Instituto de Referência em Internet e Sociedade

GDPR e suas repercussões no direito brasileiro

Primeiras impressões de análise comparativa

Instituto de Referência em Internet e Sociedade

GDPR e suas repercussões no direito brasileiro

Primeiras impressões de análise comparativa

Fabrício B. Pasquot Polido, Lucas Costa dos Anjos, Luíza Couto Chaves Brandão,

Diego Carvalho Machado, Davi Teofilo Nunes Oliveira

SUMÁRIO

1. Introdução

Entre tantas expectativas e incertezas, o **Regulamento Geral de Proteção dos Dados Pessoais da União Europeia (GDPR)**[1] entrou em vigor em 25 de maio de 2018 e, com ele, um novo paradigma de proteção de dados pessoais, não restrito apenas ao continente europeu. Sua abrangência, ambição legislativa e maturidade conceitual corroboram a ideia de que esse é um autêntico regulamento-modelo, no qual diversas outras iniciativas nacionais, regionais e intracomunitárias também serão espelhadas em busca de padrões normativos uniformes na proteção de dados pessoais. Não seria exagero afirmar que o GDPR nasce como 'monstro normativo'[2], um Leviatã a induzir condutas de conformidade ('compliance') por parte de agentes nas esferas pública e privada no campo da proteção de dados pessoais e especialmente identificáveis nos ambientes informacional e digital.

Desde sua concepção, o Regulamento nº 679/2016 busca se adequar a novo cenário envolvendo a globalização das tecnologias e dos serviços que utilizam a internet como base para suas operações. Governos, usuários e provedores de serviços serão diretamente afetados pelos dispositivos atualizados da Diretiva 95/46/CE, de 1995[3], relativa ao processamento de dados pessoais na comunidade europeia. O que já era padrão legislativo de proteção relativamente avançado, se comparado a outras jurisdições, está prestes a se adequar a termos e procedimentos mais modernos e compatíveis com as novas tecnologias de computação, automação, inteligência artificial. Nesse sentido, encontram-se os conceitos de coleta, processamento, transferência e vazamento de dados, dados sensíveis, direito ao esquecimento, entre outros, além da manutenção de uma Autoridade de Proteção de Dados Pessoais (e a positivação da determinação de um Responsável pela Proteção de Dados no contexto burocrático da macroestrutura da União Europeia[4].

Dada a relevância do mercado europeu no comércio internacional, não apenas como consumidores de produtos e serviços (inclusive digitais), mas também como prestadores de importantes serviços *online* atualmente, é de se esperar que vários outros cenários relevantes sejam afetados pela normativa europeia,como o próprio Brasil. Em um contexto legislativo que não apenas comporta, como também exige a regulamentação do tratamento de dados pessoais por meio do Marco Civil da Internet (Lei 12.965/2014), a tramitação de iniciativas como o Projeto de Lei do Senado nº 330/2013 é impulsionada pela entrada em vigor do novo Regulamento e ganha maior relevância na pauta de discussões do Poder Legislativo nacional.

A necessidade de refletir sobre as repercussões do Regulamento Geral de Proteção dos Dados Pessoais da União Europeia nos âmbitos internacional e nacional é o que motiva o Instituto de Referência em Internet & Sociedade - IRIS a analisar o

1 A sigla em inglês que se destaca nas discussões acadêmicas e nos quadros internacionais é GDPR, correspondente à *General Data Protection Regulation*. Por essa razão, será essa a sigla adotada neste paper. Em português, a sigla corresponde à RGDP. UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, Estrasburgo, 04/05/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 16/04/2018.

2 Apenas para ilustrar, o Regulamento contém 173 considerandos e 90 artigos, distribuídos em nove capítulos. O Art.4o, em especial, dispõe de 26 definições concernentes ao Regulamento, sua interpretação e aplicação.

3 UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, Estrasburgo, 24/10/1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31995L0046>. Acesso em: 15/05/2018.

4 A figura da autoridade central será analisada, sob a perspectiva do Regulamento, no próximo capítulo deste estudo.

tema. A partir de uma perspectiva comparada, não apenas em relação ao Brasil, como também à Argentina, pelas interfaces inequívocas entre a livre circulação de pessoas, bens e serviços no MERCOSUL e leis nacionais de proteção de dados pessoais, busca-se empreender um esforço de previsão dos efeitos do Regulamento Geral de Proteção dos Dados Pessoais - GDPR sobre os ordenamentos jurídicos brasileiros e argentinos. Além disso, examinam-se os possíveis conflitos e alterações às quais governos, usuários e provedores de serviços estarão sujeitos.

Assim, em um primeiro momento, a concepção do Regulamento Geral de Proteção dos Dados Pessoais da União Europeia será contextualizada a partir do arcabouço jurídico e jurisprudencial que o precedeu, delineando seus conceitos mais inovadores e os princípios norteadores da nova legislação. Em seguida, identificamos os elementos extraterritoriais do novo Regulamento e seus possíveis efeitos para o Brasil. Finalmente, em um exercício comparado de análise da legislação argentina, este artigo contextualiza o atual estado da arte da discussão sobre proteção de dados pessoais nesse importante mercado latino-americano, de alta relevância para iniciativas de integração econômica como o Mercosul, por exemplo. Em linhas finais, são endereçadas recomendações quanto à formação de um posicionamento regional acerca dos rumos que toma essa temática em âmbito global.

2. A nova normativa europeia de proteção de dados pessoais e seus contornos gerais

2.1 Contexto anterior ao Regulamento n. 2016/679

A discussão sobre a intromissão de terceiros e do Estado na vida privada de indivíduos e de sua autonomia informacional tem sido pauta das discussões da Comunidade Europeia e da União Europeia há muitos anos. Em 1950, a Declaração Europeia dos Direitos do Homem apresentou noções primárias sobre privacidade em seu artigo 8[5]. A Declaração Universal dos Direitos Humanos também previa em seu artigo 12º[6] noções que iniciaram o arcabouço legislativo que culminou nas concepções que tornaram possível a elaboração de um regulamento europeu sobre proteção de dados nos dias atuais.

Essas primeiras declarações foram elaboradas no pós-Segunda Guerra Mundial, com o objetivo de promover o Estado de Direito, a democracia, os direitos humanos e o desenvolvimento social.[7] Por meio de subsídios jurídicos aos artigos 12 e 8º, a Corte Europeia dos Direitos do Homem se posicionou em inúmeros casos envolvendo dados pessoais, principalmente envolvendo dados relacionados à interceptação de comunicações[8], vigilância[9] e proteções envolvendo o armazenamento de dados pessoais pelas

5 Art. 8. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. *Convenção Europeia dos Direitos do Homem*, 1950. Disponível em:<https://www.echr.coe.int/Documents/Convention_POR.pdf> Acesso em 05/05/2018.

6 Art 12. Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei. ONU. *Declaração Universal dos Direitos Humanos* . Paris, 1948. Disponível em: <http://www.un.org/en/universal-declaration-human-rights/>. Acesso em> 28/04/2018.

7 CONSELHO EUROPEU. *Manual da Legislação Europeia sobre Proteção de Dados*, 2014. Disponível em <https://rm.coe.int/16806ae65f>. Acesso em 10/05/2018.

8 UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. Acórdão Malone c. Reino Unido de 2 de agosto de 1984, petição n.º 8691/79. Disponíveis em: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57533%22]}>. Acesso em 12/05/2018; UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos, acórdão Copland c. Reino Unido de 3 de abril de 2007, petição n.º 62617/00. Disponível em: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-79996%22]}> Acesso em 15/05/2018.

9 UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. Acórdão Klass e o. c. Alemanha de 6 de setembro de 1978, petição n.º 5029/71. Disponível em:<https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}>. Acesso em: 05/05/2018; TEDH, acórdão Uzun c. Alemanha de 2 de Setembro de 2010, petição n.º 35623/05. Disponível em: <https://hudoc.echr.coe.int/eng#{%22item

autoridades públicas e de investigação[10]. Nesses cenários contenciosos, estados eram os principais questionados em suas condutas de violação de direitos fundamentais relativos à privacidade.

A Declaração Europeia dos Direitos do Homem e a Declaração da ONU dos Direitos Humanos foram importantes em seus respectivos contextos, pois foram as primeiras declarações internacionais subscritas por países europeus que mencionam a privacidade e o direito à sua proteção. Porém, como tratavam apenas de maneira vaga e indireta sobre a proteção de dados pessoais, a Comunidade Econômica Europeia, no início da década de 1980, buscando criar mecanismos que abordassem especificamente a proteção de dados pessoais, adotou a Convenção 108 sobre a proteção de indivíduos relativa ao processamento automático de tratamento de dados[11]. Ela almejava estabelecer métodos mais criteriosos e prevê "garantias relativas à coleta[12] e tratamento de dados pessoais"[13]. Além disso, a Convenção proíbe, "na ausência de garantias jurídicas adequadas, o tratamento de dados 'sensíveis', tais como dados sobre a raça, a opinião política, a saúde, as convicções religiosas, a vida sexual ou o registo criminal de uma pessoa". [14] No âmbito do fluxo de dados entre Estados, a Convenção prevê o livre fluxo de dados pessoais entre seus Estados signatários, mas impunha algumas restrições aos fluxos para Estados cuja regulamentação não proporcionasse uma proteção equivalente à da União Europeia[15].

Em 1995, buscando aperfeiçoar e dar corpo à Convenção No. 108, a União Europeia promulgou a Diretiva 95/46/CE, que objetivava estabelecer, harmonizar e promover igualdade no tratamento de dados pessoais pelos Estado-membros. Esse instrumento apresentava princípios de tutela na manipulação, tratamento de dados pessoais e estabeleceu direitos básicos ao titulares dos dados. No que tange à discussão sobre transferência internacional de dados, a diretiva definiu critérios e padrões para a transferência internacional de dados entre países, sem, contudo, fazer previsões de aplicações extraterritoriais[16]. Outro ponto importante, positivado na antiga Diretiva, foi a criação de um arcabouço de autoridades centrais responsáveis pela fiscalização, legislação e arbitragem em questões envolvendo a proteção de dados pessoais, denominadas autoridades centrais de proteção de dados.[17]

Todo o contexto e discussão do desenvolvimento legislativo em relação à proteção de dados pessoais demonstra como o modelo europeu foi construído a partir do reconhecimento da estatura jurídica fundamental do direito à privacidade e à proteção dos dados pessoais[18]. Uma vez que a atividade de tratamento de dados pes-

id%22:[%22001-100293%22]}>. Acesso em 10/05/2018.

10 UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos, Acórdão Leander c. Suécia de 26 de março de 1987, petição n.º 9248/81. Disponível: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}>. Acesso em: 10/05/2018; TEDH, acórdão S. and Marper c. Reino Unido de 4 de dezembro de 2008, petições n.ºs 30562/04 e 30566/04. Disponível em: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}> Acesso em 11/05/2018.

11 CONSELHO EUROPEU. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Estrasburgo*, 1981. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 02/05/2018; A Convenção foi modificada em 18/05/2018 pelo Conselho Europeu. As alterações podem ser acessadas em: <https://www.coe.int/en/web/portal/-/enhancing-data-protection-globally-council-of-europe-updates-its-landmark-convention>.

12 Na versão oficial do texto do Regulamento em português europeu, o termo utilizado é "recolha".

13 CONSELHO EUROPEU. *Manual da Legislação Europeia sobre Proteção de Dados, cit.*

14 Idem.

15 CONSELHO EUROPEU. *Manual da Legislação Europeia sobre Proteção de Dados, cit.*

16 KAPLAN, Harvey. COWING, Mark. EGLI, Gabriel. *A Primer for Data-Protection Principles in the European Union*. Disponível em: <https://www.shb.com/~/media/files/professionals/cowingmark/aprimerfordataprotectionprinciples.pdf?la=en>. Acesso em: 04/05/2018

17 GUIDI, Guilherme. *Modelos regulatórios para proteção de dados pessoais*. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 30/04/2018.

18 BYGRAVE, Lee A. *Data protection pursuant to the right to privacy in human rights treaties. International Journal of Law and*

soais enseja riscos e oportunidades à realização de direitos e liberdades fundamentais[19], os Estados europeus se pautaram em regulação abrangente e pervasiva sobre atividade de tratamento de informações relativa às pessoas naturais.

Em 2016, a União Europeia, por meio do Regulamento nº 679/2016, que ficou conhecido como Regulamento Geral de Proteção dos Dados Pessoais - GDPR[20], substitui a Diretiva nº 95/46/CE, buscando unificar a proteção dos dados pessoais na União Europeia. Como se trata de um regulamento, e não de uma diretiva, é diretamente aplicável aos 28 Estados Membros, não sendo necessária qualquer transposição para cada jurisdição nacional. Assim, é considerado como uma norma interna, prática que não acontecia com a Diretiva 95/46/CE, pois era necessário que os Estados adotassem o texto comunitário em seu direito lei interno, gerando diferentes níveis de proteção de dados em cada um dos países europeus[21].

Os principais argumentos para a fundamentação da GDPR corroboram a pertinência de uma legislação capaz de enfrentar as novas questões suscitadas pela economia digital e pervasividade das tecnologias da informação e da comunicação de forma isonômica entre os diferentes países do bloco[22].

Este capítulo inicial tem como objetivo apontar as principais mudanças decorrentes da nova regulação europeia e seus contornos gerais, fundamentais mudanças conceituais, novas previsões e principais questões inauguradas pela legislação. Como a nova normativa comunitária de proteção de dados é um regulamento bastante complexo, composto por 11 capítulos e 99 artigos, este estudo não tem como objetivo esgotar a discussão, mas sim oferecer subsídios primários para estudos e aplicações das principais mudanças advindas da regulação europeia e seus impactos no Brasil, além de uma comparação com as norma relativas à matéria na Argentina, um dos referenciais mais destacados na América Latina.

A construção de garantias relacionadas a temas que envolvam tecnologias e suas inovações em ambientes informacionais e reticulares (como é o caso da Internet e plataformas digitais) tem sido um desafio para os legisladores nos dias atuais. Em tão sensíveis como os que definem o espectro da proteção jurídica de dados pessoais, essas questões se tornam ainda mais latentes, visto que os modelos de negócios envolvendo dados pessoais são rapidamente alterados pelo ritmo das inovações e o crescimento das empresas. Desse modo, cria-se o risco de uma lei se tornar obsoleta poucos anos após sua publicação.[23]

Information Technology, v. 6, n. 3, p. 247-284, 1998.

19 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *EJJL-Espaço Jurídico: Journal of Law*, v. 12, n. 2, p. 91-108, 2011.

20 General Data Protection Regulation - GDPR. Como abordado na introdução, o termo utilizado no artigo será GDPR para referir-se ao Regulamento Geral de Proteção dos Dados Pessoais, embora seja importante observar que a consistência com a abreviatura empregada em língua portuguesa em uma das versões originais do Regulamento seja RGDP.Texto disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679>

21 Nesse sentido, c.f. GUIDI, Guilherme. *Modelos regulatórios para proteção de dados pessoais*. cit. : "Regulamentos são normas vinculativas diretamente aplicáveis a todos os países, incluindo-se aí seus cidadãos e pessoas jurídicas, valendo como se direito nacional fosse. Diretivas são normas adotadas pela Comissão e pelo Parlamento Europeu que fixam um objetivo que todos os Estados-Membros devem alcançar, cabendo a cada um decidir os meios exatos para tal, respeitando os preceitos básicos da norma supranacional."p.3.

22 CAMERON, Stephen. *'Light Reading 'The Digital Economy & GDPR'* 2017 Disponível em: <http://www.lightreading.com/oss-bss/subscriber-data-management/the-digital-economy-and-gdpr/a/d-id/730582> Acesso em: 04/05/2018.

23 Sobre a dificuldade de legislar sobre os diversos temas que envolvem a internet e novas tecnologias, cf.: KURBALIJA, Jovan. *An introduction to Internet governance.* 2010. Disponível em: <https://www.diplomacy.edu/resources/books/introduction-internet-governance> Acesso em: 04/05/2018.

2.2. Técnica normativa e dispositivos centrais do GDPR

Pensando nesses desafios, a nova regulação de proteção de dados no domínio da União Europeia foi elaborada em vários "níveis". Em um primeiro estágio, compreendido entre os artigos 1º e 11, foram positivadas garantias fundamentais amplas e definições que serão utilizadas durante todo texto do Regulamento e sua aplicação. Essa estrutura de níveis e princípios permite maior dinamização da legislação, fazendo com que ela seja menos suscetível a desatualizações. Esse método estabelece princípios e garantias que são tecnologicamente neutros - o que assegura sua aplicação futura, ainda que com mudanças razoáveis no campo tecnológico.[24]

Em seu primeiro capítulo, principalmente no artigo 4º, são definidos diversos conceitos-chave que serão utilizados ao longo de toda legislação - alguns previamente definidos na Diretiva 95/46/CE, mas aprimorados pelo novo regulamento. No artigo 4º, é possível encontrar mais de vinte e cinco conceitos-chave,[25] como as definições de dado pessoal[26], perfilamento[27], consentimento[28], processamento [29], Responsável pela proteção de dados[30], autoridade fiscalizadora[31], entre outros. Essas definições iniciais influenciam toda a legislação, visto que as noções de consentimento e de dados pessoais definem o escopo e aplicação de uma lei de proteção aos dados pessoais.

Ao definir dados pessoais, a GDPR adotou um conceito expansionista.[32] Isso quer dizer que dado pessoal pode referir-se a qualquer tipo de informação que permita sua identificação, ainda que o vínculo não seja estabelecido de imediato, mas de maneira indireta ou mediata. Essa é uma estratégia normativa que parte da premissa de que "dados anônimos são sempre passíveis de reversão"[33]. Na Diretiva revogada, dados pes-

24 GUIDI, Guilherme. *Modelos regulatórios para proteção de dados pessoais. cit.*

25 Mais informações em: <https://gdpr-info.eu/art-4-gdpr/>.

26 Art, 4 (1), GDPR: «Dados pessoais», 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. UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, *cit.*

27 Art, 4 (4), GDPR: «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações; (Tradução livre). Idem.

28 Art, 4 (11), GDPR: «Consentimento» do titular dos dados, 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; (Tradução livre). Idem.

29 Art, 4 (2), GDPR: «Tratamento», 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. Idem.

30 Art, 4 (7), GDPR: «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro; Idem.

31 Art., 4(21), GDPR: "«Autoridade de controlo», uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51.º". Idem.

32 BIONI, Bruno. *Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Grupo de Estudos em Políticas Públicas em Acesso à Informação da USP – GPOPAI, São Paulo,* 2015. Disponível em: <http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf> Acesso em: 02/05/2018.

33 Idem, p.32. Nota-se, contudo, que a possibilidade de anonimização de dados no direito europeu é matéria controversa. Isso porque, em perspectiva diversa, não se elimina a possibilidade de anonimização de dados. Devido à atual capacidade computacional e os numerosos bancos de dados digitalizados e interconectados em rede, as técnicas de anonimização poderiam fornecer garantias de privacidade e ser utilizadas para gerar processos eficazes de anonimização, mas apenas se a sua aplicação for adequadamente construída –o que significa que os requisitos prévios. Além disso, os objetivos do processo de anonimização devem ser claramente definidos. A melhor solução técnica seria tomada caso a caso, eventualmente por meio de uma combinação de métodos diferentes. Nesse sentido, para mais informações, ver: GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29.º *Parecer 05/2014 sobre técnicas de anonimização*, de 10 de abril 2018. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/

soais eram definidos apenas como como nome, imagem, endereço, e-mail, telefone e identificação pessoal[34], portanto em espectro determinado por elementos praticamente exaustivos. Trata-se de uma primeira geração de normas comunitárias relativas à regulamentação de questões afetas às novas tecnologias e proteção de dados, superada pela emergência e desdobramentos da Internet.

No novo Regulamento Europeu, integram o conceito de dados pessoais quaisquer informações que possam ser utilizadas para identificar uma pessoa, como dados de localização de usuário, IDs de dispositivos móveis e até endereço IP, em alguns casos.

A coleta de **dados sensíveis** - aqueles que revelam origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos, dados relativos à saúde ou dados relativos à orientação sexual - é expressamente proibida, nos termos do artigo 9º. A regulação prevê algumas exceções, autorizando a coleta de dados sensíveis para fins de medicina preventiva e ocupacional, para avaliar a capacidade de trabalho do funcionário, diagnóstico médico, prestação de cuidados médicos ou sociais e tratamento ou gestão de sistemas e serviços de saúde, assistência social com base no direito do Estado-Membro ou por força de contrato com um profissional de saúde.[35]

Anova normativa europeia introduz significativas mudanças em relação à Diretiva 95/46/CE: fortalece a **noção de consentimento para uso de dados pessoais** noção e esclarece o alcance da relação entre o consentimento e a coleta e processamento dos dados pessoais[36]. Segundo essa fórmula, a GDPR estabelece que o pedido de consentimento deve ser apresentado de uma forma claramente distinguível, de outros assuntos, de forma inteligível, fácil acesso e usando linguagem simples, ao invés da linguagem obscura geralmente adotada.[37] Outro elemento novo, contemplado pelo Regulamento, diz respeito à obrigação de explicação dos objetivos ou intentos da coleta de dados. Ela terá de ser precedida por uma explicação do seu propósito, demonstrando como e quem deu o consentimento e, caso a coleta de dados destine-se a diversos fins, todos deverão ser demonstrados para o usuário. Outro ponto importante é que a pessoa que consentiu com a coleta de seus dados tem o direito de retirar a autorização a qualquer momento, e sua saída deve ser tão simples quanto sua concessão.[38]

Entre as muitas normas estabelecidas pelo Regulamento, encontra-se o **princípio de responsabilidade**, central para as relações envolvendo a gestão de dados por empresas e entes da administração pública. Com entrada em vigor do Regulamento, todas as empresas passam a ser civilmente responsáveis pelo armazenamento e pela proteção de todos os dados pessoais que coletam e armazenam. Da responsabilidade decorre a obrigação de reparar qualquer dano causado aos titulares das informações coletadas e

files/2014/wp216_pt.pdf>. Acesso em 14/05/2018.

34 CONSELHO EUROPEU. *Diretiva 95/46/CE relativa à Proteção de Dados. cit.*

35 Art. 9, GDPR: "É proibido o processamento de dados pessoais revelando origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, ou filiação sindical, e processamento de dados genéticos, dados biométricos com a finalidade de identificar unicamente uma pessoa singular, dados relativos à saúde ou dados relativos a um sexualidade ou orientação sexual de uma pessoa."UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho.*cit.*

36 A regulação determina que, no caso de crianças e adolescentes, o tratamento dos dados é legal a partir dos 16 anos. Nos casos em que a criança tenha menos de 16 anos de idade, tal tratamento só será legal na medida em que o consentimento seja dado ou autorizado pelo titular da responsabilidade parental sobre a criança, desde que essa idade não seja inferior a 13 anos. Idem.

37 Art 7 (2), GDPR: Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento. Idem.

38 Art 7 (3), GDPR - O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.. Idem.

armazenadas em virtude de violação ou vazamento[39].

No que diz respeito aos dispositivos concernentes às empresas, proteções e **vazamento de dados**[40], o Regulamento enuncia uma série de deveres e obrigações. Primeiramente, é importante destacar a **obrigatoriedade de notificaçã**o[41] à autoridade de proteção de dados em até 72 horas para casos de vazamentos de dados que resultem em riscos para direitos e liberdades de indivíduos. A exposição de motivos do Regulamento assim prevê:

> 86 (...) Por conseguinte, logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deverá notificá-la à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido,a menos que seja capaz de demonstrar em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares. Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada[42].

Outra obrigação imposta aos responsáveis pelo processamento e tratamento de dados pessoais, públicos ou privados, diz respeito à necessidade de determinação de um **responsável pela proteção de dados**[43]. Ele tem o papel de aproximar os órgãos reguladores e titulares dos dados pessoais. Essa atribuição só será necessária, segundo o Art. 37, caso quem esteja a coletar dados seja um órgão público[44] ou quando as atividades principais da organização privada consistirem em:

- Operações de processamento de dados em larga escala que objetivam monitoramento regular e sistemático dos titulares de dados;
- Operações de processamento em larga escala de categorias especiais de dados, ou seja, dados sensíveis, como saúde, religião, raça, orientação sexual etc.; e dados pessoais relacionados a condenações e infrações penai.

Os Resposnáveis pela proteção de dados (RPD) exercem diversas funções, que são basicamente elencadas no Art. 39 do Regulamento n. 679/2016. Trata-se de uma pessoa com alguma experiência no ramo da segurança e proteção dos dados, designada pelas empresas que sejam responsáveis ou que atuem como subcontratadas para

39 Com a entrada em vigor do Regulamento, na data de 25 de maio de 2018, empresas passam a ser diretamente responsáveis por cuidar para que todas as informações obtidas estejam seguras, protegidas contra qualquer risco de violação ou vazamento.

40 Vazamento de dados é definido, para os fins do regulamento, no Artigo 4 como: "Quebra de segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou de outra forma processados". Idem.

41 Estabelece no Artigo 33: "Em caso de violação dos dados pessoais, o responsável pelo tratamento deve, sem demora injustificada e, se exequível, no prazo de 72 horas após ter tomado conhecimento, notificar a violação dos dados pessoais à autoridade de supervisão competente nos termos do artigo 55.º, a menos que seja improvável que a violação de dados pessoais resulte num risco para os direitos e liberdades das pessoas singulares". Idem.

42 Cf. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, Para.86.

43 "Data protection officer" traduzido livremente como responsável pela proteção de dados". Na versão oficial em português do Regulamento, referência é feita ao "encarregado pela proteção de dados", tal como indicado em outras partes da normativa (Arts. 14, 30, 33, 34 além da Seção 4).

44 O WP29 considera que o que constitui uma "autoridade ou organismo público" deve ser determinado pela legislação nacional e que esses órgãos devem nomear um gestor de proteção de dados. Entretanto, outras personalidades jurídicas singulares ou colectivas regidas pelo direito público ou privado (por exemplo, serviços de transporte público, fornecimento de água e energia, infra-estrutura radiodifusão de serviço público, alojamento público ou órgãos disciplinares) não são obrigadas a nomear um gestor, mesmo que seja altamente recomendável. Para mais informações: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048> . Acesso em 06/05/2018.

o tratamento de dados pessoais. Sua função imediata será a de supervisionar e aconselhar a empresa a respeito das obrigações contidas na GDPR. Entre essas principais funções, destacam-se as seguintes: i) monitorar e elaborar relatórios sobre a conformidade da organização com a política da GDPR; ii) a elaboração de treinamento com as partes envolvidas no processamento dos dados pessoais; e iii) a realização de avaliações para impacto de proteção de dados, sua implementação e resultado. Também atuam como intermediários entre as partes interessadas, como por exemplo, autoridades de supervisão, titulares de dados e empresas que detenham dados pessoais.[45] .

O Art. 24 do Regulamento, deixa claro que é de atribuição do Responsável pela proteção de dados "implementar medidas técnicas e organizacionais adequadas para assegurar e demonstrar que o tratamento de dados é realizado em conformidade com o presente regulamento"[46]. Ou seja, o Responsável pela Proteção de Dados atuará como um canal de comunicação entre as partes envolvidas na proteção dos dados e também como um fiscalizador de todas as práticas de tratamento de dados pessoais na organização, verificando se estão em conformidade com a GDPR e sensibilizar sobre a relevância do *compliance*[47] no tratamento dos dados dos cidadãos.[48] O não monitoramento da conformidade com a GDPR não é de responsabilidade pessoal do Responsável pela Proteção de Dados, mas da empresa ou instituição responsável pela coleta dos dados.[49]

2.3. Novos direitos positivados e ambientes informacionais

Duas categorias de direitos positivados no Regulamento Europeu têm levantado discussões sobre suas possíveis aplicações. A primeiro, estabelecido Art.17, diz repeito ao denominado "**direito ao apagamento dos dados**" ("**direito ao esquecimento**"")[50], permite que o titular dos dados solicite a quem os possua que eles sejam apagados. Também prevê ser possível ao titular requerer seus dados pessoais e interromper-lhes o compartilhamento e o uso.

As condições para uma 'pretensão jurídica de remoção estão descritas no Art.17 e contemplam, por exemplo, dados que não são mais relevantes para seus propósitos originais ou cujo consentimento foi revogado, prevendo que deverá ser levado em consideração o "interesse público na disponibilidade dos dados" ao aceitar tais solicitações. O direito ao esquecimento no Direito da União Europeia ganhou recente destaque com o caso *Google Inc v Agencia Española de Protección de Datos, Mario Costeja González* (2014)[51].

45 ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Officers ('DPOs')*. Disponível em: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>. Acesso em: 02/05/2018.

46 Art. 24, GDPR: Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.. UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho. *cit.*

47 *Compliance* é o conjunto de ações para fazer cumprir as normas, regulamentos, políticas e as diretrizes estabelecidas para o negócio e para as atividades da instituição ou empresa, bem como evitar, detectar e tratar qualquer desvio ou inconformidade que possa ocorrer, nesses casos, em relação a proteção de dados pessoais. No que se refere ao *compliance*, estão especialmente engajados escritórios de advocacia da Europa e os departamentos jurídicos de empresas transnacionais, cujas atividades são alcançadas pelo regulamento.

48 BIONI, Bruno; MONTEIRO, Renato. *O papel do Data Protection Officer.* 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-papel-do-data-protection-officer-04122017>. Acesso em: 28/04/2018.

49 ARTICLE 29 DATA PROTECTION WORKING PARTY. *The Role of the Data Protection Officer,* 2017. Disponível em:<https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/DPO%20Update%20Article%20Final.pdf>. Acesso em 30/04/2018.

50 A categoria do direito ao esquecimento ("direito a ser esquecido", segundo a expressão em português de Portugal), formulada jurisprudencialmente e transposta para a normativa europeia, é referida, em alguns idiomas oficiais da UE como: "Recht auf Löschung (Recht auf Vergessenwerden)" (alemão), "Droit à l'effacement (droit à l'oubli)" (francês), "Diritto alla cancellazione (diritto all'oblio)" (italiano) e "Derecho de supresión (el derecho al olvido)" (espanhol).

51 UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Grande Secção. Processo C-131/12, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos (AEPD), Mario Costeja González.* Luxemburgo, 13/05/2014. Disponível em: <http://curia.

O caso genuinamente oficializou um precedente judicial da CJUE em relação à matéria e promoveu inúmeras discussões sobre sua aplicação, alcance normativo e ponderação de direitos[52].

De acordo com o artigo 17(1)(*c*), a GDPR assegura o apagamento dos dados pessoais pelo titular que exercer seu direito de oposição (artigo 21) e não houver "interesses legítimos prevalecentes que justifiquem o tratamento". A noção de "interesse legítimo" configura conceito jurídico indeterminado, portanto, a demandar dos tribunais acionados a concreção normativa segundo atividade hermenêutica direcionada ao juiz ao caso concreto. Assim, devem os tribunais sopesar se existe interesse do próprio responsável pelo tratamento ou de terceiros, que seja preponderante em relação a direitos e liberdades fundamentais do titular dos dados protegidos pela lei. Alguns parâmetros objetivos são fornecidos a respeito do que possa configurar "interesse legítimo", tanto pelo GDPR[53], quanto pela jurisprudência do CJUE[54], além de outros órgãos do sistema de proteção de dados da União Europeia[55].

Direito à explicação e à oposição contra tomada de decisão automatizada

Outra categoria de direito relacionada ao ambiente informacional, estabelecida pela nova normativa europeia está associada à **oposição contra tomada de decisão automatizada**, em linha com o disposto no Art. 22 (decisões individuais automatizadas, incluindo definição de perfis) e os Arts. 13 a 15 ('Informação e acesso aos dados pessoais") do Regulamento. Regras que restringem as decisões automatizadas e exigem "explicações" sobre o funcionamento dos algoritmos têm aberto diversas discussões entre membros da academia, especialistas e outros interessados em decisões tomadas pelo aprendizado de máquina ou inteligência artificial.[56]

Decisões automáticas e sem qualquer intervenção humana parecem ir contra a noção de autonomia e personalidade no Regulamento Europeu[57]. Portanto, a orientação do Regulamento mensurar o **direito à explicação** busca fornecer alguma informação significativa sobre como os dados pessoais são utilizados em decisões automatizadas. Inúmeras controvérsias são suscitadas relativamente às possíveis aplicações dessas categoria de direito e como ela será efetivamente colocada em prática. A literatura já existente sobre o GDPR observa, de modo cauteloso, as implicações dos Arts. 13 a 15 e 22,

europa.eu/juris/document/document.jsf?docid=152065&doclang=PT>. Acesso em: 15/05/2018.

52 THE GUARDIAN, *Costeja González and a memorable fight for the 'right to be forgotten'*, 2014. Disponível em: <https://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten>. Acesso em 05/05/2018.

53 A exemplo dos seus Considerandos nº 47 a 49.

54 Como ocorreu no caso *Mario Costeja González*. Segundo o acórdão proferido: "Considera o Tribunal que esta obrigação de "suprimir da lista de resultados" decorre de um direito do titular dos dados que não pressupõe a existência de um prejuízo pela inclusão na lista de resultados "Na medida em que (…) pode, tendo .. requerer que a informação em questão deixe de estar à disposição do grande público devido à sua inclusão nessa lista de resultados, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em aceder à informação numa pesquisa sobre o nome dessa pessoa. (100/4)". TJUE, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, *cit.* (Tradução livre)

55 ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* Bruxelas: [s. n.], 2014. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Acesso em: 23/05/2018.

56 SELBST, Andrew; POWLES, Julia. Meaningful information and the right to explanation. In: *International Data Privacy Law,* vol. 7, n. 4, 2017, p. 233 ss.Disponível em <https://academic.oup.com/idpl/article/7/4/233/4762325> Acesso em: 05/05/2018.

57 JONES, Meg Leta. The right to a human in the loop: Political constructions of computer automation and personhood. *Social studies of science,* v. 47, n. 2, p. 216-239, 2017.

consideradas suas tecnicidade e complexidade.[58]

2.4. Multas e penalidades estabelecidas pela violação de conformidade

Por fim, um dos pontos essenciais que despertam discussões quanto ao alcance e aplicações diz respeito às multas e penalidades, indicadas nos artigos 83 e 84 do Regulamento n. 679/2016. A desconformidade com as exigências previstas na normativa europeia, poderá render às empresas multas administrativas em diversas circunstâncias. Será enviada uma notificação por escrito em caso de não conformidade inicial.

O grau de sancionamento pecuniário dependerá da violação apurada e engloba multas de até €10 milhões ou 2% do total do faturamento anual global no exercício financeiro anterior, dependendo de qual for o maior valor. Nesse caso, diversas são as situações previstas no GDPR, como por exemplo, violação de princípios como "*privacy by design*"[59], não cumprimento das obrigações relacionadas ao processamento ou a não designação de um Responsável pela Proteção de Dados. As multas para esses casos buscam remediar a efetiva ou potencial violação dos direitos estabelecidos nos artigos 8º, 11, 25, 39, 42 e 43 do Regulamento.

Outras sanções previstas são multas de até €20 milhões ou 4% do total do faturamento anual mundial no exercício anterior, por violações aos princípios relativos ao processamento, aos requisitos legais de processamento ou ainda dos direitos do titular dos dados. A imposição dessas sanções exigirá, por parte dos tribunais, avaliação caso a caso das circunstâncias da infração, sendo considerados fatores como a gravidade e a duração da infração, os atos intencionais ou negligentes, medidas de mitigação de danos que tenham sido implementadas, medidas técnicas e organizacionais e, por fim, o modo como a autoridade supervisora tomou conhecimento dos eventos alegadamente infrativos.[60] Essas categorias de multas visam tutelar os direitos estabelecidos nos artigos 5º, 6º, 7º, 9º, 12 à 22 e as situações envolvidas na transferência internacional de dados, previstas nos artigos 44 a 49 do GDPR.

2.5. Observações parciais de análise

Considerados esses aspectos do novo Regulamento sobre a Proteção de Dados na União Europeia, este capítulo apresentou alguns dos contornos gerais, bem como suas mais latentes discussões. Em virtude da extensão da GDPR, além da presente seção, tabela dos temas sistematizados da GDPR (anexo), auxilia o debate que se estabelece na produção científica brasileira. Os próximos capítulos tratarão dos elementos extraterritoriais do Regulamento e investigarão seus possíveis impactos, levando em consideração a comparação entre o sistema jurídico de proteção de dados no Brasil e Argentina.

58 Para aprofundamento sobre essas discussões, c.f.: WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. In: *International Data Privacy Law*, v. 7, n. 2, p. 76-99, 2017 e SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. In: *International Data Privacy Law*, v. 7, n. 4, p. 233-242, 2017.

59 "Privacidade desde a concepção". Tal abordagem busca promover a privacidade e a proteção de dados desde a concepção e elaboração de uma aplicação.

60 Conforme o art. 83, as multas devem ser efetivas, razoáveis e dissuasivas para cada caso individual. Para a decisão sobre se e qual quantidade de sanções pode ser avaliada, as autoridades têm um catálogo legal de critérios que devem ser usados na tomada de decisão. Entre outras coisas, a violação intencional, a incapacidade de tomar medidas para mitigar os danos ocorridos ou a falta de colaboração com as autoridades podem aumentar as penalidades. UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho. *cit.*

3. Interfaces extraterritoriais do Regulamento (UE) n. 2016/679 e seus efeitos no Brasil

3.1. Âmbito de aplicação do GDPR e extraterritorialidade

Uma das principais razões para já se ter afirmado que o GDPR "irá mudar não apenas as leis europeias de proteção dados, mas nada menos do que todo o mundo como o conhecemos"[61], encontra-se no âmbito de aplicação material e espacial do Regulamento.

Suas normas incidem sobre toda atividade de "tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados" (Art. 2º). O dispositivo legal, na verdade, em nada difere do texto inscrito no Art. 3(1), da Diretiva 95/46/CE. A novidade, porém, que tanto ressona e que atinge diretamente as grandes empresas de tecnologia do Vale do Silício[62], tem por fundamento o âmbito de aplicação espacial ou territorial do GDPR.

Nos termos do artigo 3(1), o Regulamento é aplicável ao tratamento de informações pessoais realizado "no contexto das atividades de um estabelecimento" de responsável pelo tratamento ou por operador **situado no território europeu**, ainda que o tratamento ocorra **fora dos limites territoriais** da União Europeia[63].

Para a compreensão do critério eleito pelo legislador europeu, é importante destacar que a noção de **estabelecimento** foi delineada principalmente a partir da jurisprudência da Corte de Justiça da União Europeia , em sua função de interpretação da Diretiva 95/46/CE, que também se fundava no alargamento do âmbito territorial de aplicação.

No caso *Weltimmo*, a Corte esclareceu que o conceito de estabelecimento se "estende a toda atividade real e efetiva — ainda que mínima — exercida mediante uma instalação estável"[64]. Construiu-se aí uma concepção flexível — não formalista — do conceito, válida "especialmente para as empresas que se dedicam a oferecer serviços exclusivamente pela Internet"[65]. Segundo o acórdão em Weltimmo:

> "(...) 28. No que respeita, em primeiro lugar, ao conceito de «estabelecimento», há que recordar que o considerando 19 da Diretiva 95/46 enuncia que o estabelecimento no território de um Estado-Membro pressupõe o exercício efetivo e real de uma atividade mediante uma instalação estável e que a forma jurídica de tal estabelecimento, quer se trate de uma simples sucursal ou

61 ALBRECHT, Jan. P. How the GDPR Will Change the World. In: *European Data Protection Law Review,* v. 2, n. 3, 2016, p. 287. Tradução livre do original: "[GDPR] will change not only the European data protection laws but nothing less than the whole world as we know it."

62 SOLON, Olivia. *How Europe's 'breakthrough' privacy law takes on Facebook and Google.* 2018. Disponível em: <https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation>. Acesso em: 09 mai. 2018.

63 Art. 3(1), GPDR: "O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União".

64 UNIÃO EUROPEIA. Court of Justice of European Union. Third Chamber. Case C-230/14, *Weltimmo s. r. o.* v. *Nemzeti Adatvédelmi és Információszabadság Hatóság*. Luxemburgo, 01/10/2015. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN>. Acesso em 10/05/2018. Tradução livre de: "[...] extends to any real and effective activity — even a minimal one — exercised through stable arrangements".

65 Idem. Tradução livre de: "This is particularly true for undertakings offering services exclusively over the Internet". Vide também DE HERT, P.; CZERNIAWSKI, M. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. In: *International Data Privacy Law*, v. 6, n. 3, 2016, p. 233.

de uma filial com personalidade jurídica, não é determinante (acórdão Google Spain e Google, C-131/12, n.° 48). Este considerando precisa, por outro lado, que, quando no território de vários Estados-Membros estiver estabelecido um único responsável pelo tratamento, deve assegurar-se, nomeadamente para evitar que a legislação seja contornada, que cada um dos estabelecimentos cumpra as obrigações impostas pela legislação nacional aplicável às respetivas atividades.

29. Daqui resulta, conforme sublinhou o advogado-geral nos n.os 28 e 32 a 34 das suas conclusões, uma concepção flexível do conceito de estabelecimento, que afasta qualquer abordagem formalista segundo a qual uma empresa só se pode considerar estabelecida no lugar em que estiver registada. Assim, para determinar se uma sociedade, responsável por um tratamento de dados, dispõe de um estabelecimento, na aceção da Diretiva 95/46, num Estado-Membro diferente do Estado-Membro ou do país terceiro em que está registada, há que avaliar tanto o grau de estabilidade da instalação como a realidade do exercício das atividades nesse outro Estado-Membro, tendo em conta a natureza específica das atividades económicas e das prestações de serviços em causa. Este entendimento vale especialmente para as empresas que se dedicam a oferecer serviços exclusivamente na Internet.

30. A este respeito, há, designadamente, que considerar, atendendo ao objetivo prosseguido por esta diretiva, que consiste em assegurar uma proteção eficaz e completa do direito à vida privada e em evitar que a legislação seja contornada, que a presença de um único representante pode, em certas circunstâncias, ser suficiente para constituir uma instalação estável se este atuar com um grau de estabilidade suficiente através dos meios necessários para a prestação dos serviços específicos em causa no Estado-Membro em questão"

No caso descrito, a atividade exercida pela sociedade empresária eslovaca *Weltimmo* envolvia a exploração de *websites* de anúncios de imóveis situados na Hungria. Após o período de um mês de fornecimento gratuito de publicidade em torno dos imóveis transacionados por terceiros, a empresa passava então a faturar o serviço e cobrar pagamentos dos anunciantes húngaros, mesmo após requerimento para a exclusão do anúncio e apagamento dos dados pessoais, formulado dentro do mencionado prazo de gratuidade.

Além dessas circunstâncias, foram considerados relevantes no exame feito pela CJUE o fato de a empresa[66] haver constituído representante na Hungria e o seu sítio eletrônico utilizar o idioma húngaro para operação das atividades. Ao final, a CJUE decidiu que a empresa responsável pelo tratamento de dados pessoais (e provedora de aplicação de internet) se dedicava a uma atividade real e efetiva no território húngaro.

Para o Regulamento, o local onde se dá o tratamento de dado pessoal é irrelevante se o estabelecimento do responsável é situado na União Europeia. A nova normativa tem evidente pertinência em vista dos avanços da internet. Alcança, por exemplo, empresas e entidades responsáveis pelo tratamento de dados que utilizam **computação em nuvem** (*cloud computing*), isto é, se valem de "arranjos pelos quais recursos computacionais são fornecidos de modo flexível e independentemente da localização, que permitem uma rápida e ininterrupta alocação de recursos sob demanda"[67], nas diferentes modalidades de serviço que podem ser adotadas.

No Art. 3º do GDPR, incluiu-se uma figura ausente no direito anterior: o **subcontratante**,[68] ou **operado**r (*processor*). Conforme estabelece o artigo 4.8 do Regulamento,

66 No contexto de interpretação e aplicação do GDPR, **empresa** é "pessoa singular ou coletiva que, independentemente da sua forma jurídica, exerce uma atividade económica, incluindo as sociedades ou associações que exercem regularmente uma atividade económica" (artigo 4(18)). UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho. *cit.*

67 MILLARD, Christopher (Ed.). *Cloud Computing Law.* Oxford: Oxford University Press, 2013. E-book. Tradução livre do orginal: "*an arrangement whereby computing resources are provided on a flexible, location-independent basis that allows for rapid and seamless allocation of resources on demand.*"

68 Termo empregado na tradução oficial do Regulamento na língua portuguesa.

subcontratante ou operador é a pessoa natural ou jurídica, a autoridade pública, agência ou órgão que trate os dados pessoais **em nome do responsável pelo tratamento** destes. Ou seja, é interposta entidade que realiza atividade de tratamento de informações pessoais em nome de um responsável que decide delegar, contratualmente[69], parte ou a totalidade das operações de tratamento de dados[70], como acontece no fornecimento de serviço de computação em nuvem e outros contratos de tecnologia da informação — *e. g.*, cessão da capacidade de processamento.

Os atos e atividades envolvendo tratamento de dados, por sua vez, encontram-se definidos, fundamentalmente, no Art.4.2 do Regulamento[71]. Devido à abrangência desses atos e atividades, além das complexas redes de negócios e contratos envolvendo empresas atuantes nos segmentos de computação e internet, o Art. 3(1) do GDPR diretamente alcança sujeitos - subcontratante ou operador- atuantes em qualquer fase ou etapa do tratamento de dados pessoais, ocorram elas dentro ou fora do domínio territorial da União.

Existem dois pressupostos para o reconhecimento de um sujeito - pessoa natural ou jurídica - como subcontratante ou operador: (i) ser ente separado e com autonomia jurídica em relação ao responsável pelo tratamento de dados pessoais; e (ii) efetuar o tratamento de informações em nome do responsável[72].

Identificada a natureza de um agente como subcontratante, o quadro fático das interações **subcontratante-responsável pelo tratamento de dados** pode se subsumir em três situações distintas: (i) tanto o subcontratante como o responsável possuem estabelecimento na União Europeia; (ii) o operador tem estabelecimento fora da União Europeia e é contratado por responsável com estabelecimento em país-membro do bloco europeu; e (iii) o estabelecimento do operador se situa no território europeu, diferentemente do responsável, localizado em país que não faz parte da União Europeia.

Em que medida se aplica o GDPR nessas situações?

Na primeira hipótese, a normativa europeia há de reger ambos agentes. Já na situação indicada no item **ii**, apesar da obviedade da aplicação do Regulamento ao responsável pelo tratamento de dados pessoais, pode surgir o questionamento quanto à regulamentação da atividade do subcontratante cujo estabelecimento se localiza fora dos limites territoriais da União Europeia.

Nesse caso, o GDPR não pode ser aplicável imediatamente ao operador à luz do critério da localização do estabelecimento do Art. 3(1) a não ser que o tratamento realizado em nome do responsável seja relativo a informações de natureza pessoal de residentes na UE para o fornecimento de bens e serviços ou o monitoramento do comportamento dos titulares dos dados, na forma do Art. 3(2). No entanto, ainda no caso de eventual inaplicabilidade direta do Regulamento, este será indiretamente vinculante ao operador em razão da obrigatoriedade do contrato, ou outro ato normativo, cujas regras se aplicam à sua atividade de tratamento de dados, conforme estabelece o artigo

69 É o que decorre da previsão do artigo 28 (3), do Regulamento: "O tratamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. [...]". UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho. *cit.*

70 VOIGT, Paul; BUSSCHE, Axel von dem (Eds.). *The EU General Data Protection Regulation (GDPR):* A Practical Guide. [s.l]: Springer, 2017. p. 20.

71 Para inteiro teor do dispositivo, ver nota 30.

72 Ibidem.

28(3)[73].

Um exemplo de aplicação indireta é ilustrado por Voigt e Bussche. X é empresa alemã que presta serviço de alocação e contratação temporária de pessoal para grandes fábricas de automóveis de toda a Europa. Devido ao fato de seu grande quadro de funcionários mudar constantemente, X armazena os dados sobre processos seletivos mediante provedor de serviço de computação em nuvem situado nos Estados Unidos da América, Y. Ainda que Y não direcione suas atividades para a União Europeia (na forma do artigo 3(2) do Regulamento.), deverá observar os parâmetros de proteção de dados do GDPR expressamente previstos no contrato que mantém com X[74].

Na terceira hipótese, por sua vez, tendo o subcontratante estabelecimento no território da União Europeia, a ele se aplica diretamente o Regulamento em relação à atividade de tratamento de dados pessoais. Nesse ponto, dada a novidade da disciplina jurídica referente à figura do subcontratante ou operador, E. J. Kindt suscita questionamento sobre a aplicação do Regulamento ao responsável — que determina as finalidades e os meios de tratamento de dados pessoais — com estabelecimento fora da União Europeia: o GDPR é aplicável em sua totalidade, inclusive ao responsável, desde o momento em que este contrata operador situado em Estado-membro da UE? Ou incidem somente as normas pertinentes ao operador — *e. g.*, Art. 32, sobre segurança no tratamento de dados?[75]

A solução mais apropriada parece ser a da aplicação do Regulamento no limite das normas jurídicas endereçadas ao subcontratante, e não estendê-la, em sua totalidade, para alcançar inclusive empresas sediadas em países não membros da União Europeia (e. g., EUA e países da América Latina) cuja atividade não se encontra compreendida nos termos do Art. 3(1) e Art. 3(2) do GDPR. Do contrário, haveria a vinculação, à normativa europeia, de qualquer entidade responsável no globo que porventura decida otimizar seus serviços de processamento de dados e de tecnologia da informação com a contratação de um operador com base na Europa[76].

Esse aspecto, aliás, poderia colocar o setor europeu de tecnologia da informação em considerável desvantagem concorrencial no mercado internacional. Problemas em matéria de jurisdição e de efetividade na aplicação das sanções do Regulamento pelos tribunais igualmente aparecem[77], visto que tratar-se-ia de uma extensão unilateral da aplicação extraterritorial da lei com discutível legitimidade[78], ao menos do ponto de vista da criação de uma 'jurisdição global' não negociada com terceiros Estados[79].

A extensão unilateral da normativa europeia afigura-se inconsistente com a estruturação atual do sistema internacional, ainda baseado em diferentes soberanias e no respeito ao princípio da não interferência[80]. Eventual mudança de abordagem, em torno

73 "*O tratamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento*, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. [...]." (grifos nossos). UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho.*cit.*

74 VOIGT, Paul; BUSSCHE, Axel von dem (Eds.). *The EU General Data Protection Regulation (GDPR), cit.* . p. 25.

75 KINDT, E. J. Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. *Computer Law and Security Review,* v. 32, n. 5, p. 737, 2016.

76 Ibidem, p. 737.

77 Ibidem, p.737 .

78 Cf. DE HERT, P.; CZERNIAWSKI, M. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. In: *International Data Privacy Law*, v. 6, n. 3, p. 240, 2016.

79 BERMAN, Paul Schiff, The Globalization of Jurisdiction.In: *University of Pennsylvania Law Review*, v. 151, n. 2, p. 311-545, 2002.

80 Em relação à problemática do sistema internacional, ver as reflexões sobre passado, presente e futuro que orbitam o conceito de soberania: KALMO, Hent; SKINNER, Quentin (Ed.). *Sovereignty in Fragments:* The Past, Present and Future of a Contested Concept.

de uma aplicação "universal" de normas de proteção de dados somente seria legítima e legal, do ponto de vista internacional, mediante instrumentos normativos adotados entre Estados e recurso a mecanismos globalmente pactuados de cooperação jurídica internacional.

3.2. Local da atividade de tratamento de dados

O artigo 3(2), trata de previsão legal que enseja significativa mudança no Direito Europeia de Proteção de Dados Pessoais, "uma das mais importantes 'conquistas' da reforma"[81]. Incidirá o Regulamento sobre o tratamento de dados pessoais de pessoas residentes na União Europeia, ainda que tenha sido efetuado por responsável pelo tratamento ou operador **não estabelecidos no território europeu**, quando as operações de tratamento se relacionarem (i) à oferta de bens ou serviços a esses titulares de dados, independentemente da exigência de pagamento; e (ii) ao monitoramento[82] do seu comportamento, desde que tal comportamento tenha lugar na União Europeia.

Do ponto de vista da política normativa adotada, o GDPR fundamentou-se no critério moderado do ponto de destino (*moderate destination approach*)[83]. Ele leva em consideração um específico direcionamento da atividade dos sujeitos — notadamente provedores de aplicação de internet — situados em algum Estado terceiro. Com efeito, o critério moderado do ponto de destino estabelece um nexo de maior proximidade entre a atividade dos agentes de tratamento de informações pessoais e os Estados-membros da União Europeia, resultando em maior legitimidade no exercício da jurisdição prescritiva (perfil regulatório-substantivo, portanto) e na fixação dos seus limites pelo legislador europeu[84].

Vale ressaltar que, nesse sentido, a decisão proferida pela CJUE no caso *Google Spain*[85] foi paradigmática para determinar o alcance da normas de proteção de dados pessoais da União Europeia para além dos limites territoriais do mercado comum e do domínio intracomunitário . A partir desse precedente da Corte, a Diretiva 95/46/CE foi reputada aplicável ao caso, a partir da existência de uma agência ou filial, estabelecida em Estado-membro da União Europeia, e da contratação de publicidade com "ligação inextricável" (*inextricable link*[86]) à atividade de tratamento de dados pessoais por meio

Cambridge University Press, 2010. No plano do Direito Internacional Público, c.f. MELLO, Celso, *Curso de direito internacional público.* Rio de Janeiro : Renovar, 2004.

81 DE HERT, P.; CZERNIAWSKI, M. Expanding the European data protection scope beyond territory. *cit.* , p. 239. Vide, também, BU-PASHA, S. Cross-border issues under EU data protection law with regards to personal data protection. In: *Information & Communications Technology Law*, v. 26, n. 3, p. 218, 2017.

82 Na versão oficial do texto do Regulamento em português europeu, o termo utilizado é "controlo".

83 A respeito desse critério, afirma Uta Kohl: "[...] Os Estados têm, por vezes, no contexto do direito privado, procurado evitar as posições extremas da abordagem do país de origem e da abordagem do país de destino, optando pelo meio termo. Este meio-termo é ocupado por uma abordagem moderada de país de destino, segundo a qual apenas os Estados que foram especificamente visados pela atividade online desfrutam de competência reguladora. Embora esta abordagem evite algumas das falhas teóricas e práticas das posições extremas, está longe de ser perfeita. Em última análise, é cercado pelo mesmo problema de aplicabilidade que qualquer abordagem de país de destino, com a desvantagem de que alguns Estados claramente afetados por certas atividades online têm que se abster de regulamentação." (tradução livre) KOHL, Uta. *Jurisdiction and the Internet:* regulatory competence over online activity. 1ª ed. Cambridge: Cambridge University Press, 2007. p. 25-26.

84 DE HERT, P.; CZERNIAWSKI, M. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. In: *International Data Privacy Law*, v. 6, n. 3, p. 239-243, 2016.

85 UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Grande Secção. Processo C-131/12, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos (AEPD), Mario Costeja González.* Luxemburgo, 13/05/2014. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT>. Acesso em: 15/05/2018.

86 Sobre a adoção do critério da "ligação inextricável" pelo TJUE, vide ARTICLE 29 DATA PROTECTION WORKING PARTY. *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain.* Bruxelas: [s. n.], 2015. p. 4. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf>. Acesso em: 15/05/2018. Vale destacar, segundo a definição lexical oferecida pelo Dicionário CALDAS AULETE, que "inextricável" é tudo aquilo que não se pode desenredar ou se desemaranhar; que se não pode deslindar ou discriminar; que não é possível desembaraçar-se ou sair (alguém); lat. *inextricabilia*.

de um motor de busca, tal como o *Google Search*, ainda que a empresa diretamente responsável pelas operações tenha sede em país terceiro[87].

O Art. 3(2)(a) estabelece inserir-se, no âmbito de aplicação do Regulamento, a atividade de tratamento de dados pessoais de residentes na União Europeia, realizada no contexto do **fornecimento de bens e serviços, ainda que não onerosos**, a eles direcionados. Para a interpretação do texto normativo, é relevante verificar o Considerando n. 23 do GDPR e os parâmetros ali traçados:

> "[...] A fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio *web* do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União."

Já quanto ao artigo 3º, 2, *b*, o dispositivo expressamente estabeleceu ser o **monitoramento comportamental** suficiente para determinar a regência pelo Direito da União Europeia, sendo aplicáveis as normas do GDPR, desde que a conduta dos titulares dos dados ocorra no território da União Europeia. A regra tem ampla aplicação para empresas provedoras de serviços de internet, tais como aplicativos de redes sociais, correio eletrônico e motores de busca, enfim, serviços que de alguma maneira monitoram a atividade *online* de seus usuários, especialmente para fins publicitários É o caso da **publicidade comportamental**, na qual são utilizados principalmente cookies[88].

Deve-se ter atenção, porém, na interpretação dessa hipótese legal de extraterritorialidade. O Regulamento tem em vista que a coleta e o processamento de **informações comportamentais** sobre hábitos de compra na internet, histórico de navegação, modo de uso de dispositivos, e a consequente identificação de interesses e preferências, ensejam sensíveis questões relativas à proteção da privacidade e dos dados pessoais.

87 Cf. BU-PASHA, S. Cross-border issues under EU data protection law with regards to personal data protection.In: *Information & Communications Technology Law*, v. 26, n. 3, p. 218, 2017.

88 "A publicidade comportamental tem por base a observação do comportamento das pessoas ao longo do tempo, procurando estudar as características deste comportamento através das suas acções (várias visitas ao mesmo sítio Web, interacções, palavras-chave, produção de conteúdo em linha [*online*], etc.), com vista a criar um perfil específico e, deste modo, apresentar-lhes anúncios que correspondem aos interesses implícitos no seu comportamento. Enquanto a publicidade contextual e a publicidade segmentada utilizam «instantâneos» daquilo que as pessoas em causa vêem ou fazem num determinado sítio Web ou características conhecidas dos utilizadores, a publicidade comportamental fornece potencialmente aos anunciantes uma imagem muito detalhada da utilização da Internet, com informações sobre muitos dos sítios Web e páginas específicas consultadas, por quanto tempo foram visualizados determinados artigos ou produtos, por que ordem, etc. [...] A maioria das tecnologias de monitorização e publicidade utilizadas no contexto da publicidade comportamental implica algum tipo de tratamento de dados relativos ao cliente. Estas tecnologias utilizam informações armazenadas no programa de navegação e no equipamento terminal do utilizador. Em especial, a tecnologia mais utilizada para monitorizar os utilizadores na Internet baseia-se em «testemunhos persistentes» [*tracking cookies* ou *persistent cookies*]. Os testemunhos permitem monitorizar a navegação de um utilizador na Internet durante um período de tempo alargado e, em teoria, através de vários domínios." (GRUPO DE TRABALHO DO ARTIGO 29º PARA A PROTECÇÃO DE DADOS. *Parecer 2/2010 sobre publicidade comportamental em linha.* Bruxelas: [s. n.], 2010, p. 5-6. Disponível em: <http://www.gpdp.gov.mo/uploadfile/2014/0505/20140505062209480.pdf>. Acesso em: 15/05/2018).

A partir do acesso a essas informações, são traçados perfis dos usuários que, classificados após aplicação do conhecimento preditivo obtido com **técnicas de perfilamento** (*profiling*) automatizado, têm suas vidas cada vez mais afetadas. Níveis de intrusividade sobre a vida, comportamentos e desenvolvimento da personalidade de usuários são intensificados a partir do avanço das implementações de Internet das Coisas (IoT) e do aperfeiçoamento e difusão das tecnologias de inteligência artificial e de decisão algorítmica[89].

Portanto, se essas tecnologias forem empregadas por entidades responsáveis estabelecidas fora do território da União Europeia, de modo a monitorar a conduta *online* e *offline*, e tratar dados pessoais de titular localizado no bloco europeu, muito provavelmente haverá incidência das normas do GDPR .

Nesse sentido, com base na inteligência do Art. 3o, parágrafos 1 e 2, pode-se cogitar alguns dos setores que serão potencialmente atingidos no Brasil pelo âmbito de aplicação material e territorial do Regulamento: (i) empresas brasileiras da área de tecnologia da informação que atuem como subcontratantes ou operadores, efetuando o tratamento de informações de natureza pessoal em nome de entidades responsáveis com estabelecimento na União Europeia; (ii) empresas que desenvolvem atividades relacionadas ao turismo ou ao deslocamento de pessoas residentes na Europa para o Brasil (por exemplo, as companhias aéreas e seus *websites*), que figurem como responsáveis pelo tratamento de dados pessoais; (iii) empresas atuantes no comércio eletrônico com prestação de serviços personalizados ou aplicativos brasileiros que façam uso de programas de rastreamento (*tracking*) dos usuários residentes na União Europeia e técnicas de perfilamento automatizado individual ou coletivo.

3.3. Transferência internacional de dados

A despeito dos elementos de extraterritorialidade do GDPR e efeitos que a normativa europeia pode produzir no sistema jurídico brasileiro ou possíveis conflitos de lei, há ainda a necessidade de se observar as possíveis repercussões em relação à **transferência internacional de dados pessoais,** disciplinada normativamente nos Arts. 44 a 50 do Regulamento Europeu.

Em termos analíticos, uma transmissão transfronteiriça de dados pessoais[90] envolve pelo menos três operações de tratamento: (i) a que tornou disponível as informações pessoais ao agente responsável ou operador (cedente) – *e. g.*, recolha ou coleta dos dados; (ii) a transmissão dessas informações a receptor sediado ou residente em Estado estrangeiro pelo cedente; e (iii) o tratamento que o receptor dos dados pessoais realiza em seu estabelecimento situado em país terceiro (*e. g.*, armazenamento em base de dados)[91].

89 Em relação ao Art. 3(2)(b) atenção merece o Considerando n. 24 do GDPR: "O tratamento de dados pessoais de titulares de dados que se encontrem na União por um responsável ou subcontratante que não esteja estabelecido na União deverá ser também abrangido pelo presente regulamento quando esteja relacionado com o controlo do comportamento dos referidos titulares de dados, na medida em que o seu comportamento tenha lugar na União. A fim de determinar se uma atividade de tratamento pode ser considerada «controlo do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

90 A respeito do tema, vide trabalho publicado pelo IRIS com comentários ao projeto de lei nº 5.276/2016, da Câmara dos Deputados: INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. *Policy Paper - Transferência Internacional de Dados no PL 5276/16.* Belo Horizonte: IRIS, 2017. Disponível em: <http://irisbh.com.br/wp-content/uploads/2017/05/Policy-Papper-Portugues.pdf>. Acesso em: 20/05/2018.

91 GIMÉNEZ, Alfonso Ortega. *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*. Madrid: Agencia Española de Protección de Datos, 2015. p. 61; BU-PASHA, S. Cross-border issues under EU data protection law with regards to personal data protection.*cit*, p. 214.

No esquema jurídico da transferência internacional dados, então, exige-se pelo menos a presença do responsável ou operador **cedente** e o responsável ou operador **receptor** dos dados. Se, à luz do GDPR, quanto ao cedente é inequívoca a aplicação direta da normativa europeia, alguma incerteza pode restar no tocante ao direito aplicável ao receptor[92]. Por essa razão, e para resguardar contra riscos de ofensa a direitos e liberdades fundamentais dos cidadãos europeus titulares dos dados, é que foi adotado, desde a vigência da Diretiva 95/46/CE, o modelo que impõe para transferência de dados a país terceiro a prévia verificação e reconhecimento do **nível de proteção adequado** do país ou organização internacional de destino[93] (Art.45).

Em essência, a regra é ancorada em **modelo geográfico** de regulamentação do fluxo de dados entre fronteiras nacionais, porquanto "objetiva proteger contra riscos gerados pelo país ou localidade para qual os dados serão transferidos".[94] A Comissão Europeia tem a atribuição de analisar o nível de proteção do país terceiro e emitir uma **decisão de adequação** com base nos critérios apontados no Art. 45(2), do Regulamento. Havendo tal decisão — sujeita a revisão quadrienal —, não se demandará prévia e específica autorização para a transmissão internacional de dados.

Além da decisão de adequação, a transferência transfronteiriça de dados pessoais pode ter lastro também (i) caso o país terceiro ou a organização internacional apresentem **garantias adequadas** (Art. 46), ou (ii) a autoridade de proteção de dados competente confeccione **regras empresariais vinculativas** (Art. 47), que hão de ser observadas por grupos de empresas ou grupos econômicos multinacionais no imprescindível fluxo internacional de informações dentro de sua estrutura organizacional. Ressalva, todavia, deve ser feita às derrogações às regras acima para situações específicas de transferência internacional de dados expressamente dispostas no Art. 49 do Regulamento. É o que ocorrerá, por exemplo, no caso da existência de contrato entre responsável pelo tratamento situado na União Europeia e subcontratante estabelecido em país não membro do bloco europeu, que não possui o reconhecimento da Comissão Europeia de oferecer adequado nível de proteção, nem apresenta garantias adequadas (Art.49(1)(c)).

Além de a disciplina do GDPR referente à transmissão de dados entre fronteiras ser pautada no modelo geográfico, também foram incluídas na normativa regras inspiradas no **modelo organizacional** de regulação. Isso porque ele se propõe a lidar com riscos gerados pela entidade que receberá as informações pessoais transferidas[95]. Nesse contexto, o legislador europeu buscou promover uma **responsabilidade organizacional** (*organizational accountability*)[96], a ser obtida mediante a criação, pelos agentes

92 BU-PASHA, S. Cross-border issues under EU data protection law with regards to personal data protection. *cit.*, p. 214.

93 Cf. PIRODDI, Paola. I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati. In: RESTA, Giorgio; ZENO-ZENCOVICH, Vincezo (Coord.). *La protezione transazionale dei dati personali*. Roma: Roma-Tre Press, 2016. p. 198-199.

94 Tradução livre de: "aims to protect against risks posed by the country or location to which the data are to be transferred [...]." (KUNER, Christopher. *Regulation of transborder data flows under data protection and privacy law:* past, present and future. OECD Digital Economy Papers, n. 187, OECD Publishing, 2011. p. 20).

95 KUNER, Christopher. *Regulation of transborder data flows under data protection and privacy law:* past, present and future. OECD Digital Economy Papers, n. 187, OECD Publishing, 2011. p. 20.

96 Em 2010, o Grupo de Trabalho do Artigo 29 emitiu parecer a respeito do princípio da responsabilidade (*principle of accountability*), oportunidade em que reconheceu que, "Em suma, um princípio de responsabilidade legal explicitamente exigiria que os responsáveis pelo tratamento de dados implementassem medidas apropriadas e efetivas para pôr em prática os princípios e obrigações da Diretiva e demonstrassem isso mediante solicitação. Na prática, isso deve se traduzir em programas escalonáveis destinados a implementar os princípios de proteção de dados existentes (às vezes chamados de 'programas de conformidade'). Como complemento do princípio, poderiam ser estabelecidos requisitos adicionais específicos destinados a por em prática salvaguardas de proteção de dados ou garantir a sua eficácia. Um exemplo seria uma provisão exigindo o desempenho de uma avaliação de impacto de privacidade para operações de processamento de dados de alto risco." (tradução livre) ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2010 on the principle of accountability.* Bruxelas: [s. n.], 2010. p.3-5. Disponível em: <http://ec.europa.eu/justice/article-29/documenta-

de tratamento de dados pessoais, de abrangentes programas de gerenciamento de privacidade. Esses programas devem, por exemplo, prever a designação de *data protection officer* (Art. 37), emitir relatório de impacto à privacidade (Art. 35), implementar regras de boas práticas, códigos de conduta (Art. 40), normas corporativas etc., orientações internas e/ou externas aplicáveis, em consonância com o Regulamento, por todo o ciclo de vida da informação objeto de tratamento, independentemente do local ou jurisdição em que esteja.

Os possíveis setores acima indicados são afetados pela imediata aplicação do novo Regulamento europeu. Para ele, ainda não existe decisão que reconheça o Brasil como país terceiro detentor de nível de proteção adequado aos padrões de tutela da privacidade e proteção de dados pessoais da União Europeia. Dessa forma, abre-se uma série de possibilidades para que entidades públicas e privadas brasileiras sejam alcançadas por medidas relacionadas à transferência internacional de dados pessoais em que o cedente seja estabelecido no território europeu.

4. Análise comparativa das repercussões do Regulamento (UE) n. 2016/679 nos direitos brasileiro e argentino

Indiscutivelmente, a mais significativa mudança no panorama regulatório europeu da privacidade de dados decorre da jurisdição prescritiva ampliada da GDPR. Suas normas se aplicam a todas operações de empresas envolvidas no os dados pessoais dos titulares de dados residentes nos Estados-membros da União Europeia, independentemente do local da sede da empresa. Anteriormente, a aplicabilidade territorial da diretiva era ambígua e referia-se ao processo de dados "no contexto de um estabelecimento".

A GDPR inova ao reforçar e explicitar seu âmbito de aplicaçãode forma muito objetiva: será aplicável ao tratamento de dados pessoais por parte de controladores e processadores na União Europeia, independentemente de o processamento ter lugar na União Europeia ou não. A GDPR aplica-se igualmente ao tratamento de dados pessoais de titulares de dados na União Europeia por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades dizem respeito à oferta de bens ou serviços a cidadãos europeus e ao acompanhamento do comportamento de usuários na União Europeia.

O cenário de incertezas quanto à compatibilidade entre a aplicação da GDPR e as normativas nacionais sobre o tema transcende o território europeu, como se pode observar a partir dos próprios princípios de aplicação extraterritorial de seus dispositivos. A busca pela globalização da oferta de serviços digitais no século XXI corrobora a conformação de um sistema internacional cada vez mais interligado por empresas e usuários que atuam em vários mercados, sujeitos a diferentes jurisdições. No contexto de aplicação extraterritorial da GDPR, a partir de um dos mais importantes mercados globais de prestação e consumo de serviços digitais, é natural que outras economias também busquem se adequar ao regime jurídico vigente, de forma a manter sua competitividade no comércio internacional.

Partindo-se dessa conjuntura, as linhas a seguir apresentam alguns paralelos entre a GPDR e as legislações argentina e brasileira, de forma a contextualizar o atual estado da arte da discussão sobre proteção de dados pessoais no domínio do Mercosul

tion/opinion-recommendation/files/2010/wp173_en.pdf>. Acesso em: 15/05/2018.

e entre países da América Latina como um todo.

4.1. Argentina

Há quase vinte anos, desde 2000, a Argentina dispõe de uma Lei de Proteção de Dados Pessoais[97]. Essa legislação também decorre de previsão constitucional específica sobre o tema, que determina, em seu artigo 43, que:

> toda pessoa poderá interpor ação para tomar conhecimento dos dados a ela referidos e de sua finalidade, que constem em registros ou bancos de dados públicos, ou os privados destinados a fornecer informações, e em caso de falsidade ou discriminação, para exigir a supressão, retificação, confidencialidade ou atualização dos mesmos[98].

Ainda que a Argentina tenha sido considerada o primeiro país latino-americano com níveis "adequados" de proteção pela União Europeia por meio das recomendações do Grupo de Trabalho d Artigo 29[99], diversas iniciativas de atualização da Lei estiveram em discussão no Congresso Nacional, entre elas um anteprojeto de lei para uma regulação de proteção de dados, apresentado pela Agência Nacional de Proteção de Dados.

O anteprojeto foi, inclusive, sujeito à consulta pública pelo equivalente ao Ministério da Justiça argentino, com participação do público em geral, instituições acadêmicas, empresas, indivíduos e associações de direitos civis durante o período de reflexão proposto, a exemplo do que ocorreu com o Marco Civil da Internet e seu decreto regulamentador no Brasil. O objetivo dessa consulta foi alinhar a lei argentina de proteção de dados à GDPR.

A lei atual tem várias áreas que abrangem, de maneira conflitante ou distinta, os principais pontos da GDPR. Uma dessas temáticas é a transferência transfronteiriça de dados pessoais de um titular para países com níveis inadequados de proteção de dados. A lei argentina vigente mantém excessivas exceções à regra geral de que as informações pessoais não poderiam ser transferidas para esses países.

De acordo com a Seção 12 da legislação em vigor, é proibida a transferência de qualquer tipo de informação pessoal a países ou entidades internacionais que não ofereçam níveis adequados de proteção, exceto: nos casos de cooperação jurídica internacional; na troca de informações médicas, seja para o tratamento individual de pacientes, seja em pesquisas epidemiológicas; no comércio de valores mobiliários e nas transferências bancárias; por meio de um arcabouço de tratados internacionais dos quais a Argentina é signatária; e quando a transferência é realizada com o propósito de cooperação internacional entre agências de inteligência no combate ao crime, ao terrorismo e ao tráfico de drogas[100].

97 ARGENTINA. *Ley 25.326: Ley de Protección de los Datos Personales.* 30 de Outubro de 2000. Disponível em: <http://www.oas.org/juridico/pdfs/arg_ley25326.pdf>. Acesso em: 16/05/2018.

98 Tradução livre: "Artículo 43. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos." ARGENTINA. *Constitución de la Nación Argentina.* Disponível em: <http://www.oas.org/juridico/mla/sp/arg/sp_arg-int-text-const.html>. Acesso em 17/05/2018.

99 Em tradução livre: "A Comissão [Europeia] até o momento emitiu sete decisões de adequação, reconhecendo Suíça, Canadá, Argentina, [entre outros] como provedores de níveis adequados de proteção". UNIÃO EUROPEIA. European Data Protection Supervisor. *Adequacy decision.* Disponível em: <https://edps.europa.eu/data-protection/data-protection/glossary/a_en>. Acesso em: 21/05/2018.

100 ARGENTINA. *Ley 25.326: Ley de Protección de los Datos Personales.* 30 de Outubro de 2000. Disponível em: <http://www.oas.

Já para as exceções do Art. 23 do Anteprojeto de Lei de Proteção de Dados Pessoais[101], não seria necessário o consentimento do titular dos dados pessoais para a transferência internacional: quando a transferência está prevista por lei ou tratado; quando essa transferência seja necessária para a prevenção ou diagnóstico médico, bem como na gestão de serviços sanitários; quando a transferência internacional é feita para **qualquer empresa do mesmo grupo econômico** do controlador de dados, desde que os dados pessoais sejam utilizados para finalidades que não sejam incompatíveis com aquelas que originaram sua coleta; quando a transferência internacional for necessária a execução de contrato celebrado por interesse inequívoco do titular dos dados, pelo responsável pelo tratamento e por um terceiro; quando a transferência internacional é necessária ou legalmente exigida para salvaguardar um interesse público, ou para a administração pública e da justiça; quando a transferência internacional é necessária para o reconhecimento, exercício ou defesa de um direito em processo judicial; quando a transferência internacional é necessária para a manutenção ou o cumprimento de uma relação jurídica entre o responsável pelo tratamento e o proprietário dos dados.

Ou seja, apesar da vanguarda da Argentina nos anos 2000, no que diz respeito à proteção de dados pessoais e na adequação de seu regime legislativo às diretrizes europeias então vigentes, a atual sistemática de exceções de consentimento para a transferência internacional de dados pode acarretar conflitos com a GDPR à luz do critério da localização do estabelecimento do Art3(1) do Regulamento. Afinal, em ambientes integradosda economia digital no globo, se prestadores argentinos de serviços online cujas atividades envolvam a transferência internacional de dados de cidadãos europeus, ou que sejam subcontratantes com estabelecimento na Argentina mas são contratados por responsável com estabelecimento em país-membro do bloco europeu, por exemplo, aplicam-se também as normativas da GDPR a esses casos *in concreto.* Isso significaria, entre outras coisas, distintos regimes de exceção para aplicabilidade da normativa europeia, e não a argentina, em casos como esse.

Nesse contexto, o Anteprojeto também introduz novas formas de determinar se uma entidade ou determinado processamento de dados estão sujeitos à legislação argentina, bastante semelhante aos critérios encontrados na GDPR. O atual regulamento de proteção de dados da Argentina se aplica a todas as pessoas pessoas jurídicas que realizam o tratamento ou processamento de pessoal dados no país, pertinente a qualquer ação que é considerada tratamento ou processamento de dados pessoais dentro do território argentino. Se um único ato isolado relacionado a dados pessoais (por exemplo, a coleta ou transferência de dados) ocorre na Argentina, mas o restante do processamento é realizado no exterior, a lei argentina se aplica também a essa ação isolada[102].

Sobre esse aspecto, é importante ressaltar que o foco da legislação de 2000 era, entre outras coisas, a introdução de conceitos basilares à proteção de dados pessoais no sistema jurídico argentino. As inovações propostas por esse Anteprojeto superam a temática e, como consequência, refletem preocupações mais atuais, a exemplo da GDPR, como a extensão de seu âmbito de aplicação:

org/juridico/pdfs/arg_ley25326.pdf>. Acesso em: 16/05/2018.

101 Conforme artigo 23 e seguintes. ARGENTINA. *Ley 25.326: Ley de Protección de los Datos Personales.* 30 de Outubro de 2000. Disponível em: <http://www.oas.org/juridico/pdfs/arg_ley25326.pdf>. Acesso em: 16/05/2018.

102 D'AURO, Maximiliano; VARELA, Inés de Achaval. Data protection in Argentina: overview. *Association of Corporate Council's Multi-Jurisdictional Guide 2014/15.* P. 01. Disponível em: <http://www.ebv.com.ar/images/publicaciones/trdatap.pdf>. Acesso em: 16/05/2018.

Artigo 4º - As regras desta lei aplicam-se quando:

a) O responsável pelo tratamento estiver localizado no território nacional, mesmo que quando o processamento de dados ocorra fora do dito território;

b) A pessoa responsável pelo tratamento não está estabelecida no território nacional, mas em um lugar onde a legislação nacional é aplicada sob a lei internacional;

c) O tratamento de dados de proprietários residentes na República Argentina é realizada por um controlador que não esteja estabelecido no território nacional e as atividades desse tratamento estão relacionadas a oferta de bens ou serviços aos titulares dos dados na República Argentina, ou com o acompanhamento de seus atos, comportamentos ou interesses[103].

Se aprovado dessa forma, o Anteprojeto instaura mecanismos de verificação de sua aplicabilidade bastante semelhantes àqueles da GDPR, analisados no item anterior deste estudo.

4.2. Brasil

A proteção dos dados pessoais no Brasil se aproxima do modelo europeu, uma vez que reconhece seu status de direito fundamental como desdobramento da tutela da privacidade[104]. Contudo, o sistema jurídico brasileiro ainda prevê uma normativa fragmentária e insuficiente. Há lei - geral ou especial - que regule de forma abrangente a atividade de tratamento de dados pessoais realizada por entidades públicas e privadas, seja em ambiente interconectado em redes digitais ou não.

Percebe-se desde já, portanto, que reside aí uma significativa diferença da proteção de dados pessoais no Brasil relativamente ao direito argentino.

Em partes, a razão para a disparidade entre os sistemas desses dois países se encontra no texto das suas respectivas Constituições[105]. O teor do Art. 43 da Constituição da Nação Argentina, descrito no item anterior, versa sobre o *habeas data* e lhe confere múltiplas funções a fim de proteger a autodeterminação informativa do indivíduo[106].

Por sua vez, na Constituição da República de 1988, apesar de o direito à privacidade ter sido consagrado no artigo 5º, incisos X e XI, foi no inciso LXXII que o constituinte cuidou diretamente das informações pessoais e de seu estatuto jurídico, positivando a garantia do *habeas data*. Esta, entretanto, possui função jurídica muito restrita se confrontada com o homônimo instituto argentino.

A ação constitucional de **habeas data** no ordenamento jurídico brasileiro tem o propósito de garantir ao cidadão o poder de acesso e retificação dos seus dados pessoais que porventura estejam armazenados em registros governamentais e bancos de dados de caráter público. Como remédio constitucional, na verdade, não é instrumento de concretização da autodeterminação sobre as próprias informações, devido ao seu

103 ARGENTINA. *Anteproyecto de Ley de Protección de los Datos Personales.* 2017. Disponível em: <https://www.justicia2020.gob.ar/wp-content/uploads/2017/02/Anteproyecto-de-ley-PDP.pdf>. Acesso em 17/05/2018.

104 Neste sentido, entre outros: DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006. p. 323-326; LEONARDI, Marcel. *Tutela da privacidade na internet.* São Paulo: Saraiva, 2011. p. 67-90; MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 27-37; MORAES, Maria Celina Bodin de. Ampliando os direitos da personalidade. In: MORAES, Maria Celina Bodin de.(org.)*Na medida da pessoa humana: estudos de direito civil-constitucional.* Rio de Janeiro: Renovar, 2010. p. 140-145; SARLET, Ingo W.; MARINONI, Luiz G.; MITIDERO, Daniel. *Curso de Direito Constitucional.* São Paulo: Revista dos Tribunais, 2012. p. 418.

105 Cf. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais, cit.*p. 326 et seq.

106 Ibidem, p. 349. Sobre o *habeas data* na Argentina, cf. BÁZAN, Víctor. El Hábeas Data Como Medio de Tutela del Derecho Fundamental a la Autodeterminación Informativa. In: *Revista de Direito Público,* Porto Alegre-Brasília, n. 38, p. 205-208, mar./abr. 2011.

âmbito de proteção muito restrito[107]. Considerando que sua gênese é associada ao contexto do fim do regime ditatorial brasileiro, no qual foi adotada a prática de "utilização, por autoridades públicas, de dados inteiramente falsos ou contendo erros, visando a fins políticos e com grave prejuízo de direitos individuais"[108], o *habeas data* tem limitado e peculiar papel no sistema jurídico nacional. Tais características foram observadas na regulamentação do procedimento pela Lei nº 9.507/1997. Da mesma forma, a natureza das informações acessadas é muito específica: como instrumento de proteção de direitos da personalidade via remédio constitucional, o *habeas data* alcança apenas dados a serem conhecidos ou retificados, que se refiram à pessoa do impetrante, e destituídos de caráter genérico[109]. Nesse sentido de análise, ele pressupõe uma espécie de autodeterminacão 'contida' de dados.

Em 1990, sob a influência do *Fair Credit Reporting Act* norte-americano, o **Código de Defesa do Consumidor (CDC)** buscou tutelar a pessoa vulnerável no mercado de consumo relativamente aos bancos de dados criados, em particular com escopo e proteção ao crédito, como se pode verificar em seus Arts. 43 e 44[110]. A bem da verdade, o CDC foi a primeira lei especial que, em sede infraconstitucional, disciplinou a atividade de tratamento de dados pessoais. Contudo, o enfoque estatutário de estabelecer certo equilíbrio na coleta de informações sobre inadimplemento do consumidor para fins de concessão de crédito[111], reduziu o alcance da aplicação de suas normas.

Ainda assim, uma série de preceitos positivados no CDC especificam normas estruturantes da proteção de dados pessoais, de modo a afastar a incompreensão muitas vezes disseminada de que inexiste base legal no Brasil para esse campo: (i) possibilidade de acesso às informações do consumidor armazenadas nos bancos de dados (*princípio do acesso*); (ii) os dados devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão (*princípio da qualidade dos dados*); (iii) necessidade de comunicação da formação de base de dados sobre consumidor(es) (*princípio da transparência*); (iv) limite de 5 (cinco) anos para armazenamento de informações negativas (*princípio da necessidade*)[112].

Com a edição da Lei nº 12.414/2011, o regramento relativo aos bancos de dados de consumidores foi complementado com o tratamento dos cadastros de adimplemento[113]. A legislação visa regular a formação de **históricos de crédito** dos consumidores, em que os bancos de dados são alimentados regularmente com "informações positi-

107 Segundo MENDES, Gilmar. *Curso de Direito Constitucional.* 12.ed. São Paulo: Saraiva, 2017, pp.459-60, "uma reflexão livre sobre o tema há de indicar que o objeto protegido pelo 'habeas data' só em parte traduz a preocupação hoje manifestada pela ideia de autodeterminação sobre dados pessoais desenvolvidas em várias ordens constitucionais". O autor ressalva, contudo, que o texto constitucional não deixa dúvidas de que o instituto protege a pessoa não somente em relação a banco de dados de caráter público geridos por entidades governamentais diretamente; ele também se destina a tutelar a pessoa em relação a banco de dados de caráter público geridos por entes privados.

108 DALLARI, Dalmo de Abreu. O *habeas data* no sistema jurídico brasileiro. In: *Revista da Faculdade de Direito da Universidade de São Paulo*, São Paulo, v. 97, p. 242, 2002.

109 Cf. Gilmar F. MENDES, *Curso de Direito Constitucional.* 12.ed. cit., p.460.

110 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes; [...] Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor. BRASIL. Lei nº 8.078, de 11 de setembro de 1990. *Código de Defesa do Consumidor.* Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Acesso em 21/05/2018.

111 DONEDA, Danilo. *A proteção dos dados pessoais nas relações de consumo:* para além da informação creditícia. Brasília: SDE/DPDC, 2010. p. 11.

112 Cf. MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 142-143.

113 BRASIL. *Lei nº 12.414*, de 9 de junho de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 21/05/2018.

vas"[114]. Trata-se de lei importante para a tutela do titular dos dados diante das empresas de classificação de crédito (*credit scoring*), que tratam esses dados para avaliar de forma personalizada o grau de risco na concessão de crédito pessoal.

O Código Civil de 2002, por sua vez, destinou apenas o artigo 21[115] à disciplina do direito à privacidade, ignorando por completo a noção de proteção de dados pessoais, suas restrições frente a outros direitos e liberdades (*e. g.,* liberdade de expressão e comunicação), e toda a complexidade que é própria da contemporânea sociedade da informação, hiperconectada, com acesso cada vez mais difuso às tecnologias da informação e da comunicação. Nas palavras de Anderson Schreiber, "[a] mera observação da vida cotidiana revela que, ao contrário da assertiva retumbante do art. 21, a vida privada da pessoa humana é violada sistematicamente"[116].

Já a Lei nº 12.527 de 2011, a **Lei de Acesso à Informação (LAI)**[117], é aplicável aos órgãos e entidades da administração pública direta e indireta. Com o objetivo de promover uma administração pública transparente e dar certa concretude ao direito à informação dos brasileiros, a LAI desempenha importante papel na área da proteção dos dados pessoais. Além de conceber informação pessoal praticamente nos mesmos termos que a legislação europeia (artigo 4º, IV)[118], determina que o titular dos dados terá acesso às informações que lhe sejam pertinentes, e que a privacidade e proteção dos dados pessoais configura limite ao acesso à informação por parte de terceiros (artigos 6º, 31 e 32)[119].

Em complementação a esse arcabouço jurídico, o direito à proteção dos dados pessoais também foi expressamente inscrito no texto na Lei nº 12.965 de 2014, o **Marco Civil da Internet**[120]. As disposições do Marco Civil da Internet são aplicáveis a qualquer operação relacionada à coleta, ao armazenamento, à retenção, ao tratamento e à comunicação de dados pessoais por provedores de conexão e provedores de aplicativos de internet, quando pelo menos uma dessas ações ocorre no Brasil. Reconhecido como legislação pioneira no mundo e exemplo do multissetorialismo que caracteriza a governança da internet, o Marco Civil estabeleceu, em seu artigo 3º, III, elaboração de lei es-

114 Para Leonardo Roscoe Bessa, "[e]mbora sob a ótica exclusivamente econômico-financeira seja possível justificar que não apenas o *histórico de crédito* do candidato ao empréstimo, mas também outras informações são auxiliares para uma melhor definição do perfil da pessoa e, consequentemente, para possibilitar análise de risco mais precisa, evitando a inadimplência, e, ao mesmo tempo, a possibilidade de taxa de juros menor, o enfoque jurídico aponta em outra sentido: o da necessidade de delimitar e restringir o número, a qualidade e a forma de tratamento de informações positivas pelos bancos de dados de proteção ao crédito. O aumento de número de informações pessoais pode representar ofensa à dignidade da pessoa humana, aos direitos da personalidade (privacidade e honra)." (BESSA, Leonardo Roscoe. *Cadastro positivo: comentários à Lei 12.414, de 09 de julho de 2011*. São Paulo: Revista dos Tribunais, 2011. p. 45),

115 "Art. 21, Código Civil:. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma"BRASIL. Lei nº 10.406, de 10 de janeiro de 2002.

116 SCHREIBER, Anderson. *Direito da personalidade.* 2. ed. rev. e atual. São Paulo: Atlas, 2013, p. 142-143.

117 BRASIL. Lei nº 12.527, de 18 de novembro de 2011. *Lei de Acesso à Informação.* Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 21/05/2018.

118 "Art. 4º Para os efeitos desta Lei, considera-se: [...] IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável".

119 "Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a: [...] III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso. [...] Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. Art. 32. Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar: [...] IV - divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal".

120 Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; [...] Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. [...] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.BRASIL. Lei nº 12.956, de 23 de abril de 2014. *Marco Civil da Internet.* Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 21/05/2018.

pecífica para a proteção de dados, matéria suscetível, portanto, à atividade legiferante.

Em relação a dispositivos que regulam a **transferência internacional de dados** no Brasil, a proteção de dados oferecida pelo Marco Civil da Internet ainda é limitada quando comparada ao complexo sistema previsto pela GDPR[121]. O Projeto de Lei 5.276, enviado ao Congresso Nacional pela Presidência da República, no dia 13 de maio de 2016, é um dos principais projetos de lei de proteção de dados pessoais atualmente em discussão no Congresso Nacional e tem um capítulo completo destinado a regular as transferências internacionais.

Ainda no âmbito do Poder Executivo, o então Anteprojeto de Lei sobre Proteção de Dados seguiu o modelo de consulta pública em que o Marco Civil foi baseado. O texto do Ministério da Justiça foi disponibilizado online e aberto a comentários de quaisquer usuários. Desse modo, tal qual no processo de elaboração do Marco Civil, viabilizou-se o debate entre múltiplos atores: membros da sociedade civil, academia, setores governamentais, regulatórios e indústria. De modo geral, o Projeto de Lei trata de temas como os direitos dos usuários e o tratamento, coleta e armazenamento de dados pessoais.

A análise do Projeto de Lei nº 5.276/2016, especialmente no que diz respeito a dispositivos referentes à transferência internacional de dados, revela forte influência do modelo europeu de proteção de dados sobre a futura disciplina normativa no Brasil. O modelo europeu adota um **critério essencialmente geográfico** para definir as situações em que a transferência internacional de dados é permitida ou não. Em um mundo cada vez mais globalizado, regulações baseadas em critérios territoriais se revelam problemáticas e obsoletas, na medida em que a geografia passa a importar cada vez menos no âmbito da tecnologia e dos negócios.

O Instituto de Referência em Internet e Sociedade já se posicionou no sentido de recomendar a adoção de um **modelo organizacional** para essas hipóteses[122], e não geográfico, capaz de transcender as fronteiras dos Estados, fazendo com que o nível de proteção dos dados os acompanhe por onde seguirem ou fluírem, uma vez que os deveres de diligência são atribuídos à entidade que os coleta e não ao Estado para onde serão transferidos os dados. O modelo organizacional seria plenamente compatível e consistente com o disposto no Art. 11 do Marco Civil da Internet, que demanda a aplicação da lei brasileira aos dados coletados no Brasil, e não resultaria em entraves jurisdicionais pelo fato de os dados terem sido transferidos para outras jurisdições.

O modelo organizacional, conforme recomendado pelo IRIS, tem a vantagem de contornar esses problemas obrigando as entidades exportadoras a manter proteção contínua de dados pessoais transferidos para outras organizações, independentemente de sua localização geográfica. A proteção realizar-se-ia por meio da obrigatoriedade de cláusulas contratuais entre exportador e importador de dados, bem como da responsabilidade solidária entre eles[123].

121 Esse tema foi tratado de forma abrangente e minuciosa, especialmente no que diz respeito às propostas em pauta no Congresso Nacional, por meio do Projeto de Lei 5.276, em estudo publicado pelo IRIS - Instituto de Referência em Internet e Sociedade, de 2017, intitulado *Policy Paper - Transferência Internacional de Dados no PL 5276/16.* Belo Horizonte: IRIS, 2017. Disponível em: <http://irisbh.com.br/wp-content/uploads/2017/05/Policy-Papper-Portugues.pdf>. Acesso em: 20/05/2018.

122 INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. *Policy Paper - Transferência Internacional de Dados no PL 5276/16,* p.33. Belo Horizonte: IRIS, 2017. Disponível em: <http://irisbh.com.br/wp-content/uploads/2017/05/Policy-Papper-Portugues.pdf>. Acesso em: 20/05/2018.

123 Na prática, o modelo organizacional é mais centrado no fortalecimento dos eixos da responsabilidade compartilhada entre os agentes econômicos atuantes nos mercados da economia digital, computação, informática e internet, em geral; nele, as autoridades de proteção de dados teriam muito mais um papel regulatório e de conformidade, restando nas empresas importadoras e exportadoras de dados o dever primário de preservar a higidez da proteção dos dados tratados e processados na cadeia da transferência. O modelo geográfico, por sua vez, pode padecer de riscos de degradação da própria qualidade regulatória, considerando que deveres de diligência

O Art. 33 do PL 5.276/2016, se aprovado, estabelecerá que uma transferência internacional apenas seria permitida se fornecida a países com níveis equivalentes de proteção de dados, ou quando expressamente consentida por titulares de dados, após informações específicas sobre a natureza internacional da operação e os riscos envolvidos.

O Projeto de Lei nº 5.276/2016 não é o único que aborda os problemas de proteção de dados atualmente no Brasil. Outras propostas legislativas estão em tramitação no Congresso Nacional: o Projeto de Lei nº 4.060/2012, de autoria do deputado Milton Monti, e o Projeto de Lei nº 181/2014, de autoria do senador Vital do Rego. Em julho de 2016, devido a uma proposta do deputado Alexandre Leite, o PL 5276/2016 foi apensado ao PL 4.060/2012, o que contribuiu para restaurar a incerteza quanto à aprovação do texto base.

Importante destacar que o Projeto de Lei 5276/2016 é o que mais se aproxima do design legislativo vislumbrado pela GDPR. Em muitos aspectos, o essa proposta é a melhor referência para o início da discussão no país. O PL 4060/2012, por sua vez, está alinhado com os interesses de conglomerados de marketing digital, com o objetivo de facilitar acesso a dados dos consumidores para fins de marketing e alavancagem de modelos de negócios e oferta de produtos e serviços nessa área. Por fim, o PL 181/2014 já não é tão abrangente quanto o Projeto de Lei 5276/2016, nem tão restritivo quanto o PL 4060/2012.

5. Conclusões e recomendações

O GDPR não é apenas direito vigente para a União Europeia; seu alcance é, indubitavelmente, global[124]. Agentes econômicos atuantes em mercados de países que interagem com a União Europeia, ou que pretendem se inserir nos novos segmentos de mercado na economia digital contemporânea devem se preocupar com possíveis alinhamentos de suas legislações de proteção de dados de seus países à GDPR, em vigor desde 25 de maio de 2018

Nesse cenário, as preocupações de *compliance* com os novos parâmetros apresentados pela GDPR levam atores de diferentes setores da economia da informação a adotar medidas jurídicas e técnicas no campo da proteção de dados pessoais. Entre as ações pertinentes, podem-ser mencionadas a revisão de contratos e acordos, atualização de termos de uso de usuários e políticas de privacidade ao redor do mundo, bem como a adoção de novas estruturas corporativas para a efetivação da proteção de dados.

A conformidade aos novos preceitos normativos estabelecidos pelo novo Regulamento Europeu deve ser a pauta principalmente de empresas ou de organizações internacionais receptoras de informações pessoais provenientes da União Europeia, entidades responsáveis pelo tratamento de informações ou subcontratante a quem se aplica o Regulamento, na forma do seu Art. 3º.

Igualmente, a partir das considerações a respeito das repercussões extraterritoriais da GDPR, como pano de fundo para a análise comparativa dos direitos argentino

são atribuídos primariamente ao Estado para onde serão transferidos os dados (país destino, país receptor), e não à pessoa jurídica ou natural que os coleta. Sobre as distintas variações e aplicações do modelo, cf. IRIS, *Policy Paper - Transferência Internacional de Dados no PL 5276/16*, cit., p.33 ss.

124 MADGE, Robert. *GDPR's global scope:* the long story. Disponível em: <https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f>. Acesso em: 14/05/2018.

e brasileiro, o Instituto de Referência em Internet e Sociedade entende que o Estado brasileiro, notadamente mediante os órgãos dos poderes executivo e legislativo, devem adotar medidas e endereçar práticas domésticas que se alinhem a um objetivo de maximização do objetivo de proteção de dados pessoais, dentre as quais:

> (i) comprometer-se com a aprovação da uma lei geral de proteção dos dados pessoais, que abranja a atividade de tratamento de informações por entes públicos e privados, e que se paute no risco gerado às pessoas naturais, com garantias adequadas à proteção dos direitos e liberdades fundamentais dos titulares dos dados, tal como se vê na GPDR;
>
> (ii) proceder à adesão à Convenção N. 108 do Conselho da Europa, tratado internacional mais expressivo sobre tutela da privacidade no contexto do fluxo transfronteiriço de dados, que foi recentemente atualizado às novas demandas de sociedades permeadas de tecnologias orientadas por dados[125] e que permite adesões por Estados não membros do Conselho da Europa[126];
>
> (iii) desenvolver e adotar políticas públicas, ações governamentais, além de programas educativos envolvendo atores do legislativo, legislativo, judiciário, academia, setores da indústria, organizações da sociedade civil e cidadãos, para disseminação de conhecimento e prática em torno da proteção de dados pessoais e, espera-se, da futura Lei.

Essas recomendações se fundamentam em razões de ordem interna e externa. A edição de lei regulamentadora da atividade de tratamento de dados pessoais no Brasil, além de atender ao imperativo da Constituição da República de 1988 e de princípios e diretrizes do Marco Civil relativamente à tutela da privacidade e proteção dos dados de caráter pessoal, também manterá o país em posição estratégica relação ao Estados-membros da União Europeia e dentro do bloco do Mercosul. Como visto, a Argentina já discute a reforma de sua legislação para se adaptar à GDPR e ao novo contexto da economia digital e o Brasil deveria se integrar a esse debate e promover medidas mais consentâneas com a posição que ocupa entre as grandes economias do globo.

6. Referências Bibliográficas

6.1. Livros e capítulos de livro

BESSA, Leonardo Roscoe. *Cadastro positivo*: comentários à Lei 12.414, de 09 de julho de 2011. São Paulo: Revista dos Tribunais, 2011.

CONSELHO EUROPEU. *Manual da Legislação Europeia sobre Proteção de Dados,* 2014. Disponível em <https://rm.coe.int/16806ae65f>. Acesso em 10/05/2018.

DONEDA, Danilo. *A proteção dos dados pessoais nas relações de consumo:* para além da informação creditícia. Brasília: SDE/DPDC, 2010.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

125 COUNCIL OF EUROPE. *Enhancing data protection globally:* Council of Europe updates its landmark convention, 2018. Disponível em: <https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808ac976>. Acesso em: 07/06/2018.

126 Cf. procedimento previsto no Artigo 23 da Convenção - Adesão de Estados não membros: (1)- Após a entrada em vigor da presente Convenção, o Comité de Ministros do Conselho da Europa poderá convidar qualquer Estado não membro do Conselho da Europa a aderir à presente Convenção mediante decisão tomada pela maioria prevista na alínea d) do artigo 20º do Estatuto do Conselho da Europa e por unanimidade dos representantes dos Estados contratantes com direito de assento no Comité. (2) Para qualquer Estado aderente, a Convenção entrará em vigor no 1º dia do mês seguinte ao termo de um prazo de três meses após a data do depósito do instrumento de adesão junto do Secretário-Geral do Conselho da Europa.

GIMÉNEZ, Alfonso Ortega. *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita.* Madrid: Agencia Española de Protección de Datos, 2015.

KALMO, Hent; SKINNER, Quentin (Ed.). *Sovereignty in Fragments:* The Past, Present and Future of a Contested Concept. Cambridge University Press, 2010.

KAPLAN, Harvey. COWING, Mark. EGLI, Gabriel. *A Primer for Data-Protection Principles in the European Union.* Culture Clash! Data Protection, Freedom of Information and Discovery, 2009.

KOHL, Uta. *Jurisdiction and the Internet:* regulatory competence over online activity. 1ª ed. Cambridge: Cambridge University Press, 2007.

LEONARDI, Marcel. *Tutela da privacidade na internet.* São Paulo: Saraiva, 2011.

MELLO, Celso, *Curso de direito internacional público.* Rio de Janeiro : Renovar, 2004.

MENDES, Gilmar. Curso de Direito Constitucional. 12.ed. São Paulo: Saraiva, 2017

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MILLARD, Christopher (Ed.). *Cloud Computing Law*. Oxford: Oxford University Press, 2013. E-book.

MORAES, Maria Celina Bodin de. Ampliando os direitos da personalidade. In: _____. *Na medida da pessoa humana:* estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010. p. 121-148.

PIRODDI, Paola. I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati. In: RESTA, Giorgio; ZENO-ZENCOVICH, Vincezo (Coord.). *La protezione transazionale dei dati personali.* Roma: Roma-Tre Press, 2016. p. 169-238.

SARLET, Ingo W.; MARINONI, Luiz G.; MITIDERO, Daniel. *Curso de Direito Constitucional.* São Paulo: Revista dos Tribunais, 2012.

SCHREIBER, Anderson. *Direito da personalidade.* 2. ed. rev. e atual. São Paulo: Atlas, 2013.

VOIGT, Paul; BUSSCHE, Axel von dem (Eds.). *The EU General Data Protection Regulation (GDPR):* A Practical Guide. [s.l]: Springer, 2017.

6.2. Artigos científicos

ALBRECHT, Jan. P. How the GDPR Will Change the World. *European Data Protection Law Review*, v. 2, n. 3, p. 287–289, 2016.

BÁZAN, Víctor. El Hábeas Data Como Medio de Tutela del Derecho Fundamental a la Autodeterminación Informativa. *Revista de Direito Público*, Porto Alegre-Brasília, n. 38, p. 191-231, mar./abr. 2011.

BERMAN, Paul Schiff, The Globalization of Jurisdiction, *University of Pennsylvania Law Review*, v. 151, n. 2, p. 311-545, 2002.

BIONI, Bruno. *Xeque-Mate*: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Grupo de Estudos em Políticas Públicas em Acesso à Informação da USP – GPOPAI, São Paulo, 2015.

BU-PASHA, S. Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law*, v. 26, n. 3, p. 213–228, 2017.

BYGRAVE, Lee. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology*, volume 6, pp. 247–284, 1998.

DALLARI, Dalmo de Abreu. O *habeas data* no sistema jurídico brasileiro. *Revista da Faculdade de Direito da Universidade de São Paulo*, São Paulo, v. 97, p. 239-253, 2002.

DE HERT, P.; CZERNIAWSKI, M. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*, v. 6, n. 3, p. 230–243, 2016.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico,* Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

D'AURO, Maximiliano; VARELA, Inés de Achaval. Data protection in Argentina: overview. *Association of Corporate Council's Multi-Jurisdictional Guide 2014/15.* Disponível em: <http://www.ebv.com.ar/images/publicaciones/trdatap.pdf>. Acesso em: 16/05/2018.

GUIDI, Guilherme. *Modelos regulatórios para proteção de dados pessoais.* Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 30/04/2018.

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. *Policy Paper - Transferência Internacional de Dados no PL 5276/16.* Belo Horizonte: IRIS, 2017. Disponível em: <http://irisbh.com.br/wp-content/uploads/2017/05/Policy-Papper-Portugues.pdf>. Acesso em: 20/05/2018.

JONES, Meg. The right to a human in the loop: Political constructions of computer automation and personhood. *Social Studies of Science***,** v. 47, n. 2, p. 216 - 239, 2017.

KINDT, E. J. Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. *Computer Law and Security Review*, v. 32, n. 5, p. 729–748, 2016.

KUNER, Christopher. *Regulation of transborder data flows under data protection and privacy law*: past, present and future. OECD Digital Economy Papers, n. 187, OECD Publishing, 2011.

SELBST, Andrew; POWLES, Julia. Meaningful information and the right to explanation. *International Data Privacy Law*, v. 7, n. 4, p. 233–242, 2017.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, v. 7, n. 2, p. 76-99, 2017.

6.3. Legislação

ARGENTINA. *Anteproyecto de Ley de Protección de los Datos Personales.* 2017. Disponível em: <https://www.justicia2020.gob.ar/wp-content/uploads/2017/02/Anteproyecto-de-ley-PDP.pdf>. Acesso em 17/05/2018.

_____. *Constitución de la Nación Argentina.* Disponível em: <http://www.oas.org/juridico/mla/sp/arg/sp_arg-int-text-const.html>. Acesso em 17/05/2018.

_____. *Ley 25.326: Ley de Protección de los Datos Personales.* 30 de Outubro de 2000. Disponível em: <http://www.oas.org/juridico/pdfs/arg_ley25326.pdf>. Acesso em: 16/05/2018.

BRASIL. Lei 10.406, de 10 de janeiro de 2002. *Código Civil.* Disponível em: <http://www.planalto.gov.br/CCivil_03/Leis/2002/L10406.htm>. Acesso em 21/05/2018.

_____. *Lei nº 12.414,* de 9 de junho de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 21/05/2018.

_____. Lei nº 12.527, de 18 de novembro de 2011. *Lei de Acesso à Informação.* Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 21/05/2018.

_____. Lei nº 12.956, de 23 de abril de 2014. *Marco Civil da Internet.* Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 21/05/2018.

_____. Lei nº 8.078, 11 de setembro de 1990. *Código de Defesa do Consumidor.* Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Acesso em 21/05/2018.

CONSELHO EUROPEU. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Estrasburgo, 1981. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 02/05/2018;

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, Estrasburgo, 24/10/1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31995L0046>. Acesso em: 15/05/2018.

_____. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, Estrasburgo, 04/05/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 16/04/2018.

6.4. Decisões judiciais

UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos., *Acórdão Leander c. Suécia* de 26 de março de 1987, petição n.º 9248/81. Disponível: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}>. Acesso em: 10/05/2018;

_____.Corte Europeia de Direitos Humanos, *Acórdão S. and Marper c. Reino Unido* de 4 de dezembro de 2008, petições n.ºs 30562/04 e 30566/04. Disponível em: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}> Acesso em 11/05/2018.

_____. Corte Europeia de Direitos Humanos. *Acórdão Klass e o. c. Alemanha* de 6 de setembro de 1978, petição n.º 5029/71. Disponível em:<https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}>. Acesso em: 05/05/2018; TEDH, acórdão Uzun c. Alemanha de 2 de Setembro de 2010, petição n.º 35623/05. Disponível em: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-100293%22]}>. Acesso em 10/05/2018.

_____. Corte Europeia de Direitos Humanos. *Acórdão Malone c. Reino Unido* de 2 de agosto de 1984, petição n.º 8691/79. Disponíveis em: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57533%22]}>. Acesso em 12/05/2018; TEDH, acórdão Copland c. Reino Unido de 3 de abril de 2007, petição n.º 62617/00. Disponível em: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-79996%22]}> Acesso em 15/05/2018.

_____. Court of Justice of European Union. Third Chamber. Case C-230/14, *Weltimmo s. r. o.* v. *Nemzeti Adatvédelmi és Információszabadság Hatóság*. LuxemburgO, 01/10/2015. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN>. Acesso em 10/05/2018.

_____. Tribunal de Justiça da União Europeia. Grande Secção. Processo C-131/12, *Google Spain SL, Google Inc.* c. *Agencia Española de Protección de Datos (AEPD), Mario Costeja González.* Luxemburgo, 13/05/2014. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT>. Acesso em: 15/05/2018.

6.5. Outros textos e documentos

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Officers ('DPOs').* Disponível em: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>. Acesso em: 02/05/2018.

_____. *Opinion 3/2010 on the principle of accountability*. Bruxelas: [s. n.], 2010. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf>. Acesso em: 15/05/2018.

_____. *Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* Bruxelas: [s. n.], 2014. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Acesso em: 23/05/2018.

_____. *The Role of the Data Protection Officer,* 2017. Disponível em:<https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/DPO%20Update%20Article%20Final.pdf>. Acesso em 30/04/2018.

_____. *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain.* Bruxelas: [s. n.], 2015. p. 4. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf>. Acesso em: 15/05/2018.

BIONI, Bruno; e MONTEIRO, Renato. *O papel do Data Protection Officer*. 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-papel-do-data-protection-officer-04122017>. Acesso em: 28/04/2018.

BUERGER, Sarah. *How the GDPR changed the Argentina Personal Data Protection Act.* 2017. Disponível em: <https://www.michalsons.com/blog/argentina-personal-data-protection-act/25090>. Acesso em: 16/05/2018.

CAMERON, Stephen. *'Light Reading 'The Digital Economy & GDPR',* 2017 Disponível em: <http://www.lightreading.com/oss-bss/subscriber-data-management/the-digital-economy-and-gdpr/a/d-id/730582> Acesso em: 04/05/2018.

GRUPO DE TRABALHO DO ARTIGO 29º PARA A PROTECÇÃO DE DADOS. *Parecer 2/2010 sobre publicidade comportamental em linha.* Bruxelas: [s. n.], 2010. Disponível em: <http://www.gpdp.gov.mo/uploadfile/2014/0505/20140505062209480.pdf>. 21/05/2018.

COUNCIL OF EUROPE. *Enhancing data protection globally:* Council of Europe updates its landmark convention**,** 2018. Disponível em: <https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808ac976>. Acesso em: 07/06/2018.

MADGE, Robert. *GDPR's global scope:* the long story. Disponível em: <https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f>. Acesso em: 14/05/2018.

SOLON, Olivia. *How Europe's 'breakthrough' privacy law takes on Facebook and Google.* 2018. Disponível em: <https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation>. Acesso em: 09/05/2018.

THE GUARDIAN, *Costeja González and a memorable fight for the 'right to be forgotten'*, 2014. Disponível em: <https://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten>. Acesso em 05/05/2018.

UNIÃO EUROPEIA. European Data Protection Supervisor. *Adequacy decision.* Disponível em: <https://edps.europa.eu/data-protection/data-protection/glossary/a_en>. Acesso em: 21/05/2018.

7. Anexo

7.1. Temas sistematizados da GDPR

Sistematização do Regulamento geral de proteção de dados pessoais

Capítulo I

Artigos 1 – 4

- Disposições gerais (âmbito e objetivos, definições).

Capítulo II

Artigos 5 – 11

- Princípios;
- Princípios que regem o processamento de dados;
- Bases legais;
- Crianças, categorias confidenciais de dados pessoais;
- Processamento que não requer identificação.

Capítulo III

Artigos 12 – 23

- Direitos do titular dos dados;
- Direito à transparência e à informação;
- Direito ao acesso;
- Direito à retificação;
- Direito à exclusão (”Direito de ser esquecido”);
- Direito à retificação;
- Direito à restrição de processamento;
- Direito à portabilidade de dados;
- Direito à objeção;

- Direito a não estar sujeito a decisões automáticas.

Capítulo IV

Artigos 24 – 43

- Responsabilidade do “Controller”;
- Proteção de dados por concepção e padrão;
- Controllers conjuntos;
- Representantes de controllers sem estabelecimento na UE;
- Função e obrigações do “Processador”;
- Obrigação de garantir a segurança do processamento de dados;
- Notificação de Violação (Artigos 33, 34);
- Avaliações do impacto da proteção de dados;
- Obrigação de ter um oficial de proteção de dados / escopo e atribuições;
- Códigos de conduta e certificações.

Capítulo V

Artigos 44 – 50

- Transferência Internacional de Dados a outros países;
- Adequação, cláusulas modelos, normas corporativas obrigatórias.

Capítulo VI

Artigos 51 – 59

- Autoridades fiscalizadoras independentes (autoridades de proteção de dados/ DPAs);
- Requisitos, escopo, competência, atribuições e poderes;
- Os poderes incluem o poder de impor uma multa administrativa de até 4% do faturamento mundial no caso de violação da Regulamentação.

Capítulo VII

Artigos 60 – 76

- Estruturas de Cooperação e consistência na aplicação da lei;
- Cooperação entre DPAs e a “loja com atendimento único” (loja de 28 tipos de atendimento);
- “Mecanismo de consistência”;
- Criação do Conselho Europeu de Proteção de Dados (EDPB).

Capítulo VIII

Artigos 77 – 91

- Recursos, responsabilidades e penalidades;
- Direitos do titular dos dados;
- Providenciar ações representativas em nome dos titulares dos dados, se tais órgãos existirem;
- Condições para a imposição de multas administrativas e outras penalidades.

Capítulo IX

Artigos 85 – 91

- Disposições relativas a situações específicas de processamento;
- Liberdade de expressão e informação;
- Acesso público a documentos oficiais.

Capítulo X

Artigos 92 – 93

- Atos delegados e de implementação;
- Participação da comissão além do EDPB;

- Atos delegados somente precisam ser comunicados ex post ao EP e ao Conselho;
- Comitologia.

Capítulo XI

Artigos 94 – 99

- Disposições finais;
- Anulação da atual Diretiva de Proteção de Dados de 1995;
- Relação com a atual Diretiva ePrivacy 2002/58/EC;
- Entrada em vigor e aplicação.