponível em: <https://www.datatilsynet.no/en/news/2021/intention-to-issue--10-million-fine-to-grindr-llc2/>. Acesso em: 29 mar. 2022.

DÖHMANN, Indra Spiecker gen. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. *In*: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.); BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. *E-book*.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021. *E-book*.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.); BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. *E-book*.

ESPANHA. **Constitución Española**. Boletín Oficial del Estado, Madri, n. 311, 1978. Disponível em: <https://www.boe.es/eli/es/c/1978/12/27/(1)/con>. Acesso em: 28 fev. 2022.

EUROPEAN DATA PROTECTION SUPERVISOR. **The History of the General Data Protection Regulation**. Disponível em: <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en>. Acesso em: 27 fev. 2022.

EUROPEAN PARLIAMENT. **CM 2213/16**. Disponível em: <https://www.europarl.europa.eu/cmsdata/99614/Procedure_ecrite_GDPR_EN.docx>. Acesso em: 28 fev. 2022.

FOITZIK, Piotr. Publicly available data under the GDPR: Main considerations. **International Association of Privacy Professionals**. Disponível em: <https://iapp.org/news/a/publicly-available-data-under-gdpr-main-considerations>. Acesso em: 20 mar. 2022.

FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. **Jota**. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018>. Acesso em: 16 mar. 2022.

GDPR HUB. **Article 9 GDPR**. Disponível em: <https://gdprhub.eu/index.php?title=Article_9_GDPR>. Acesso em: 29 mar. 2022.

GELLMAN, Barton; BLAKE, Aaron; MILLER, Greg. Edward Snowden comes forward as source of NSA leaks. **The Washington Post**. Washington, 9 jun. 2013. Disponível em: <https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html>. Acesso em: 28 fev. 2022.

GRATTON, Louis-Philippe. Article 9 GDPR. Processing of special categories of personal data. **GDPR Text**. Disponível em: <https://gdpr-text.com/read/article-9/>. Acesso em: 29 mar. 2022.

GRUPO DE TRABALHO DE PROTECCÇÃO DE DADOS DO ARTIGO 29.º. **Parecer 3/2013 sobre limitação da finalidade (WP 203, 2 de abril de 2013)**. Disponível em: <https://www.gpdp.gov.mo/uploadfile/2017/0127/20170127113421380.pdf>. Acesso em: 8 abr. 2022.

INFORMATION COMISSIONER'S OFFICE. **What are the conditions for processing?** Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/5>. Acesso em: 20 mar. 2022.

KOCH, Richie. What is the LGPD? Brazil's version of the GDPR. **GDPR.EU**. Disponível em: <https://gdpr.eu/gdpr-vs-lgpd/>. Acesso em: 12 fev. 2022.

LANGENEGGER, Natalia; GOBBATO, Andréa. Acesso à Informação com a Lei Geral de Proteção de Dados pessoais: desafios no âmbito do Poder Judiciário. **Revista do Advogado:** Lei Geral de Proteção de Dados Pessoais, n. 144, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html>. Acesso em: 21 mar. 2022.

LIMA, Cíntia Rosa Pereira de (coord.). **Comentários à Lei Geral de Proteção de Dados:** Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020. *E-book*.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *In*: MENDES, Gilmar Ferreira (coord.); SARLET, Ingo Wolfgang (coord.); COELHO, Alexandre Zavaglia P. (coord.). **Direito, inovação e tecnologia**. São Paulo, Saraiva, 2015. *E-book*.

MENKE, Fabiano. Spiros Simitis e a primeira lei de proteção de dados do mundo. **Migalhas**. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-protecao-de-dados-do-mundo>.

Acesso em: 26 fev. 2022.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado:** Lei Geral de Proteção de Dados Pessoais, n. 144, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html>. Acesso em: 21 mar. 2022.

OLIVEIRA, Ricardo. A importância da LGPD e seu papel no ordenamento jurídico brasileiro. *In*: OLIVEIRA, Ricardo (coord.); COTS, Márcio (coord.). **O Legítimo interesse e a LGPDP**. 2. ed. São Paulo: Thomson Reuters Brasil, 2021. *E-book*.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em: <https://www.un.org/sites/un2.un.org/files/udhr.pdf>. Acesso em: 28 fev. 2022.

OVERLY, Steven. Report: Trump-linked firm exploited data on 50 million Facebook users. **Politico**. Washington, 17 de março de 2018. Disponível em: <https://www.politico.com/story/2018/03/17/facebook-trump-campaign-data-cambridge-analytica-423599>. Acesso em: 20 mar. 2022.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**. 3. ed. São Paulo: Saraiva, 2021. *E-book*.

PORTUGAL. **Constituição da República Portuguesa**. Diário da República, Lisboa, n. 86, 1976. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em: 28 fev. 2022.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/2018. *In*: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.); BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. *E-book*.

SATARIANO, Adam. Facebook's WhatsApp is fined for breaking the E.U.'s data privacy law. **The New York Times**. Londres, 02 set. 2021. Disponível em: <https://www.nytimes.com/2021/09/02/business/facebook-whatsapp-privacy-fine.html>. Acesso em: 1 out. 2021.

SCHNEIDER, Harvey A. **Katz v. United States:** The Untold Story. Sacramento: McGeorge L. Rev., 2016. Disponível em: <https://scholarlycommons.pacific.edu/mlr/vol40/iss1/2>. Acesso em: 28 fev. 2022.

SCOTT, Mark. Cambridge Analytica did work for Brexit groups, says ex-staffer. **Politico**. Londres, 30 de julho de 2019. Disponível em: <https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/>. Acesso em: 20 mar. 2022.

SENADO FEDERAL. **Acesso à Informação Pública**: Uma leitura da Lei nº 12.527, de 18 de novembro de 2011. Disponível em: <https://www12.senado.leg.br/transparencia/arquivos/sobre/cartilha-lai/> Acesso em: 20 mar. 2022.

STEWART, Potter, and Supreme Court Of The United States. U.S. Reports: **Katz v. United States**, 389 U.S. 347. 1967. Disponível em: <https://www.loc.gov/item/usrep389347/>. Acesso em: 28 fev. 2022.

TAFT, William Howard, and Supreme Court Of The United States. U.S. Reports: **Olmstead v. United States**, 277 U.S. 438. 1927. Disponível em: <https://www.loc.gov/item/usrep277438>. Acesso em: 28 fev. 2022.

TAVARES, Giovanna Milanez. **O tratamento de dados pessoais disponíveis publicamente e os limites impostos pela LGPD**. Rio de Janeiro: Processo, 2022

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Jornal Oficial da União Europeia, Luxemburgo, L 119, 2016. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1564-1-1>. Acesso em 1º de outubro de 2021.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.); BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. *E-book*.

WALFORD, Ben. Does the GDPR apply to companies outside of the EU? **GDPR.EU**. Disponível em: <https://gdpr.eu/companies-outside-of-europe/>. Acesso em: 12 fev. 2022.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, Boston, v. IV, n. 5, pp. 193-220, dez. 1890. Disponível em: <https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 28 fev. 2022.