SÉRIE **PROFESSOR EDVALDO BRITO**

Proteção de dados pessoais: novas perspectivas

Maurício Requião
Organizador

EDUFBA

Como é que o Instagram sabe que quero comprar uma geladeira nova? Por que a Netflix me indicou esse filme? Não vou ler esses termos de privacidade, só aceitar. Estas são, muito provavelmente, vivências pelas quais boa parte dos leitores já passaram.

À medida que a tecnologia avança, ampliando a parte da vida que é mediada pelo mundo digital, novas comodidades e igualmente novos desafios são trazidos à sociedade contemporânea. Um desses desafios diz respeito à proteção de dados pessoais, tema sobre o qual versa esta obra. Cada interação realizada na Internet, e frequentemente até fora dela, pode significar a coleta de dados pessoais, muitas vezes sequer sem o conhecimento de seus titulares. Estes dados vêm sendo utilizados por empresas e governos não apenas para analisar tendências e comportamentos, como também para os influenciar ou mesmo predizê-los. Esta obra se propõe a analisar esta questão sob diversas perspectivas.

Bárbara Veiga Góes
Daniel de Araújo Paranhos
Diego Carneiro Costa
Edilton Meireles
Fernando Araújo dos Santos
Fernanda Rêgo Oliveira Dias
Jéssica Andrade Modesto
Laércio Martins
Laura Lucia da Silva Amorim
Lorena Esquivel de Brito
Marcos Ehrhardt Jr.
Maria Clara Seixas
Marta Carolina Giménez Pereira
Maurício Requião
Mayana Barbosa Oliveira
Rafael da Silva Santana
Rafaela Lamêgo e Aquino Rodrigues de Freitas
Rodrigo Castro Nascimento
Salvador Morales Ferrer
Teila Rocha Lins D'Albuquerque
Wendel Machado de Souza

Apoio:
Programa de Pós-Graduação em Direito (PPGD/UFBA)
Proap/Capes

SÉRIE **PROFESSOR EDVALDO BRITO**

Maurício Requião
Organizador

Proteção de dados pessoais: novas perspectivas

Bárbara Veiga Góes, Daniel de Araújo Paranhos, Diego Carneiro Costa, Edilton Meireles, Fernando Araújo dos Santos, Fernanda Rêgo Oliveira Dias, Jéssica Andrade Modesto, Laércio Martins, Laura Lucia da Silva Amorim, Lorena Esquivel de Brito, Marcos Ehrhardt Jr., Maria Clara Seixas, Marta Carolina Giménez Pereira, Maurício Requião, Mayana Barbosa Oliveira, Rafael da Silva Santana, Rafaela Lamêgo e Aquino Rodrigues de Freitas, Rodrigo Castro Nascimento, Salvador Morales Ferrer, Teila Rocha Lins D'Albuquerque e Wendel Machado de Souza

Autores

Salvador
Edufba
2022

Grafia atualizada conforme o Acordo Ortográfico da Língua Portuguesa de 1990, em vigor no Brasil desde 2009.

COORDENAÇÃO EDITORIAL
Susane Santos Barros

CAPA E PROJETO GRÁFICO
Gabriela Nascimento

COORDENAÇÃO GRÁFICA
Edson Sales

EDITORAÇÃO
Zeta Studio

COORDENAÇÃO DE PRODUÇÃO
Gabriela Nascimento

REVISÃO E NORMALIZAÇÃO
Tikinet Edição LTDA.

Sistema Universitário de Bibliotecas – UFBA

P969 Proteção de dados pessoais: novas perspectivas / Maurício Requião, Organizador. - Salvador: EDUFBA, 2022.
6,2 MB (PDF) ; (Professor Edvaldo Brito).

Modo de acesso: https://repositorio.ufba.br/handle/ri/35799
Textos em português e espanhol.
ISBN: 978-65-5630-363-5

1. Proteção de dados pessoais – Brasil - Legislação. 2. Consentimento (Direito). 3. Direito à privacidade. 4. Segredos comerciais – Brasil - Legislação. I. Requião, Maurício. II. Título: novas perspectivas.

CDU – 34

Elaborada por Geovana Soares Lira CRB-5: BA-001975/O

EDITORA AFILIADA À

ASOCIACION DE EDITORIALES UNIVERSITARIAS DE AMERICA LATINA Y EL CARIBE

Associação Brasileira das Editoras Universitárias

Edufba
Rua Barão de Jeremoabo, s/n, *Campus* de Ondina
Salvador - Bahia CEP 40170-115 Tel: +55 (71) 3283-6164
www.edufba.ufba.br | edufba@ufba.br

Sumário

PREFÁCIO

A presente obra coletiva, organizada pelo Professor Maurício Requião, é mais um importante passo na produção de pesquisa teórica e empírica e, especialmente, na direção para a construção de uma dogmática sofisticada da Lei Geral de Proteção de Dados (LGPD) no campo jurídico. Desde o ano passado, tenho dialogado com Maurício e com a comunidade jurídica da Universidade Federal da Bahia (UFBA). Primeiro, a respeito da sua importante contribuição sobre o capitalismo de vigilância e as investidas antidemocráticas em meio ao cenário de calamidade pública causado pela pandemia.[1] E, posteriormente e mais especificamente, sobre o consentimento enquanto um processo de tomada de decisão e não como um ato pontual de declaração de vontade do titular.[2]

A riqueza desta obra não está apenas no seu conteúdo em si, mas, também, na forma com que foi organizada por permitir diversidade de olhares. No que diz respeito à vinculação institucional, as faculdades presentes nesta obra são: Universidade Federal da Bahia, Faculdade Baiana de Direito, Faculdade Meridional, Fundação Getulio Vargas, Insper, Universidade Federal de Pernambuco, Universidade Federal de Alagoas, Centro Universitário de Goiatuba, Faculdade Pio Décimo em Aracaju, Universidade de Caxias do Sul, Faculdade de Direito da Universidade de Lisboa, Universidade Católica do Salvador,

1 REQUIÃO, Maurício. Covid-19 e as entranhas do capitalismo de vigilância. *In*: BIONI, Bruno Ricardo *et al*. (org.). *Os dados e o vírus*: pandemia, proteção de dados e democracia artificial. São Paulo: Data Privacy BR, 2020.

2 BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. *In*: DONEDA, Danilo *et al*. (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2020.

Universidade de Coimbra, Universidade Autônoma do México, Universidad del Museo Social Argentino, Universidad de Valencia, Universidad Cardenal Herrera CEU de Valencia, Ilustre Colegio de Abogados de Alzira. Os articulistas estão em diferentes níveis em suas jornadas acadêmicas, concentradas principalmente na área do Direito, havendo a presença de trabalhos elaborados por graduandos e graduandas, graduados e graduadas, mestrandos e mestrandas, mestres e mestras, doutorandos e doutorandas, doutores e doutoras, pós-doutores e pós-doutoras. Esse tipo de conhecimento intergeracional é essencial para estruturar um campo novo de saberes.

Após a leitura do conjunto das obras selecionadas para publicação, foi possível dividi-las em cinco blocos temáticos. O primeiro bloco ou eixo temático, denominado "O consentimento como fundamento para o tratamento de dados", compreende estudos voltados para o entendimento desta base legal autorizativa. No primeiro trabalho que integra o bloco, "A natureza jurídica do consentimento para tratamento de dados pessoais", Maurício Requião argumenta que a razão de o consentimento ser uma das hipóteses mais utilizadas para o tratamento de dados pessoais se dá, principalmente, pelo fato de já ser uma categoria jurídica sedimentada com longo histórico de uso e por já trazer consigo a anuência do titular dos dados. Além desta análise inicial, o autor aborda ainda a problemática que envolve os usos do consentimento, que foram estudados à larga no campo do Direito Privado, como, por exemplo, as questões dos vícios de consentimento. No segundo trabalho, "Limites à utilização do consentimento como base legal adequada para o tratamento de dados pessoais", Fernanda Rêgo Oliveira Dias traz uma extensa reflexão sobre a referida base legal. Objetivando demonstrar que a LGPD contempla limitações ao uso do consentimento, a autora demonstra quais são esses limites e quais são os critérios para a verificação do consentimento válido e adequado, capaz de preencher as características da adjetivação previstas em lei. E no terceiro e último trabalho deste eixo, cujo título é

"El consentimiento del menor en la nueva Ley de Protección de Datos Española, en el reglamento europeo y en el Derecho Comparado", Salvador Morales Ferrer contribui para o entendimento do consentimento como base legal para o tratamento de dados pessoais de crianças e adolescentes, sob uma visão internacional, a partir de um estudo de direito comparado, que leva em consideração a legislação de proteção de dados brasileira, a colombiana, a argentina, a espanhola e a europeia, com um paralelo com as legislações que tratam especificamente da proteção dos direitos de crianças e adolescentes.

Os temas relacionados aos segredos de empresa ganharam eixo próprio, cujo título é "O direito de propriedade intelectual e a Lei Geral de Proteção de Dados". O primeiro integrante é "El secreto empresarial y la protección de datos: un breve enfoque en el ordenamiento jurídico brasilero", de autoria de Marta Carolina Giménez Pereira e Mayana Barbosa Oliveira. O capítulo aborda a relação da proteção de dados pessoais de consumidores com os institutos tradicionais da Propriedade Industrial que visam a proteção de dados de natureza privada e buscam a proteção anticompetitiva dos atores no mercado. As autoras concluem que com a chegada da LGPD, tornou-se ainda mais essencial para a sobrevivência das empresas, em um mercado competitivo, identificar e restringir o acesso aos dados que elas querem proteger através do sigilo comercial. O segundo capítulo, "Segredos industriais e comerciais: proteção ao agente de tratamento de dados pessoais trazida pela Lei Geral de Proteção de Dados", elaborado por Maria Clara Seixas, aborda os segredos industriais e comerciais como exceção aos princípios da transparência e autodeterminação informativa. Assim como no trabalho anterior, discorreu-se sobre a necessária ponderação de interesses que é a característica da LGPD, materializada, no caso, pela distinção entre interesses sociais dos titulares de dados em contraposição aos direitos dos agentes de tratamento de dados. Fechando o bloco, Wendel Machado de Souza traz, em "Segredos de empresa, propriedade intelectual e a proteção de dados pessoais no

ordenamento jurídico brasileiro", uma análise dos segredos comerciais e industriais, em relação com a LGPD; o autor conclui que esses institutos devem exercer importante função em três aspectos distintos que configuram a compreensão do tema como essencial: os direitos dos titulares, as obrigações dos agentes de tratamento e a atuação da Autoridade Nacional de Proteção de Dados (ANPD).

O terceiro eixo temático traz capítulos voltados à compreensão de certos conceitos de direito atuais ou que ganham atualidade e relevância em razão de avanços tecnológicos e da implementação da LGPD, desta feita, por tratar-se de um bloco de horizontes amplos, é denominado "Avanços tecnológicos, LGPD e a ciência do Direito", justamente pela característica enciclopédica deste último elemento denominador. Em "A necessidade como elemento modulador da validade dos atos de tratamento de dados pessoais", primeiro capítulo do bloco, Rafael da Silva Santana aborda o que considera um dos pontos focais da LGPD, o princípio da necessidade, elemento norteador que tem a característica de limitar o tratamento de dados pessoais ao mínimo necessário à obtenção dos resultados propostos pelos agentes de tratamento. No segundo capítulo, "Tutela jurídica dos dados pessoais: uma relação com os direitos de personalidade", a autora Lorena Esquivel de Brito elabora um estudo que contribui para a discussão a respeito do paradoxo: exposição deliberada da vida privada e necessidade de proteção dos direitos de personalidade, discussão que compreende os direitos à proteção dos dados pessoais dos cidadãos. O foco é na problemática que é resultado de avanços nas tecnologias de tratamento de dados pessoais e como instrumentos jurídicos e tecnológicos podem apresentar soluções para eventuais violações de direitos dos indivíduos. Em "Breves notas sobre anonimização e proteção de dados pessoais", Marcos Ehrhardt Jr. e Jéssica Andrade Modesto identificam que as técnicas de anonimização podem ser um caminho viável para garantir a proteção dos direitos fundamentais dos indivíduos sem concretizarem um entrave ao avanço tecnológico e econômico.

No quarto capítulo, escrito por Laura Lucia da Silva Amorim e cujo título é "Tik Tok – dá-me teus dados e te direi quem és: a socialdigitalidade e a possível flexibilização de conceitos fundamentais", traz-se importante reflexão sobre as condições da sociedade atual, defendendo que o cidadão da "socialdigitalidade", motivado pela sua própria vontade ou necessidade, representadas por uma curiosidade e vontade de interagir no ambiente da internet, renuncia sua privacidade em troca de "informação, exibição, exposição". O capítulo que fecha o bloco foi elaborado por Bárbara Veiga Góes e Teila Rocha Lins D'Albuquerque. Em "Responsabilidade civil no descumprimento da nova Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)", faz-se uma análise de como o ordenamento jurídico brasileiro, em específico a LGPD, cuida da responsabilidade civil dos agentes de tratamento e, subsidiariamente, constrói uma apologia à interpretação do direito à proteção dos dados pessoais como um direito fundamental distinto do direito à privacidade. Ao final, os autores apontam o que consideram uma omissão da LGPD, a não caracterização da responsabilidade civil dos agentes de tratamento de dados pessoais como subjetiva ou objetiva. Como medida de colmatação, aponta-se a interpretação e aplicação da responsabilidade objetiva como regra.

O quarto bloco temático, "O problema do uso dos dados pessoais sensíveis", é composto por quatro trabalhos voltados à análise deste tema candente. Em "A discriminação algorítmica e as novas perspectivas sobre o tratamento de dados pessoais sensíveis", Diego Carneiro Costa aborda a problemática dos *softwares* de inteligência artificial que, ao premiarem a efetividade, reproduzem preconceitos gerando discriminação quando utilizados para processos de tomada de decisão. A problemática é exacerbada, pois, cada vez mais, essas ferramentas tecnológicas têm sido empregadas por empresas e mesmo pela Administração Pública, que visam atribuir eficiência e acurácia aos seus processos de tomada de decisão. No segundo capítulo, "Inteligência artificial, saúde mental e os dados: a dimensão digital

na Reforma Psiquiátrica brasileira", Laércio Martins salienta que é a rara a produção acadêmica de juristas no campo da saúde mental, o que justifica a contribuição do autor para a compreensão da relação entre os avanços tecnológicos informacionais, a proteção de dados e Lei da Reforma Psiquiátrica (Lei nº 10.216/2001), que resultou em um movimento de desinstitucionalização no Brasil. Rodrigo Castro Nascimento é o autor de "A pseudonimização como medida protetiva para os dados pessoais sensíveis referentes à saúde", no qual é defendido que mesmo sendo objeto de forte regulamentação, o tratamento de dados pessoais referentes à saúde ainda merece cuidados por conta da potencialidade da exposição desses dados resultante de situações de vazamento que não são raras. No último capítulo que compõe o bloco destinado ao estudo dos temas relacionados ao tratamento de dados pessoais sensíveis, o trabalho cujo título é "Pornografia *on-line* e LGPD: interpretando dados sensíveis", traz uma análise de Fernando Araújo dos Santos, que estuda o processo de adaptação dos *sites* pornográficos à LGPD, o que se construiu a partir da análise de políticas de privacidade, termos de serviço e políticas de *cookies*. Em interpretação interessante realizada à luz da teoria da textura aberta do direito, o autor conclui que os dados pessoais ordinários podem ser considerados dados sensíveis quando avaliados no caso concreto. Avança afirmando que todos os dados pessoais obtidos por *sites* pornográficos devem ser considerados sensíveis, afastando a pretensão à escolha da base legal do legítimo interesse.

O último bloco temático, "A LGPD e as consequências para as relações de emprego", é composto por dois trabalhos. No primeiro deles, "Linhas básicas da Lei Geral de Proteção de Dados na relação de emprego", Edilton Meireles realiza estudo dos reflexos da LGPD na relação de emprego, com o apontamento de substanciais modificações que são o fruto da nova legislação ao assegurar maior proteção ao trabalhador. Conclui-se que a LGPD irá trazer fortes impactos para as relações de emprego e que caberá aos empregadores o enquadramento

legal, sob pena de serem responsabilizados civilmente em caso de descumprimento das normas estabelecidas pela lei de proteção de dados. No segundo capítulo, de autoria de Daniel de Araújo Paranhos e cujo título é "O papel do Estado na proteção de dados dos seus servidores e suas consequências para o endividamento da categoria", analisa-se o dever do Estado em conformar os deveres norteadores de transparência e publicidade, e, no âmbito das proteção de dados pessoais dos servidores públicos, como poderá resultar na diminuição dos índices de endividamento da categoria. Afirma o autor que a Administração Pública falha na proteção dos dados de servidores públicos que mantém em sua posse, razão pela qual conclui que o Poder Público ainda precisa dar efetividade à LGPD.

Por mais trabalhos coletivos como este que consigam capturar a complexidade obrigacional e de interesses por trás da proteção de dados pessoais, é o coro que eu entoaria como convite a sua leitura. Quer no seu todo ou através de uma análise pontual dos seus capítulos, este livro energiza da melhor forma possível o tema em um ano-chave que é o da efetivação da implementação da LGPD com a plena operação da Autoridade Nacional de Proteção de Dados.

Bruno Bioni
bruno@dataprivacy.com.br
Doutor em Direito Comercial e Mestre em Direito Civil na Faculdade de Direito da Universidade de São Paulo. Foi study visitor do Departamento de Proteção de Dados Pessoais do European Data Protection Board/EDPB e do Conselho da Europa, pesquisador visitante no Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa. É autor do livro Proteção de Dados Pessoais: a função e os limites do consentimento. É membro da Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade/LAVITS, e também da International Association of Privacy Professionals – IAPP, com Certificação CIPP/E. É diretor fundador do Data Privacy Brasil, um espaço de intersecção entre uma escola de cursos e uma associação de pesquisa na área de privacidade e proteção de dados.

A NATUREZA JURÍDICA DO CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS

Maurício Requião

Introdução

O tratamento de dados pessoais, embora possa se iniciar também por outras bases, tem o consentimento como uma de suas hipóteses mais comumente utilizadas. Isso se deve, provavelmente, tanto à longa história e uso do consentimento como categoria jurídica, como também ao fato de que o consentimento é modo que já traz, em tese, a expressa anuência do titular de dados quanto ao tratamento que se realizará.

Porém, o consentimento para o tratamento de dados pessoais, igualmente traz consigo vários problemas, que já são estudados a longa data pelo Direito Privado. Nesse sentido, por exemplo, a questão dos vícios de consentimento como defeitos do negócio jurídico. A esses problemas regulares encontrados em outros negócios jurídicos, alguns outros se somam, talvez não enquanto novas categorias jurídicas, mas ao menos em novo contexto.

Entretanto, a aplicação de determinadas consequências depende da análise da natureza jurídica desse consentimento. Assim é que este capítulo se propõe a contribuir para o tema da proteção de dados pessoais, justamente realizando tal análise que ainda resta pouco explorada na doutrina.

Para tanto, se inicia com algumas considerações sobre o consentimento, enquanto categoria geral aplicável no Direito, com o que se objetiva buscar alguma base prévia para tratar do consentimento especificamente na proteção de dados.

Em seguida, se passa para a análise da natureza jurídica do consentimento para tratamento de dados pessoais, tendo por base os requisitos de cada tipo de fato conforme firmado pela teoria do fato jurídico, nos moldes desenvolvidos por Marcos Bernardes de Mello.

Por fim, no último tópico, são realizadas algumas especificações classificatórias que parecem ser úteis para a solução de problemas práticos que envolvem o consentimento para tratamento de dados pessoais.

O consentimento

A ideia do consentimento como suporte fático para a prática de diversos atos não se inicia com o tema do tratamento de dados pessoais.[1] Nesta primeira seção, o objetivo é realizar levantamento de algumas situações em que o consentimento já vem sendo trabalhado, para, partindo de conhecimento já mais consolidado, se abordar o consentimento como requisito para tratamento de dados pessoais.

No Direito Civil, *locus* privilegiado da atuação da autonomia no Direito, diversos são os pontos vinculados ao consentimento. Apenas analisando o texto do Código Civil de 2002 (CC-2002), o termo consentimento é utilizado 39 vezes. Aparece no campo da teoria geral das Obrigações,[2] no Direito dos Contratos,[3] no Direito Empresarial,[4] no

1 SOLOVE, Daniel J. Introduction: privacy self-management and the consent dilemma. *Harvard Law Review*, Cambridge, v. 126, p. 1880-1903, 2013.

2 CC-2002, arts. 278, 299 e 362.

3 CC-2002, arts. 496, 533, 578, 632, 820 e 838.

4 CC-2002, arts. 995, 999, 1.002, 1.003, 1.017, 1.092, 1.114, 1.127 e 1.145.

Direito das Coisas,[5] no Direito de Família[6] e no Direito das Sucessões.[7] Além dessas situações, diversas outras, seja na doutrina ou no próprio Código, por vezes utilizando outras expressões como "autorização", também são vinculadas ao consentimento, como acontece, por exemplo, em algumas situações que envolvem a autonomia como pressuposto para realização dos direitos da personalidade.[8]

Também no Direito Penal, o enquadramento em diversos dos seus tipos passa pela análise do consentimento.[9] Há certa discussão sobre o consentimento ser "causa que sempre afasta a tipicidade ou ser causa que ora pode determinar a atipicidade da conduta e ora funcionar como hipótese de justificação, afastando-se assim a ilicitude do ato".[10] Fato é que, em qualquer das explicações adotadas, determinados tipos só estarão plenamente caracterizados e imputarão responsabilidade caso não haja o consentimento do titular do bem jurídico envolvido. Assim, por exemplo, a ocorrência de um crime de estupro decorre do fato de ter sido o ato sexual realizado sem consentimento.

A Bioética é, talvez, o campo relacionado ao Direito que mais já se debruçou sobre o consentimento, por conta da análise do termo de consentimento informado ou termo de consentimento livre e esclarecido

5 CC-2002, arts. 1.272, 1.306, 1.387, parágrafo único, 1.420, § 2°, 1.445 e 1.449.

6 CC-2002, arts. 1.519, 1.550, 1.558, 1.574, 1.611, 1.614, 1.634, III, IV, V e VI, 1.642, III, 1.650 e 1.717.

7 CC-2002, arts. 1.972 e 2.021.

8 BORGES, Roxana Cardoso Brasileiro. *Direitos de personalidade e autonomia privada*. 2. ed. São Paulo: Saraiva, 2007. p. 127.

9 Obviamente nem todo tipo penal pode ser mitigado pelo consentimento, até mesmo pelo fato de que alguns bens tutelados pelo Direito Penal são considerados indisponíveis, de modo que algumas lesões ultrapassariam a esfera de análise de disponibilidade por parte do indivíduo, trazendo também a análise das consequências para o corpo social. Neste sentido: MINAHIM, Maria Auxiliadora. *Autonomia e frustração da tutela penal*. Saraiva: São Paulo, 2015. p. 72.

10 MINAHIM, *op. cit.*, p. 68.

(TCLE).[11] Este consiste em procedimento pelo qual, excetuadas as situações de risco iminente de morte, após elucidar o paciente ou seus familiares, no caso de impossibilidade ou risco de dano para aquele, se obtém o consentimento para a realização de atos médicos.[12] É, portanto, situação que envolve o exercício da autonomia do paciente, a partir de informações que lhe são prestadas.[13]

Encontra-se na doutrina certa tendência de apontar a natureza jurídica do TCLE como ato jurídico[14] e, embora não haja a especificação de que tipo de ato (se *stricto sensu* ou negócio), em alguns casos se encontra a afirmação de que seria ato jurídico unilateral.[15] Em virtude da natureza de ato jurídico, são apontados elementos essenciais para sua existência e validade, como capacidade do paciente, clareza do texto, assinatura voluntária e participação do paciente na construção do documento.[16]

É relevante desde já destacar três pontos relativos ao TCLE que podem ser bastante úteis ao abordar o consentimento para tratamento de dados pessoais. O primeiro, como dito, é o de que se trata de um processo. Assim, as informações de diagnóstico e possibilidades terapêuticas serão continuamente trazidas ao paciente para que se possa ter realmente o TCLE. Não se trata, portanto, simplesmente de

11 MANZINI, Merlei Cristina; MACHADO FILHO, Carlos D'Apparecida Santos; CRIADO, Paulo Ricardo. Termo de consentimento informado: impacto na decisão judicial. *Revista Bioética*, São Paulo, v. 28, n. 3, p. 517-521 2020. Há certo dissenso sobre termo de consentimento informado e termo de consentimento livre e esclarecido serem ou não sinônimos. Para os autores neste ponto referidos, o primeiro diria respeito ao tratamento médico e o segundo, à pesquisa em seres humanos. Esta discussão, entretanto, é irrelevante para os objetivos deste capítulo.

12 CASTRO, Carolina Fernandes de *et al*. Termo de consentimento livre e esclarecido na assistência à saúde. *Revista Bioética*, São Paulo, v. 28, n. 3, p. 522-530, 2020.

13 SILVA, Maristela Freitas. Consentimento informado: estratégia para mitigar a vulnerabilidade na assistência hospitalar. *Revista Bioética*, São Paulo, v. 25, n. 1, p. 30-38, 2017.

14 MANZINI; MACHADO FILHO; CRIADO, p. 518, 2020; CASTRO *et al*., *op. cit.*, p. 523.

15 *Ibidem*, p. 518.

16 *Ibidem*, p. 510.

um documento entregue inicialmente ao paciente que teria o condão de autorizar o profissional de saúde a qualquer conduta ou o isentar de responsabilidade.

O segundo ponto, de certa forma vinculado às observações acima apontadas, decorre do fato de ter o TCLE dupla função: "jurídica, para eventual defesa do profissional, e ética, como processo contínuo de esclarecimento na relação entre médico e paciente, protegendo a autodeterminação deste último".[17] Entretanto, conforme pesquisas que vêm sendo realizadas, o TCLE muitas vezes é formulado e apresentado de modo que pouco atende ao seu objetivo ético. Uso de termos técnicos, grande número de páginas e problemas éticos na transmissão das informações se apresentam como alguns problemas que impedem a realização adequada desse objetivo.[18]

Na literatura bioética, inclusive, é possível encontrar artigos que focam mais na análise voltada para a questão jurídica, encaminhando-se para discussões sobre responsabilidade civil,[19] bem como para a questão ética, seguindo o viés das possibilidades do TCLE como modo de superar, em alguma medida, as dificuldades surgidas pela condição de múltipla vulnerabilidade do paciente.[20]

Por último, mas não menos importante, o TCLE lida com o ser humano numa situação de vulnerabilidade, relacionada à saúde e ao conhecimento técnico, seja no campo do tratamento médico[21] ou da pesquisa científica.[22] Igualmente, o consentimento para proteção de dados pessoais também encontra o titular dos dados em situação de vulnerabilidade, ao menos técnica e econômica.

17 CASTRO *et al.*, *op. cit.*, p. 523.

18 *Ibidem*, p. 523.

19 MANZINI; MACHADO FILHO; CRIADO, *op. cit.*, p. 520.

20 SILVA, *op. cit.*, p. 37.

21 *Ibidem*, p. 32..

22 COSAC, Danielle Cristina dos Santos. Autonomia, consentimento e vulnerabilidade do participante de pesquisa clínica. *Revista Bioética*, São Paulo, v. 25, n. 1, p. 19-29, 2017.

No que toca ao tratamento de dados pessoais, o consentimento figura na Lei Geral de Proteção de Dados (LGPD) como uma das bases legais que autorizam o tratamento, com expressa previsão no art. 7°, I. Por se entender que a proteção de dados pessoais é direito fundamental, bem como por se concordar com sua proximidade à natureza dos direitos da personalidade, os regramentos do consentimento aqui deverão dialogar firmemente com os pontos anteriormente expostos.

Justamente por isso é que parece inevitável a comparação entre o consentimento para tratamento de dados pessoais e o TCLE visto acima.[23] Ambos tratam de situações em que há grande disparidade informacional e técnica, em que um dos envolvidos está permitindo a interferência em direito fundamental seu e em que há clara situação de vulnerabilidade de um dos figurantes.

Assim, por conta dessa similaridade, as soluções encontradas para o consentimento na bioética podem também ser pensadas como aplicáveis no tema da proteção de dados pessoais. A primeira delas talvez seja o reconhecimento de que a formulação do consentimento é um processo.[24] A exemplo do quanto já apontado no campo da bioética, não se pode pensar no consentimento como simples meio de exoneração de responsabilidade para o controlador ou operador, notadamente quando se busca constituí-lo através do aceite de longo e complexo documento, que muitas vezes extrapola os limites de compreensão de quem a ele adere.

Deste modo, o caminho utilizado para obtenção desse consentimento – que é, em regra, a apresentação ao usuário, quando da instalação do aplicativo, dos "termos de privacidade" ou "termos de uso", em que se tem indicada a política geral de tratamento de

23 BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. *In*: DONEDA, Danilo *et al*. (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2020.

24 BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 250.

dados que será aplicada ao usuário titular dos dados caso ele a aceite – encontra-se como insuficiente.

Há, em verdade, enorme número de problemas envolvendo o consentimento para tratamento de dados. Entretanto, muitos desses problemas decorrem não de falhas, mas da própria natureza estrutural do capitalismo de vigilância, fazendo com que seus protagonistas busquem, pelos mais diversos artifícios, acumular o maior número possível de dados pessoais.[25]

A análise das consequências do capitalismo de vigilância, embora não sejam aqui desprezadas, não são alvo deste capítulo. Os problemas são, conforme dito, múltiplos e complexos, e tentar esgotá-los aqui acabaria desvirtuando o objetivo central deste texto, que é a discussão da natureza jurídica do consentimento para tratamento de dados pessoais. A despeito disso, devem ser sempre lembrados como pano de fundo para toda a discussão a seguir desenvolvida.

Natureza jurídica do consentimento para o tratamento de dados pessoais

A discussão sobre a natureza jurídica, especialmente quando surgem novas situações que reclamam a tutela jurídica, é extremamente necessária. E isso se dá não por preciosismo acadêmico, mas sim porque a categorização em determinada natureza jurídica traz uma série de efeitos práticos que podem mudar enormemente a disciplina do instituto em questão.

Na doutrina nacional, Danilo Doneda, ao tratar do tema da natureza jurídica do consentimento para o tratamento de dados pessoais, afirma dois pontos com os quais se concorda enquanto base para este capítulo. Primeiro, que seria inadequada a realização de "neo-dogmatismos", que se caracterizariam como "uma transposição rasa do consentimento

25 ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for the future at the new frontier of power. London: Profile Books, 2019. p. 11.

negocial para o consentimento ao tratamento de dados pessoais".[26] Em segundo lugar, afirma que tratar o consentimento considerando que tenha natureza puramente negocial seria algo prejudicial, porque legitimaria sua inserção "em estruturas contratuais, dificultando a sua valoração em função dos atributos da personalidade que estão em jogo".[27]

Realiza o autor tais afirmações, por conta de preocupação, que aqui se compartilha, da comoditização dos dados pessoais,[28] que desprezaria a sua tutela enquanto direito de caráter claramente existencial, em favor da exploração do seu valor patrimonial, dentro da lógica do capitalismo de vigilância. Afinal, boa parte das teorias sobre a tutela de dado pessoais, como também apontado por Doneda, trazem em alguma medida abertura para a transformação dos dados pessoais em um ativo a ser explorado.[29]

A partir de tais considerações, conclui-se, então, que o consentimento não pode ser considerado um negócio jurídico.[30] Doneda é acompanhado nessa posição em artigo escrito por Gustavo Tepedino e Chiara Spadaccini de Teffé.[31] Aponta consonância da sua afirmação com a doutrina italiana, embora destaque que, também lá, há defensores da natureza negocial do consentimento para o tratamento de dados pessoais.

A despeito das críticas que traz, Doneda chega, inclusive, a afirmar que este consentimento seria ato jurídico unilateral,[32] sem especificar se fala do gênero ou espécie. Entretanto, diante da negativa da natureza

26 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2020. p. 301.

27 *Ibidem*, p. 302.

28 *Ibidem*, p. 297.

29 DONEDA, *op. cit.*, p. 290-295. Nesse rol a tutela proprietária, a tutela aquiliana, a tutela de autorregulamentação, a tutela como braço da *lex mercatoria* e a tutela baseada na própria tecnologia.

30 *Ibidem*, p. 303.

31 TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei geral de proteção de dados pessoais* – e suas repercussões no direito brasileiro. 2. ed. São Paulo: Revista dos Tribunais, 2020. p. 293.

32 DONEDA, *op. cit.*, p. 303.

de negócio jurídico, parece razoável supor que o estaria classificando como ato jurídico *stricto sensu*.

Por outro lado, Juliana Dantas e Eduardo Henrique Costa se posicionam no sentido de que o consentimento, conforme previsto na LGPD, seria negócio jurídico.[33] Este texto, apesar dos problemas apontados por Doneda, acompanha essa conclusão.

O consentimento para tratamento de dados pessoais, dentro da teoria do fato jurídico, deve ser classificado como negócio jurídico, desde que adequadamente delimitadas as características do negócio em questão. Caracterizar o consentimento como negócio jurídico, como se sustentará a seguir, não implica, de forma alguma, prejuízo aos interesses do titular dos dados pessoais. Pelo contrário, pode trazer um número ainda maior de tutelas protetivas.

Os atos jurídicos *lato sensu*, como colocado por Pontes de Miranda, "são os meios mais eficientes da atividade inter-humana, na dimensão do direito. Neles e por eles, a vontade, a inteligência e o sentimento inserem-se no mundo jurídico, edificando-o".[34] Dividem-se em ato jurídico *stricto sensu* e negócio jurídico. O ponto em comum entre ambos é justamente a presença da vontade como elemento do seu suporte fático.

Para avançar na discussão, se faz necessário primeiro trazer a definição de negócio jurídico. Este, para Marcos Bernardes de Mello, se caracteriza como

> o fato jurídico cujo elemento nuclear do suporte fático consiste em manifestação ou declaração consciente de vontade, em relação à qual o sistema jurídico faculta às pessoas, dentro de limites predeterminados e de amplitude vária, o poder de escolha de

33 DANTAS, Juliana de Oliveira Jota; COSTA, Eduardo Henrique. A natureza jurídica do consentimento previsto na Lei Geral de Proteção de Dados: ensaio à luz da teoria do fato jurídico. *In*: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; MALHEIROS, Pablo (coord.). *Direito Civil e tecnologia*. Belo Horizonte: Fórum, 2020. p. 86.

34 PONTES DE MIRANDA. *Tratado de direito privado*: parte geral. Rio de Janeiro: Borsoi, 1954. Tomo 2. p. 446.

> categoria jurídica e de estruturação do conteúdo eficacial das relações jurídicas respectivas, quanto ao surgimento, permanência e intensidade no mundo jurídico.[35]

Nessa definição se pode notar o traço distintivo entre o ato jurídico *stricto sensu* e o negócio jurídico, já que, apenas neste último, há a possibilidade de escolha da categoria jurídica e de estruturação do conteúdo eficacial a partir da exteriorização de vontade.

Já Antônio Junqueira de Azevedo, por sua vez, ao definir negócio jurídico, manifesta preocupação com sua questão estrutural, afirmando que, por tal concepção, haja alargamento da ótica pela qual se enxerga o negócio jurídico, suplantando a visão do autor do negócio, para fazer seu exame também pelo prisma social e jurídico.[36] Essa ressalva é interessante à análise que ora se realiza, pois dialoga com alguns dos problemas enfrentados pelo consentimento, como se detalhará mais adiante.

Vistas essas definições clássicas, se passa à análise de adequação do consentimento à categoria de negócio jurídico. De início, destaca-se que o consentimento, indiscutivelmente, é um ato que tem a exteriorização de vontade como parte do seu suporte fático. Isso é verificável a partir da leitura da própria LGPD que, no seu art. 5°, XII, apresenta definição do consentimento, firmando, assim, seu suporte fático hipotético da seguinte maneira: "consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".[37]

35 MELLO, Marcos Bernardes de. *Teoria do fato jurídico*: plano da existência. 14. ed. São Paulo: Saraiva, 2007. p. 189.

36 AZEVEDO, Antônio Junqueira de. *Negócio jurídico*: existência, validade e eficácia. 4. ed. São Paulo: Saraiva, 2013. p. 21.

37 BRASIL. "http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2013.709-2018?OpenDocument" Lei n° 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n° 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, 15 ago. 2018. p. 59.

Note-se que o texto legal aponta o consentimento como uma *manifestação* por parte do titular, indicando ainda que ele envolve sua *concordância*, formulando descrição típica dos atos de vontade. O que, por si, são características típicas dos atos de vontade.

Assim, a vontade precisa estar presente quando alguém consente o tratamento de seus dados pessoais. Portanto, a vontade se apresenta como elemento nuclear, ou seja, elemento essencial para sua existência, integrando o suporte fático para que ocorra o consentimento. Assim, desde que haja a exteriorização da vontade, eventuais vicissitudes que a afetem dirão respeito à análise do plano da validade ou da eficácia.

Sendo a exteriorização da vontade parte do suporte fático, o consentimento, na teoria do fato jurídico, já se apresenta necessariamente como um ato jurídico *lato sensu*. Dentro do gênero, poderia ser ato jurídico *stricto sensu* ou negócio jurídico. A distinção aqui se faz porque, conforme já dito, enquanto no primeiro não haveria possibilidade de modificação do conteúdo eficacial, tal modificação seria possível no segundo.[38]

O consentimento para tratamento de dados pessoais traz, em sua essência, a possibilidade de modificação do conteúdo eficacial.[39] Se muitas vezes isso não se dá na prática, não se deve à natureza do ato de consentir, mas sim à estrutura contratual em que ele se insere, ou seja, o fato de se apresentar como sendo de adesão.

O contrato de adesão, embora acabe por limitar a escolha das categorias eficaciais por uma das partes, não perde sua natureza de negócio jurídico. Ademais, importante destacar que o consentimento para tratamento de dados pessoais normalmente não é o próprio contrato, embora esteja a ele relacionado, como se explorará na seção seguinte.

38 MELLO, *op. cit.*, p. 192.

39 DANTAS; COSTA, *op. cit.*, p. 83.

Temas específicos da área de proteção de dados pessoais, as ideias de *privacy by default* e *privacy by design*, também trazem informações que reforçam o até aqui sustentado. Este modelo faz com que se exija "do usuário uma conduta comissiva, ativa, no sentido de diminuir a proteção conferida à sua privacidade, e não o contrário".[40]

Devem, portanto, os termos de consentimento trazer a configuração de maior proteção possível ao titular dos dados, de modo que, através de sistema *opt-in*, o titular dos dados possa autorizar outros pontos relativos ao tratamento. Ou seja, *através de exteriorização de vontade pode o sujeito modificar a eficácia do consentimento.*

Parece suficientemente claro, portanto, que não apenas a vontade é um fator que compõe o suporte fático do consentimento para tratamento de dados pessoais, mas também que ela tem o poder para modificar o conteúdo desta eficácia, seja em questões como a abrangência dos dados pessoais cedidos, seja para questões outras como possibilidade de cessão a terceiros, indicação de finalidade e até mesmo de duração do tratamento, todas, aliás, expressamente previstas na LGPD.

Suplantado este ponto, se passa, a seguir, a discutir duas questões de classificação do negócio jurídico que, dentre as diversas apresentadas pela doutrina, parecem centrais para que se entenda como essa categoria jurídica pode ser útil à proteção de dados pessoais.

Consentimento para tratamento de dados pessoais é negócio jurídico unilateral e autônomo

Os negócios jurídicos bilaterais, para Marcos Bernardes de Mello, são aqueles que "se formam a partir de manifestações de vontade distintas,

40 LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design: conceito, fundamento e aplicabilidade na LGPD. *In*: DONEDA, Danilo *et al*. (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2020.

porém coincidentes, recíprocas e concordantes sobre o mesmo objeto".[41] Já os unilaterais "têm existência e eficácia autônoma, por isso não supõem nem provocam reciprocidade ou correspectividade de efeitos jurídicos. Para existirem, basta a manifestação de vontade suficiente à composição do seu suporte fáctico".[42]

Podem-se apontar como exemplos de negócios jurídicos unilaterais a promessa de recompensa, a oferta, o testamento e a instituição da fundação. Já como exemplo de negócios jurídicos bilaterais citam-se, suficiente por todos dada sua relevância, os contratos.

Os negócios jurídicos de consentimento para tratamento de dados pessoais se dão, usualmente, como pressuposto de um contrato. O consentimento costuma ser colocado como requisito para que se possa acessar certo produto ou serviço objeto de um contrato. Muitas vezes, inclusive, como requisito inafastável, já que não consentir nos exatos termos previstos no contrato de adesão implica a impossibilidade de acesso ao objetivo que se pretende.

O fato de muitas vezes o consentimento ser dado durante a formação de um contrato não significa que seja necessariamente negócio jurídico bilateral, já que é possível que negócio jurídico unilateral seja inserido num bilateral sem que com isso perca sua autonomia e identidade própria.[43] A dúvida seria, portanto, se o consentimento é mera cláusula num negócio jurídico bilateral ou se pode ser caracterizado como negócio jurídico unilateral naquele inserido.

Levando em conta a natureza personalíssima do seu objeto, bem como as determinações da LGPD sobre o tema, é mais adequada a sua classificação como negócio jurídico unilateral.[44] Tratá-lo como negócio jurídico unilateral é mais compatível com as previsões legais sobre o

41 MELLO, *op. cit.*, p. 203.

42 *Ibidem*, p. 201.

43 *Ibidem*, p. 203.

44 DANTAS; COSTA, *op. cit.*, p. 86.

consentimento, especialmente quando se pensa na questão da possibilidade de revogação do consentimento e possíveis efeitos deste no contrato.

Neste ponto, porém, ainda mais importante do que a discussão quanto à sua natureza ser de negócio unilateral ou bilateral, é a constatação de sua autonomia em relação ao negócio que leva o consentimento a ser emitido. Isso significa reconhecer o consentimento, por si só, como negócio jurídico independente do contrato para o qual será aplicado, embora a ele seja relacionado.

A revogação do consentimento se encontra prevista na LGPD em seu art. 8º, §5º,[45] podendo ocorrer a qualquer tempo, mediante manifestação expressa do titular. Surge daí, na doutrina, conforme já apontado, a justificada preocupação em que a revogação deste consentimento não possa trazer efeitos patrimoniais adversos ao titular, o que aconteceria caso viesse a ser considerada como uma espécie de inadimplemento contratual.

Considerar o consentimento como negócio jurídico unilateral e autônomo contribui para a solução desse problema. O consentimento se coloca como negócio jurídico unilateral e autônomo, e que é *condição* para a realização e continuidade do negócio bilateral subsequente, e não como cláusula advinda deste. Assim, sua revogação não implica em descumprimento contratual, mas sim em perda da eficácia desse negócio jurídico subsequente.

Dentro dessa lógica, se assenta de modo muito mais confortável a compatibilização da possibilidade de revogação do consentimento a qualquer tempo *e* a ausência de inadimplemento por parte do titular de dados.

A análise de situações concretas, inclusive, confirma a hipótese aqui sustentada, em aspecto estrutural. A família de produtos que inclui *Facebook*, *Instagram* e Messenger, por exemplo, traz dois documentos separados. Um que se constitui como termos de uso e outro, como política de dados.

45 BRASIL, op cit.

Na descrição dos "termos de uso", poucas coisas que poderiam ser referidas como autorização para uso de dados pessoais surgem como obrigação ao usuário do serviço. Traduz, muito mais, descrição sobre o que a rede social fornece ao usuário, em cláusula intitulada "O Serviço Instagram", bem como um rol de deveres e autorizações por parte do usuário contratante, elencadas em cláusula intitulada "Seus compromissos". Ressalvadas menções pontuais, o que há sobre o tema do consentimento para tratamento de dados nestes "termos de uso" é, em verdade, a menção e redirecionamento a outro documento, que é o da "política de dados".[46]

Este segundo documento, por sua vez, nada trata quanto ao negócio jurídico bilateral em que há prestação e contraprestação descritas acima. Constitui-se como verdadeiro inventário dos mais diversos pontos de tratamento de dados pessoais, que deve ser consentido pelo titular de tais dados, de modo *pari passu* à celebração do contrato. Traz, inclusive, aos usuários brasileiros, referência à LGPD e a afirmação de que "em determinadas circunstâncias, você também tem o direito de contestar e restringir o tratamento de seus dados pessoais ou de revogar seu consentimento quando tratamos dados fornecidos por você com base nesse consentimento".[47]

Esse exemplo, acredita-se, ajuda a clarificar a cisão entre o negócio jurídico unilateral do consentimento para tratamento de dados e o negócio jurídico bilateral para utilização do *Instagram* pelo usuário.

46 INSTAGRAM. *Termos de uso*. [São Paulo]: Instagram, 2020. Disponível em: https://pt-br.facebook.com/help/instagram/581066165581870. Acesso em: 29 nov. 2020.

47 INSTAGRAM. *Política de dados do Instagram*. [São Paulo]: Instagram, 2020. Disponível em: https://help.instagram.com/519522125107875?helpref=page_content. Acesso em: 29 nov. 2020.

Conclusão

A classificação do consentimento para tratamento de dados pessoais como negócio jurídico unilateral e autônomo é não somente a tecnicamente mais adequada, como também a que oferece maior proteção ao titular de dados.

Seu reconhecimento como negócio jurídico traz toda a regulamentação protetiva das diversas causas de invalidade e, notadamente, dos defeitos do negócio jurídico. Assim, por exemplo, um consentimento seria anulável por erro, por não ser suficientemente claro; por dolo, quando do uso de interfaces maliciosas que induzam o titular a permitir tratamentos que normalmente não permitiriam; por lesão, considerando a inexperiência do titular de dados em negócios jurídicos que envolvam a sua autorização para tratamento. As situações são, para além destes breves exemplos, bem diversificadas.

É bem verdade que a classificação como ato jurídico não retiraria a possibilidade de tais proteções. Entretanto, como disposto, há por demais espaço para regulamentação eficacial do consentimento para o tratamento de dados, inclusive com a possibilidade de estipulação de condição, termo e encargo, para que não se enxergue com clareza que se trata de negócio jurídico.

Por fim, a sua caracterização como unilateral e autônomo, se dá de modo muito similar ao encontrado no TCLE na Bioética. Tais características, inclusive, se coadunam com a necessidade de que o consentimento não seja uma prisão para o titular dos dados, que não mais o poderia revogar sobre pena de inadimplemento contratual. Ao contrário, deixam clara sua possibilidade de revogação, até por se tratar de processo, que pode a qualquer momento ser modificado pelo titular dos dados pessoais.

Referências

AZEVEDO, Antônio Junqueira de. *Negócio jurídico*: existência, validade e eficácia. 4. ed. São Paulo: Saraiva, 2013.

BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. *In*: DONEDA, Danilo *et al.* (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2020. p. 149-162.

BORGES, Roxana Cardoso Brasileiro. *Direitos de personalidade e autonomia privada*. 2. ed. São Paulo: Saraiva, 2007.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

CASTRO, Carolina Fernandes de *et al.* Termo de consentimento livre e esclarecido na assistência à saúde. *Revista Bioética*, São Paulo, v. 28, n. 3, p. 522-530, 2020. Disponível em: https://revistabioetica.cfm.org.br/. Acesso em: 26 nov. 2020.

COSAC, Danielle Cristina dos Santos. Autonomia, consentimento e vulnerabilidade do participante de pesquisa clínica. *Revista Bioética*, São Paulo, v. 25, n. 1, p. 19-29, 2017. Disponível em: https://revistabioetica.cfm.org.br/. Acesso em: 26 nov. 2020.

DANTAS, Juliana de Oliveira Jota; COSTA, Eduardo Henrique. A natureza jurídica do consentimento previsto na Lei Geral de Proteção de Dados: ensaio à luz da teoria do fato jurídico. *In*: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; MALHEIROS, Pablo (coord.). *Direito Civil e tecnologia*. Belo Horizonte: Fórum, 2020. p. 69-88.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2020.

INSTAGRAM. *Termos de uso*. [São Paulo]: Instagram, 2020. Disponível em: https://pt-br.facebook.com/help/instagram/581066165581870. Acesso em: 29 nov. 2020.

INSTAGRAM. *Política de dados do Instagram*. Disponível em https://help.instagram.com/519522125107875?helpref=page_content. Acesso em: 29 nov. 2020.

LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design: conceito, fundamento e aplicabilidade na LGPD. *In*: DONEDA, Danilo *et al.* (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2020. p. 447-458.

MANZINI, Merlei Cristina; MACHADO FILHO, Carlos D'Apparecida Santos; CRIADO, Paulo Ricardo. Termo de consentimento informado: impacto na decisão judicial. *Revista Bioética*, São Paulo, v. 28, n. 3, p. 517-521, 2020. Disponível em: https://revistabioetica.cfm.org.br/. Acesso em: 26 nov. 2020.

MELLO, Marcos Bernardes de. *Teoria do fato jurídico*: plano da existência. 14. ed. São Paulo: Saraiva, 2007.

MINAHIM, Maria Auxiliadora. *Autonomia e frustração da tutela penal*. Saraiva: São Paulo, 2015.

PONTES DE MIRANDA. T*ratado de direito privado*: parte geral. Rio de Janeiro: Borsoi, 1954. Tomo 2.

SILVA, Maristela Freitas. Consentimento informado: estratégia para mitigar a vulnerabilidade na assistência hospitalar. *Revista Bioética*, São Paulo, v. 25, n. 1, p. 30-38, 2017. Disponível em: https://revistabioetica.cfm.org.br/. Acesso em: 26 nov. 2020.

SOLOVE, Daniel J. Introduction: privacy self-management and the consent dilemma. *Harvard Law Review*, Cambridge, v. 126, p. 1880-1903, 2013. Disponível em: https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf. Acesso em: 4 jan. 2020.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei geral de proteção de dados pessoais* – e suas repercussões no direito brasileiro. 2. ed. São Paulo: Revista dos Tribunais, 2020.

ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for the future at the new frontier of power. London: Profile Books, 2019.

LIMITES À UTILIZAÇÃO DO CONSENTIMENTO COMO BASE LEGAL ADEQUADA PARA O TRATAMENTO DE DADOS PESSOAIS

Fernanda Rêgo Oliveira Dias

Introdução

O capítulo foi pensado no presente contexto da era digital, marcado pela coleta e tratamento de dados pessoais massivos e diante da entrada em vigor do regramento brasileiro sobre proteção de dados, a Lei Geral de Proteção de Dados Pessoais (LGPD),[1] em que pese o tema da privacidade e proteção de dados já estar presente em outros diplomas normativos brasileiros.

Como se visualiza facilmente, colher o consentimento do titular de dados tem sido a estratégia mais utilizada pelos controladores para realização do tratamento de dados, principalmente pelos controladores que atuam no meio digital. É cada vez mais comum, ao abrir *sites*, se deparar com boxes ou caixas perguntando se o usuário consente com o respectivo tratamento de dados.

1 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

Apesar de o consentimento ser, de fato, base legal listada pela LGPD como capaz de autorizar o tratamento, ele não pode, nem deve, ser amplamente utilizado em qualquer situação e de forma genérica.

O consentimento tem limites à sua utilização como base legal para o tratamento de dados. No presente capítulo, esses limites serão abordados da seguinte maneira: na primeira parte será feita uma apresentação do tema e seus principais conceitos; na segunda parte serão demonstrados os limites gerais à utilização do consentimento; e, por último, na terceira parte serão trazidos critérios objetivos para a verificação do consentimento válido e adequado, capaz de preencher as características exigidas por lei (livre, informado, inequívoco e com finalidade determinada).

Ao longo do texto serão trazidos diversos artigos da LGPD brasileira e será feito um paralelo, em muitos pontos, com o regulamento europeu sobre o tema (*General Data Protection Regulation*) que funciona como referência para o brasileiro, orientando tanto a aplicação, quanto a interpretação do novo diploma normativo nacional.

Bases legais da LGPD

A importância de estudar as bases legais quando a temática é proteção de dados reside no fato de que as bases legais são as situações ou hipóteses responsáveis por autorizar e permitir o tratamento de dados no Brasil, nos termos da LGPD[2] – regramento sobre proteção de dados no Brasil, inspirado na legislação europeia[3] e que entrou em vigência no ano de 2020.

A LGPD, apesar de tutelar o tratamento de dados além do meio digital (abrangendo também o mundo *off-line*), surge diante do contexto atual de constante e crescente volume de dados fornecidos pelos

2 *Ibidem*.

3 *General Data Protection Regulation (EU GDPR)*.

indivíduos, através da internet, na "Sociedade da Informação"[4] onde predomina a "*hiperinformação*"[5] e uma economia de dados "interconectada por um sistema nervoso eletrônico".[6]

Esse contexto apontou para a necessidade da criação de legislação específica para a proteção de dados pessoais visando conferir ao indivíduo instrumentos legais para a tutela de seus dados e direitos,[7] bem como para facilitar o controle dos dados tratados e definir deveres e responsabilidades daqueles que realizam os tratamentos de dados pessoais.[8]

A fim de contextualizar o leitor com conceitos imprescindíveis à compreensão do presente artigo, é importante conceituar o que seria tratamento de dados pessoais, termo com definição ampla dada pela própria LGPD (artigo 5º, inciso X):

> Art. 5º Para os fins desta Lei, considera-se: [...] X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.[9]

4 DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In*: MARTINS, Guilherme Magalhães (coord.). *Direito Privado e Internet*: atualizado pela Lei 12.965. São Paulo: Atlas, 2014. p. 61-78.

5 HAN, Byung-Chul. *Sociedade da transparência*. Tradução: Enio Paulo Giachini. Petrópolis: Vozes, 2017.

6 CASTELLS, Manuel. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Tradução: Maria Luiza X. de A. Gorges. Rio de Janeiro: Zahar, 2013. p. 11.

7 BUCHAIN, Luiz Carlos. A Lei Geral de Proteção de Dados: noções gerais. *Revista dos Tribunais*, São Paulo, ano 108, v. 1010, p. 209-229, 2019.

8 TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo (coord.). *Lei Geral de Proteção de Dados Pessoais*: e suas repercussões no Direito brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 287-322.

9 BRASIL. Lei nº 13.709, *op. cit.*

Do mesmo modo, o conceito de titular de dados também deve ser esclarecido: sendo o titular sempre uma pessoa física, conforme a LGPD (artigo 5º, inciso V), é a *pessoa natural a quem se referem os dados pessoais que são objeto de tratamento*.[10]

Já dado pessoal, conforme a referida lei (artigo 5º, inciso I), seria a *informação relacionada a pessoa natural identificada ou identificável*.[11]

Feita a contextualização do tema e entendidos os conceitos imprescindíveis, é retomada a importância do estudo das bases legais. De modo geral as bases legais que autorizam o tratamento de dados estão elencadas nos incisos do artigo 7º da lei:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I – mediante o fornecimento de consentimento pelo titular;
> II – para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;

10 BRASIL. Lei nº 13.709, *op. cit.*

11 *Ibidem*.

> VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.[12]

Vale ressaltar que o artigo 11 da LGPD[13] também elenca bases legais, porém para o tratamento de dados pessoais sensíveis, dados aos quais a lei acrescenta uma camada a mais de proteção.

Deve-se observar também que para que o tratamento realizado seja legítimo, é suficiente a utilização de apenas uma das bases legais elencadas, sendo possível ainda que mais de uma base legal autorize determinado tratamento de dados.[14]

Assim, quando um agente de tratamento realiza o tratamento de dados ele precisa estar amparado em pelo menos uma das bases legais elencadas na lei que fundamente sua atividade.[15]

Os agentes de tratamentos são divididos entre controladores e operadores: aqueles (pessoas físicas ou jurídicas) que coletam os dados e tomam as decisões referentes ao tratamento de dados pessoais (controlador) ou aqueles que realizam o tratamento de dados pessoais em nome do controlador (operador), conforme o artigo 5º da lei.[16] Por

12 BRASIL. Lei nº 13.709, *op. cit.*

13 BRASIL. Lei nº 13.709, ***op. cit***.

14 LIMA, Caio César Carvalho. Capítulo II Do Tratamento de Dados Pessoais. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 179-214.

15 TEPEDINO; TEFFÉ, *op. cit.*

16 BRASIL. Lei nº 13.709, *op. cit.*

isso, cabe ao controlador definir qual a base legal mais apropriada em cada caso.[17]

Daí a importância de se discutir quais os limites de aplicação e uso de cada uma das bases legais que não podem ser utilizadas de maneira indiscriminada, na medida em que o uso indiscriminado permitiria abusos no tratamento de dados pessoais dos respectivos titulares, bem como desrespeitaria os fundamentos da referida lei, dispostos no artigo 2º.[18]

É dizer, para que o tratamento de dados ocorra é preciso que ele ocorra dentro de certos limites. Tais limites incluem observância aos fundamentos e princípios da lei (artigos 2º e 6º, respectivamente), observância aos direitos do titular de dados e a definição de critérios objetivos para a utilização e aplicação das bases legais. Todos esses limites ainda devem ser aplicados a partir de uma reflexão que considere o contexto brasileiro de tratamento de dados.

Entre as bases legais elencadas na lei, da leitura do artigo 7º se infere que algumas necessitam de um debate maior para a definição dos seus limites quando comparadas às outras, que parecem ter uma aplicação mais restrita e mais bem definida.[19]

Exemplo: o inciso IV do artigo 7º autoriza o tratamento de dados *para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais*.[20] Além de a maioria dos controladores não realizar tal tipo de atividade, a própria lei traz a definição do que seria órgão de pesquisa (artigo 5º, inciso XVIII[21]), daí que esta é, evidentemente, uma base legal com aplicação restrita

17 LEONARDI, Marcel. Principais bases legais de tratamento de dados pessoais no setor privado. *In*: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). *Caderno Especial*: Lei Geral de Proteção de Dados (LGPD). São Paulo: Revista dos Tribunais, 2019. p. 71-85.

18 BRASIL. Lei nº 13.709, ***op. cit***.

19 *Ibidem*.

20 BRASIL. Lei nº 13.709, *op. cit*.

21 *Ibidem*.

devida à sua própria descrição e que não suscita grandes debates acerca dos seus limites.

Contudo, esse não é o caso de outras bases legais que exigem um debate maior, como as bases legais relativas ao consentimento, execução do contrato e legítimo interesse do controlador ou de terceiros (respectivamente elencadas nos incisos I, IV e IX do referido artigo 7º).[22]

O presente trabalho se atém a analisar os limites para a utilização do consentimento como capaz de autorizar o tratamento de dados. Ou seja, analisar os fundamentos e princípios trazidos pela lei, os direitos do titular de dados e a definição de critérios objetivos para um consentimento válido.

No contexto brasileiro, essa análise ganha relevância diante do contexto social da população que, muitas vezes, não tem níveis de conhecimento, informação e escolaridade elevados, o que torna necessário o debate sobre o tema a fim de se efetivar uma proteção aos titulares de dados.

Consentimento: definição e limites gerais

O consentimento do titular, como visto, é a primeira base legal trazida pela lei como hipótese autorizativa do tratamento de dados pessoais.

O fato de ela ser a primeira base legal listada denota sua importância, contudo, pode também causar uma ideia errada de que ela se adequa à maioria dos casos, o que não é verdade como se verá adiante, apesar de ser uma base legal muito utilizada pelos controladores, principalmente no setor privado. É, em verdade, uma base legal utilizada normalmente, pelo controlador, numa relação direta com o titular dos dados, principalmente por meio do aceite de termos de uso, políticas de privacidade e afins.[23]

22 *Ibidem*.

23 LEONARDI, *op. cit.*

O consentimento é também base legal capaz de autorizar, inclusive, o tratamento de dados pessoais sensíveis, conforme disciplina o artigo 11 da LGPD. A esses dados a lei acrescenta uma série de proteções específicas diante do seu maior impacto na vida do indivíduo que é seu titular. Assim, os dados pessoais sensíveis são aqueles que se referem à:

> origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.[24]

Em relação ao conceito propriamente dito do consentimento, a própria legislação também traz uma definição como *manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*, no artigo 5º, inciso XII,[25] definição muito similar à definição da GDPR.[26]

Tal definição não esgota os limites de utilização do consentimento como base legal para o tratamento de dados, mas é um ponto de partida para a discussão, uma vez que ela exige um consentimento livre, informado, inequívoco e voltado para uma finalidade específica.

Contudo, será preciso definir critérios para o que pode ser considerado como consentimento, efetivamente, livre, informado, inequívoco e com finalidade específica. A definição desses critérios será mais bem detalhada no próximo tópico deste capítulo, porém, é importante essa introdução.

24 BRASIL. Lei nº 13.709, *op. cit.*

25 *Ibidem*.

26 Art. 4º (11) da *General Data Protection Regulation (EU GDPR)*: 11. 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.

Então, de forma geral, o consentimento representa a liberdade de escolha, é instrumento da manifestação individual por meio da qual permite que terceiros utilizem, para determinados fins, os dados do respectivo titular.[27]

Como limites gerais ao consentimento, podemos extrair da legislação os princípios e fundamentos que a norteiam e os direitos dos titulares de dados. Tais limites devem ser considerados no momento da análise se o consentimento é base legal adequada a ser utilizada em determinado caso prático.

Sobre os fundamentos trazidos pela LGPD enquanto limites à utilização do consentimento para autorizar o tratamento de dados, destaca-se a importância de se considerar, na análise, se estão sendo atendidos no caso prático o respeito à privacidade, a inviolabilidade da intimidade, da honra e da imagem, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.[28]

Os fundamentos da lei são como sua base, sua razão,[29] portanto, o fornecimento do consentimento pelo titular e a utilização desse consentimento como base legal apropriada a um caso concreto não se dão de qualquer forma, pois eles devem respeitar os fundamentos.

Ou seja, o simples fornecimento do consentimento pelo titular para o acesso à câmera do seu dispositivo celular por um aplicativo, não autoriza que tal câmera acesse indiscriminadamente domínios invioláveis da vida doméstica, pessoal e privada, por exemplo, sob pena de se estar ferindo o direito à intimidade e privacidade do indivíduo,[30] nesse caso, fundamentos muito importantes da LGPD.

27 TEPEDINO; TEFFÉ, *op. cit.*

28 BRASIL. Lei nº 13.709, *op. cit.*

29 COMPARATO, Fábio Konder. *Rumo à Justiça*. São Paulo: Saraiva, 2010. p. 41.

30 WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*. Cambridge, v. 4, n. 5, p. 193-220, 1890.

Do mesmo modo, um agente de tratamento, ainda que possua o consentimento fornecido pelo titular do dado, deve se preocupar com a exatidão e completude que aqueles dados refletem, sob pena de ferir outro fundamento da lei: o livre desenvolvimento da personalidade. Isso porque os dados tratados passam a representar, perante terceiros, a identidade daquele indivíduo, tendo a proteção de dados papel importante na realização do homem na sociedade e em suas relações.[31]

Sobre os princípios orientadores trazidos pela LGPD, a maioria dispostos no artigo 6º[32] da lei, ainda que seja dado pelo titular o consentimento para o tratamento de dados pessoais, tal tratamento só terá lugar se observado tais princípios, uma vez que os princípios determinam a aplicação das demais normas a eles subordinadas.[33]

Os princípios mais relevantes para este trabalho são os princípios da finalidade, adequação, necessidade, livre acesso e transparência e não discriminação.

Nesse sentido, ainda que exista consentimento fornecido pelo titular, o tratamento de dados somente terá lugar se a finalidade específica e detalhada do tratamento existir e tiver sido devidamente informada (princípio da finalidade), se o tratamento se ativer à sua finalidade respectiva (princípio da adequação) e se o tratamento ocorrer somente sobre os dados necessários para o cumprimento daquela finalidade – é o que a normativa europeia sobre proteção de dados[34] chama, em seu artigo 5º, de minimização de dados – (princípio da necessidade), uma vez que *para a proteção jurídica da privacidade, é fundamental restringir,*

31 BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. São Paulo: Renovar, 2018. p. 86.

32 BRASIL. Lei nº 13.709, *op. cit.*

33 LUCCA, Newton de. Marco Civil da Internet. Uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III*: Marco civil de internet. Quartier Latin, 2015. p. 9.

34 General Data Protection Regulation (EU GDPR), *op. cit.*

tanto no tempo, como na qualidade e quantidade, as informações que circulam pelos bancos de dados.[35]

Além disso, o titular deve ter meios de consultar informações claras e precisas, quanto à forma e à duração do tratamento dos seus dados (princípio do livre acesso e transparência), principalmente no meio virtual, no qual, com o avanço tecnológico, o tratamento de dados sofre diversas mudanças rapidamente. Por fim, não é permitido o tratamento realizado com fins de discriminação de qualquer tipo (princípio da não discriminação), como, por exemplo, aqueles tratamentos que possam dificultar o acesso ao crédito ou a empregos por determinados indivíduos.[36]

Inclusive, nesse ponto da obrigatoriedade de não discriminação, o próprio regramento europeu – muito útil como parâmetro para interpretação da LGPD e orientação para sua aplicação prática – dispõe:

> A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião

35 BESSA, Leonardo Roscoe. *Cadastro positivo*: comentários à Lei 12.414/2011. São Paulo: Revista dos Tribunais, 2011. p. 93-94.

36 TEPEDINO; TEFFÉ, *op. cit.*

> ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos.[37]

Por fim, em relação aos direitos do titular de dados (trazidos no capítulo III[38] da LGPD), a lei assegura a titularidade de seus dados pessoais e os direitos fundamentais de liberdade, de intimidade e de privacidade ao titular, bem como assegura direitos do titular diante do controlador de dados, incluídos aí os direitos do titular de solicitar a eliminação de dados, ainda que estes sejam tratados com seu consentimento, de ser informado sobre a possibilidade e consequências do não fornecimento do consentimento para o tratamento, bem como o direito de revogar o consentimento dado anteriormente.

Ou seja, para que um controlador se utilize da base legal do consentimento para o tratamento de dados, não basta colher o consentimento do titular, ele deve garantir os direitos daquele titular de dados que, aplicados juntos, buscam uma completa proteção de dados pessoais.[39] Ou seja, o controlador deve eliminar dados solicitados pelo titular, deve acatar revogação de consentimento, além de dever informar acerca da existência da possibilidade de não ser dado aquele consentimento e o que aconteceria nesse caso.

Não basta colher o consentimento, se não forem respeitados os direitos do titular. Nesse ponto, os direitos do titular são verdadeiros limites à utilização indiscriminada do consentimento e, caso o consentimento seja colhido e utilizado para o tratamento de dados, porém, em paralelo, o titular não tenha seus direitos respeitados, essa questão pode ser discutida pelo titular, inclusive judicialmente

37 Considerando 71 da General Data Protection Regulation (EU GDPR), *op. cit.*

38 BRASIL. Lei nº 13.709, *op. cit.*

39 MALDONADO, Viviane Nóbrega. Capítulo III Dos Direitos do Titular. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 215-243.

ou através de uma denúncia no Ministério Público, a fim de o titular fazer valer seus direitos.

Explorados alguns limites gerais para a utilização do consentimento como base legal suficiente ao tratamento de dados – fundamentos e princípios trazidos pela LGPD e direitos do titular –, será trabalhada a seguir a importância da definição de critérios objetivos para um consentimento válido e quais seriam tais critérios, a fim de fornecer um viés mais prático na investigação acerca da correta aplicação do consentimento como base legal em um caso concreto.

Critérios objetivos para um consentimento válido

A preocupação em trazer conceitos objetivos para o estabelecimento de um consentimento válido surge na era tecnológica e digital atual, marcada pela coleta e pelo tratamento massivo de dados pessoais dos indivíduos, pela mercantilização desses dados e diversas dificuldades de transparência e informação na comunicação ao titular sobre o tratamento dos seus dados.[40] Essa preocupação é ainda mais necessária no Brasil, quando, como já dito, grande parte da população, muitas vezes, não tem níveis de informação geral e escolaridade elevados.

O que é certo afirmar é que, hoje, se visualiza o fracasso do modelo do *notice-and-consent*,[41] que presume uma ampla cognição dos extensos termos de uso e políticas de privacidade para contratações entre as partes – especialmente contratações *on-line*. Também não se adequa mais à realidade atual e à própria LGPD o modelo *take it or leave it*

40 TEPEDINO; TEFFÉ, *op. cit.*

41 ZANATTA, Rafael. *Proteção de Dados Pessoais como Regulação de Risco*: uma nova moldura teórica?. *In*: ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1., 2017, Rio de Janeiro. *Anais* [...]. Rio de Janeiro, [*s. n.*], 2017. p. 175-193.

choice,[42] modelo da lógica binária das políticas de privacidade,[43] nas quais o usuário ou aceita indiscriminadamente todas as disposições e termos do serviço/aplicativo ou não pode utilizá-lo.

Esses modelos antigos dão lugar ao consentimento com as seguintes características: livre, informado, inequívoco e com finalidade determinada. Tais características são exigidas pela própria LGPD, como já visto, e podem ser constatadas a partir da verificação sobre se há ou não a obediência a determinados critérios.

Atendidos determinados critérios, estarão presentes as características necessárias para o consentimento ser utilizado como base legal adequada para o tratamento de dados pessoais.

Comecemos definindo o consentimento livre. Livre é o consentimento no qual o titular pode escolher aceitar ou recusar a utilização de seus dados sem vícios de consentimento, sem vícios de manifestação da vontade.[44]

Não poderá o titular sofrer pressão ou coação para a entrega dos seus dados, o que é um critério muito importante uma vez que o controlador de dados normalmente está em uma posição superior sobre o titular que é hipossuficiente na relação e – em regra – ocupa a posição de consumidor do produto ou serviço fornecido.

Inclusive, por esse mesmo motivo, não é recomendado que a base legal do consentimento seja utilizada em relação aos tratamentos de dados nas relações de emprego ou nas relações com o poder público, isso porque, normalmente, o empregador e o ente público (controladores) estarão em posição hierarquicamente superior ao empregado ou cidadão que tem seus dados coletados naquelas situações.[45]

42 BORGESIUS, Frederik. J. Zuiderveen; KRUIKEMEIER, Sanne; BOERMAN, Sophie C.; HELBERGER, Natali. Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy regulation. *European Data Protection Law Review*, Berlin, v. 3, n. 3, p. 353-368, 2017.

43 TEPEDINO; TEFFÉ, *op. cit.*

44 TEPEDINO; TEFFÉ, *op. cit.*.

45 ARTICLE 29 Working Party (European Data Protection Board – EDPB). [*S. l.*: *s. n.*], 2017.

Tal entendimento da livre manifestação da vontade implica no fato segundo o qual, consequentemente, o titular deverá ter opções em relação a quais serão os dados coletados, considerando seus possíveis usos, podendo escolher entre fornecer ou não dados que não sejam necessários para a realização de determinado serviço ou compra.

No mesmo sentido também dispõe a GDPR:

> Artigo 7º Condições aplicáveis ao consentimento. [...] 4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.[46]

Inclusive, o *Article 29 Working Party*[47] aborda o caso prático de um banco que solicita consentimento dos seus clientes para utilizar os dados de pagamentos para fins de *marketing*, o que, evidentemente, não é necessário para a execução dos serviços bancários. Nesse caso, não poderia a negativa do cliente em consentir com o tratamento de seus dados para finalidade de *marketing* provocar a negativa da prestação dos serviços bancários.

É por essa razão que, caso o fornecimento de determinado dado seja indispensável para a realização daquele serviço, isso será informado de forma destacada ao titular, conforme o indica o artigo 9º, §3º da LGPD.[48]

Essa possibilidade de escolha do titular de dados em fornecer ou não dados que não sejam necessários para a realização de determinado serviço ou compra, também implica no preenchimento de um outro critério: o critério da granularidade. É dizer: o consentimento deve ser

46 *General Data Protection Regulation* (EU GDPR).

47 Article 29 Working Party (European Data Protection Board – EDPB). Guidelines on Consent under Regulation 2016/679. [*S. l.*: *s. n.*], 2016.

48 BRASIL. Lei nº 13.709, *op. cit.*

dado de forma granular que permita ao titular escolher quais dados vai fornecer e para quais finalidades, não se permitindo o modelo *take it or leave it* mencionado anteriormente.

Nesse sentido, leciona Bruno Bioni:

> Em síntese, o 'cardápio de opções' à disposição do cidadão calibrará o quão livre é o seu consentimento, na exata medida em que esse 'menu' equaliza tal relação assimétrica.
> Um exemplo claro dessa abordagem é a emergência dos chamados painéis de privacidade que procuram fugir da lógica do 'tudo' ou 'nada' das políticas de privacidade e, em última análise, da dinâmica dos contratos de adesão. O leque de opções dessas ferramentas oxigena processos de tomadas de decisões antes sufocados pela lógica binária do *take-it* ou *leave-it*.[49]

O critério da granularidade também será necessário para verificar a presença da característica do consentimento com finalidade determinada. Os critérios, por vezes, podem ser comuns para a verificação de determinadas características essenciais ao consentimento válido.

Outro critério que o consentimento livre também exige é o acesso facilitado do titular a retirar tal consentimento a qualquer tempo e de forma simples, sem ser prejudicado.[50] Nesse sentido, a LGPD dispõe em seus artigos 8º e 15:

> Art. 8º. § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do *caput* do art. 18 desta Lei.

49 BIONI, *op. cit.*, p. 248-249, grifo do autor.

50 Considerando 42 *da General Data Protection Regulation (EU GDPR)*, grifo do autor.

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: [...] III – comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público.[51]

Ou seja, os critérios para um consentimento livre são: ausência de vícios de manifestação da vontade, existência de escolha do titular e opções em relação a quais serão os dados coletados, granularidade e acesso facilitado do titular, principalmente para revogar o consentimento.

Já consentimento com a característica de ser informado é aquele em que o titular possui as informações corretas, completas, transparentes e suficientes sobre o tratamento de dados que terá lugar, suas finalidades e motivos, riscos e consequências,[52] possibilitando a tomada de decisão consciente sobre dispor ou não dos seus dados pessoais.

Por isso a LGPD dispõe que, em caso de alteração nas informações sobre finalidades, forma e duração do tratamento, identificação do controlador ou compartilhamento de dados, o titular deve ser informado:

> Art. 8º. § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º[53] desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.[54]

51 BRASIL. Lei nº 13.709, *op. cit.*

52 BIONI, *op. cit.*, p. 244-248.

53 "Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I – finalidade específica do tratamento; II – forma e duração do tratamento, observados os segredos comercial e industrial; III – identificação do controlador; [...] V – informações acerca do uso compartilhado de dados pelo controlador e a finalidade [...]". BRASIL. Lei nº 13.709, *op. cit.*

54 *Ibidem*.

As informações que devem ser disponibilizadas obrigatoriamente ao titular de dados estão no artigo 9º da LGPD e, caso sejam muito extensas para constar na cláusula de consentimento, podem constar em políticas de privacidade ou documentos correlatos que estejam disponíveis de fácil acesso ao titular, indicando na cláusula de consentimento onde e como encontrar tais informações.

A lei ainda reforça a exigência de transparência e exatidão das informações fornecidas ao titular sob pena de se considerar nulo o consentimento colhido:

> Art.9º. § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.[55]

Outro critério para que o consentimento seja informado é a disponibilização de informações de maneira clara, numa linguagem simples que seja facilmente compreendida pelo titular: devem ser evitados termos técnicos desnecessários de difícil compreensão pelo público geral e textos longos (informações podem ser concentradas preferencialmente em um ou poucos documentos). Além disso, a comunicação deve ocorrer na língua portuguesa.[56]

Inclusive, a forma por meio da qual é fornecido o consentimento não precisa ser escrita; pode ser adotada outra forma, desde que o titular possua as informações necessárias para a tomada daquela decisão.

Nesse sentido, um exemplo trazido pelo *Article 29 Working Party*[57] é o seguinte: girar um celular em sentido horário ou deslizar o dedo na tela do aparelho podem ser opções de indicar o consentimento,

55 BRASIL. Lei nº 13.709, *op. cit.*

56 LIMA, *op. cit.*

57 ARTICLE 29 Working Party (European Data Protection Board – EDPB). Guidelines on Consent under Regulation 2016/679, op. cit.

desde que as informações sobre o modo de manifestar a concordância tenham sido passadas de maneira clara para o titular.

Ou seja, os critérios para um consentimento informado são: completude e transparência da informação fornecida ao titular sobre o tratamento de dados, ao lado da utilização de linguagem simples e de fácil compreensão.

Por sua vez, consentimento inequívoco é aquele evidente, não ambíguo. Ele não necessita ser escrito, mas deve ocorrer por meio idôneo capaz de demonstrar a manifestação da vontade do titular, como menciona o artigo 8º da LGPD. Assim, o consentimento pode ocorrer por meio de cliques, preenchimento de caixas, áudio, vídeo, entre outros, desde que configure uma ação afirmativa que não deixe dúvidas sobre a intenção do cidadão.[58]

Ainda, caso o meio adotado para o consentimento seja o escrito, para deixá-lo evidente, deve vir destacado das demais cláusulas contratuais:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.[59]

A GDPR, também buscando a necessidade da evidência do consentimento, determina que o silêncio ou opções previamente validadas não são capazes de constituir um consentimento válido:

> O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto

58 BIONI, *op. cit.*, p. 249.251.

59 BRASIL. Lei nº 13.709, *op. cit.*

> que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento.[60]

Ou seja, os critérios para um consentimento inequívoco são evidência e não ambiguidade, ao lado de meio idôneo capaz de demonstrar a manifestação da vontade do titular.

Já consentimento para finalidade determinada, que se relaciona ao consentimento informado, é aquele no qual a finalidade da coleta e tratamento dos dados é conhecida pelo titular.

Aqui, o propósito do agente de tratamento deverá ser explícito, ou seja, aquelas informações como "estamos colhendo seus dados para melhorar sua experiência como cliente"[61] são muito genéricas e não representam a coleta de um consentimento válido.

A LGPD também dispõe sobre a necessidade de determinação da finalidade na coleta do consentimento, inclusive prevendo que caso ocorra mudança na finalidade do tratamento de dados pessoais, tal mudança deverá ser informada ao titular (artigo 9º, §2º),[62] bem como caso o controlador necessite compartilhar os dados com terceiros deverá colher consentimento para tal finalidade (artigo 7º, §5º).[63]

Essa preocupação com a observância da finalidade no tratamento de dados já estava presente no regramento brasileiro desde o Marco Civil da Internet, que dispunha em seu artigo 16 ser vedada a guarda, na provisão de aplicações de internet, de *dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular*.[64]

60 Considerando 32 da General Data Protection Regulation (EU GDPR).

61 BIONI, *op. cit.*, p. 249.251.

62 BRASIL. Lei nº 13.709, *op. cit.*

63 *Ibidem*.

64 BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: seção 1, Brasília, DF, ano 151, n. 77, p. 1-3, 24 abr. 2014.

Tal disposição do Marco Civil da Internet se comunica também com o princípio da necessidade já trabalhada no item 3, deixando claro que, ao analisar se um consentimento é válido ou não, deve ser feita uma interpretação conjunta dos limites trazidos no presente capítulo para se chegar a uma conclusão correta.

Outro critério que deve ser preenchido para a caracterização do consentimento com finalidade determinada, é o critério da granularidade já trabalhado ao abordar a característica do consentimento livre. Nos dizeres do artigo 8º, §4º da LGPD, *o consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas*.

No mesmo sentido, a GDPR:

> Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.[65]

Ou seja, os critérios de um consentimento previsto para uma finalidade determinada envolvem a informação do titular sobre a finalidade ou as finalidades daquela coleta e tratamento e o cumprimento do critério da granularidade.

Cabe lembrar ainda que, quando o consentimento é fornecido em situações que apresentam maior risco para o titular dos dados – quais sejam, o consentimento para o tratamento de dados pessoais sensíveis (artigo 11, inciso I), para o tratamento de dados de crianças (artigo 14, §1º) ou para transferência internacional de dados pessoais (artigo 33, inciso VIII) –, a LGPD[66] adiciona duas outras características que devem ser cumpridas: o consentimento deverá ser específico e destacado.

65 Considerando 43 da General Data Protection Regulation (EU GDPR).

66 BRASIL. Lei nº 13.709, *op. cit.*

Específico é o consentimento expresso que exige maior atuação do titular de dados ao fornecer sua anuência. Concordando com esse posicionamento, Bioni leciona:

> Uma das maneiras de extrair essa carga participativa maior do titular dos dados seria adotar mecanismos que chamassem mais a sua atenção. Deve haver um alerta que isole não só o dever-direito de informação, como, também, a declaração de vontade, colando-a à situação na qual é exigido o consentimento específico. [...] Mais uma vez, será necessário analisar o grau e a qualidade de interação de todo o processo que desengatilha a declaração de vontade. Isso pode variar de mensagens textuais, imagens até um sistema que combine ambos e seja de dupla verificação do consentimento, como seria o caso em que o titular dos dados dá o 'concordo' em um website e, posteriormente, o confirma por e-mail.[67]

E destacado é o consentimento que fornece ao titular efetivo acesso ao local ou documento que esclarece todos os fatos relevantes sobre o tratamento de seus dados pessoais, o que pode se concretizar através do destaque das partes relativas ao tratamento de dados no texto, vídeo ou áudio que contém a informação. Por exemplo, se as informações de tratamento de dados forem veiculadas em texto escrito, o trecho respectivo pode receber destaque através de recursos como uso de caixa alta ou negrito.[68]

Feitas todas as considerações, fica evidenciado que para um consentimento ser livre, informado, inequívoco e com finalidade determinada (e em alguns casos ainda específico e destacado), devem ser observados todos os critérios expostos acima. Isso implica no dever de o agente de tratamento, ao colher o consentimento do titular, se preocupar com o atendimento desses critérios.

Por outro lado, a exposição de critérios objetivos para que o consentimento seja utilizado como base legal adequada ao tratamento

67 BIONI, *op. cit.*, p. 252.

68 LIMA, *op. cit.*, p. 198-210.

de dados, facilita que o titular, no caso concreto, visualize se aquele consentimento fornecido possui ou não validade e possa, assim, exigir seus direitos perante o controlador.

Considerações finais

Diante do exposto, serão trazidas algumas considerações finais:

A análise desenvolvida mostra que o caminho para verificação do consentimento válido e adequado para servir como base legal ao tratamento de dados pessoais é um caminho longo e perpassa pela verificação dos seus limites, tanto os gerais, quanto os critérios objetivos;

Os limites gerais expostos foram: os princípios e fundamentos que norteiam a LGPD, bem como os direitos dos titulares de dados. O consentimento deve sempre estar de acordo com essas bases;

Além de observar os limites gerais postos, o consentimento deve ser também livre, informado, inequívoco e com finalidade determinada. Tais características exigem a obediência a determinados critérios a serem atendidas, de modo que o consentimento deve atender aos critérios de: ausência de vícios de manifestação da vontade, existência de escolha do titular e opções em relação a quais serão os dados coletados, granularidade, acesso facilitado, completude e transparência da informação fornecida, utilização de linguagem simples e de fácil compreensão, não ambiguidade e uso de meio idôneo capaz de demonstrar a manifestação da vontade do titular;

Em casos específicos, o consentimento ainda deverá ser específico e destacado;

Existe a expectativa que a Autoridade Nacional de Proteção de Dados (ANPD), criada pela LGPD, também regule o tema e elabore regramentos, inclusive emitindo pareceres e orientações sobre o que seria um consentimento válido e adequado;

Assim, apesar de amplamente utilizado, nem sempre o consentimento é a base legal mais adequada para todos os casos. Isso ocorre

diante da dificuldade prática em atender aos limites e critérios para um consentimento válido e adequado, bem como diante da dificuldade operacional do agente de tratamento em checar a todo tempo se o consentimento está vigente, uma vez que há ampla possibilidade de revogação do consentimento pelo titular, devendo os controladores buscarem, em muitos casos, outras bases legais para a justificativa do tratamento de dados pessoais.

Referências

ARTICLE 29 Working Party (European Data Protection Board – EDPB). *Guideline 259/2017*. [*S. l.: s. n.*], 2017.

ARTICLE 29 Working Party (European Data Protection Board – EDPB). Guidelines on Consent under Regulation 2016/679. [*S. l.: s. n.*], 2016.

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

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. São Paulo: Renovar, 2018.

BORGESIUS, Frederik. J. Zuiderveen; KRUIKEMEIER, Sanne; BOERMAN, Sophie C.; HELBERGER, Natali. Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy regulation. *European Data Protection Law Review*, Berlin, v. 3, n. 3, p. 353-368, 2017.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: seção 1, Brasília, DF, ano 151, n. 77, p. 1-3, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

BUCHAIN, Luiz Carlos. A Lei Geral de Proteção de Dados: noções gerais. *Revista dos Tribunais*, São Paulo, ano 108, v. 1010, p. 209-229, 2019.

CASTELLS, Manuel. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Tradução: Maria Luiza X. de A. Gorges. Rio de Janeiro: Zahar, 2013.

COMPARATO, Fábio Konder. *Rumo à Justiça*. São Paulo: Saraiva, 2010.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In*: MARTINS, Guilherme Magalhães (coord.). *Direito Privado e Internet*: atualizado pela Lei 12.965. São Paulo: Atlas, 2014. p. 61-78.

GENERAL Data Protection Regulation (EU GDPR). [*S. l.: s. n.*], [2016].

LEONARDI, Marcel. Principais bases legais de tratamento de dados pessoais no setor privado. *In*: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). *Caderno Especial*: Lei Geral de Proteção de Dados (LGPD). São Paulo: Revista dos Tribunais, 2019. p. 71-85.

LIMA, Caio César Carvalho. Capítulo II Do Tratamento de Dados Pessoais. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 179-214.

LUCCA, Newton de. Marco Civil da Internet. Uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III*: Marco civil de internet. São Paulo: Quartier Latin, 2015. p. 9.

HAN, Byung-Chul. *Sociedade da Transparência*. Tradução Enio Paulo Giachini. Petrópolis, RJ: Vozes, 2017.

MALDONADO, Viviane Nóbrega. Capítulo III Dos Direitos do Titular. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 215-243.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo (coord.). *Lei Geral de Proteção de Dados Pessoais*: e suas repercussões no Direito brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 287-322.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, p. 193-220, 1890.

ZANATTA, Rafael. Proteção de Dados Pessoais como Regulação de Risco: uma nova moldura teórica?. *In*: ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1., 2017, Rio de Janeiro. *Anais* [...]. Rio de Janeiro: [*s. n.*], 2017. p. 175-193.

EL CONSENTIMIENTO DEL MENOR EN LA NUEVA LEY DE PROTECCIÓN DE DATOS ESPAÑOLA, EN EL REGLAMENTO EUROPEO Y EN EL DERECHO COMPARADO

O CONSENTIMENTO DO MENOR NA NOVA LEI DE PROTEÇÃO DE DADOS ESPANHOLA, NO REGULAMENTO EUROPEU E NA LEI COMPARATIVA

Salvador Morales Ferrer

Introducción

En este, Siglo XXI en que vivimos, son pocos los menores que en estas sociedades desarrolladas que declaran no utilizar algunas de las más famosas herramientas, como *Facebook*, *Instagram* o, *Twitter*. Por tanto, el legislador español basándose en la Constitución Española de 1978[1] en su artículo 39 párrafo 4º de la Constitución Española que señala: "Los niños gozarán de la protección prevista en los acuerdos internacionales que velan por sus derechos". Por lo que, el legislador español se adecua a la Declaración Universal de Derechos Humanos[2] que en

1 ESPAÑA. *Constitución Española*. Navarra: Editorial Aranzadi S.A. Cizur Menor, 2003.

2 UNIÓN EUROPEA. Declaración Universal de Derechos Humanos [República del Paraguay]: Unión Europea, 1948.. Adoptada y proclamada por la Asamblea General en su resolución 217 A (III), de 10 de diciembre de 1948. p. 4.

su artículo 12 menciona: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" y, dos décadas después España se consolido en el Pacto de Derechos Civiles y Políticos[3] en su artículo 17 que señala: "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques" y, la Convención sobre los Derechos del Niño que en su artículo 16 manifiesta: "Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, o su correspondencia, ni de ataques ilegales a su honra y a su reputación. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".[4] En definitiva, el texto constitucional español se adecua a las normativas internacionales. Por lo que, tanto el legislador español en la Protección de datos de 2018, así como el legislador europeo se adaptaron a la protección del menor y del adolescente en las redes sociales y, al mismo tiempo el legislador latino americano promulgó su legislación en la protección de este colectivo. Con el presente artículo se pretende realizar un análisis jurídico-descriptivo y, sus efectos tanto en España, Europa y algunos países de latino américa, El artículo tiene la siguiente estructura: el primero trata sobre la introducción de la protección de los menores y adolescentes; el segundo esboza la protección de datos de los menores y, adolescente como elemento protector; el tercero presenta la protección del menor y los adolescentes en el Reglamento Europeo;

3 PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS. Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966. Entrada en vigor: 23 de marzo de 1976, de conformidad con el artículo 49 Lista de los Estados que han ratificado el pacto. p. 7.

4 ESPAÑA. Convención sobre los Derechos del Niño. I Disposiciones generales. Jefatura del Estado. *Boletín Oficial del Estado* (BOE), Madrid. n. 313. BOE-A-1990-31312.

el cuarto atiende a la Protección de Datos de los menores y adolescentes en Brasil; el quinto aborda en la Protección de Datos en Colombia como elemento principal la protección de los menores y adolescentes; el sexto analiza quienes serán los que protejan a los menores y adolescentes en Colombia; el séptimo aclara la protección de los menores y, adolescentes en la nuevas tecnologías en Argentina; el octavo muestra las conclusiones del artículo de investigación; el noveno se refiere a las Referencias Bibliográficas.

La protección jurídica del menor y del adolescente en la Ley de Protección de Datos española

Por tanto, la Agencia Española de Protección de Datos en adelante (AEPD), ha conseguido que *Facebook Instagram* o, otras redes adecuen la edad mínima de sus usuarios a la legislación española establece que la edad mínima para que los menores puedan compartir información en este tipo de servicios es de catorce años. Tras el anuncio de la compañía a la AEPD, España se convierte en el único país en el que *Facebook* ha incrementado la edad mínima a catorce años para poder registrarse y, ser miembro de su red social. Respecto a la Ley de Protección de datos Española de 2018, está basada en el artículo 14 párrafo 8º de la Constitución Española que señala: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[5], del mismo modo hay que citar la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales que en su artículo 7 manifiesta:

5 ESPAÑA. Constitución Española, *op. cit.*, p. 75.

> El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela[6].

Por tanto, diferencia la edad del menor o, la menor en la edad que sea mayor de catorce años, excepto para la realización de un negocio jurídico, en el cual se recabará consentimiento del tutor, que pueden ser los padres progenitores o, adoptivos e incluso si no existen ambos, serán los tutores. Por otro lado, los menores o, las menores de catorce años, sí necesitarán el consentimiento del o, de los que ejercen la patria potestad, al hilo el autor Díaz manifiesta:

> La privacidad de la menor encierra, no sólo aquellas circunstancias que conforman la intimidad de las personas, sino también los datos o elementos que sirven para identificarla o diferenciarla de otras. Su peculiaridad, en cuanto derecho, deriva hacia la disposición que pueda hacerse por parte de terceros, y en consecuencia al control que el propio sujeto tenga sobre su contenido. De este modo, la principal preocupación que subyace en torno a los menores de edad estriba la configuración de su capacidad para prestar un consentimiento válido y eficaz. A menudo, las intromisiones ilegítimas en el derecho a la intimidad del menor van ligadas a la

6 ESPAÑA. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Jefatura del Estado. *Boletín Oficial del Estado (BOE)*: Madrid, seción 1, n. 294, 6 dez. 2018. p. 17.

> utilización en las redes sociales de imágenes o afirmaciones que ponen en entredicho su consideración social, por lo que con frecuencia se encuentran ligadas al amparo de otros derechos[7].

Por tanto, implican imágenes sensibles del menor o, la menor en las redes sociales que pueden derivarse estos en terceras personas atentando contra la intimidad del menor o, la menor, sin el previo consentimiento, al hilo cabe mencionar la Sentencia del Tribunal Supremo en sus Fundamentos de Derecho Segundo manifiesta:

> los menores tienen derecho al honor, intimidad e imagen y destaca que se considera intromisión ilegítima cualquier utilización de su imagen o su nombre en las medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contrario a sus intereses incluso sí consta el consentimiento del menor o de sus representantes legales; no digamos, si no media tal consentimiento[8].

Por lo cual, tanto el menor o, la menor de menores de catorce años o, los mayores de catorce años, si se vulnera su protección del honor, intimidad o, imagen por terceros bien si son menores de edad respecto a la edad penal que existe en España se les aplicará la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil en adelante (Ley del menor) como especifica su artículo 4 párrafo 3º manifiesta:

7 DÍAZ, Jesús. Redes sociales: incumplimiento sistemático de los controles técnicos versus vulneración reiterada de los derechos del menor. *Diario La Ley*, Madrid, n. 9326, 2018. p. 3.

8 Tribunal Supremo (Sala Primera de lo Civil) (Ponente: O'Callaghan Muñoz, Xavier) (Sentencia 774/2006 de 13 de Julio). Rec. 2947/2000. LA LEY 70229/2006.

> Se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales[9]

Por lo cual, aunque exista el consentimiento del menor o, la menor mayor de catorce años o, incluso menores de catorce años, los terceros que utilicen sus imágenes o, atenten contra su intimidad, se procederá a la aplicación de medidas penales y subsidiariamente responsabilidad civil, de esta forma como manifiesta la Ley del menor en su artículo 4 párrafo 4º:

> Sin perjuicio de las acciones de las que sean titulares los representantes legales del menor, corresponde en todo caso al Ministerio Fiscal su ejercicio, que podrá actuar de oficio o a instancia del propio menor o de cualquier persona interesada, física, jurídica o entidad pública[10]

Por lo que, se podrán intervenir penalmente de oficio en algunos casos, puesto como muy bien se expresa la Constitución Española en su artículo 20 párrafo 4º: "Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia"[11]. Lo que conlleva a la conclusión que tanto los menores de catorce años, así como los mayores de catorce años están protegidos

9 ESPAÑA. Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil. Jefatura del Estado. *Boletín Oficial del Estado (BOE)*: Madrid, seción 1, n. 15, 16 ene. 1996.

10 ESPAÑA. Ley Orgánica 1/1996, *op. cit.*, p. 8.

11 ESPAÑA. Constitución Española, *op. cit.*, p. 79.

en la Ley de Protección de Datos Personales y la garantía de los derechos digitales de España.

La protección jurídica del menor y del adolescente en el reglamento europeo

El Reglamento renuncia finalmente a determinar la edad mínima para el menor o, la menor para que otorgue el consentimiento como manifiesta el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) en adelante (RGPD) en su artículo 8 párrafo 3 que señala: "El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño"[12]. Por otro lado, el RGPD[13] en su artículo 8 párrafo 1º apartado 2º manifiesta: "Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años", por tanto, la RGPD, ofrece un libre albedrio a los Estados Miembros de la Unión Europea. Por otra parte, la RGPD en su artículo 8 párrafo 1º menciona: "Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como

12 UNIÓN EUROPEA. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*: Luxemburgo, 2016. p. L.119/38.

13 UNIÓN EUROPEA. Reglamento (UE) 2016/679, *op. cit.*, p. L.119/37.

mínimo 16 años".[14] por lo cual, son una serie de recomendaciones a los Estados miembros. Por otra parte, cabe mencionar al autor López que señala:

> Se trata de una solución de compromiso ante dos posturas que se enfrentaron en la tramitación del Reglamento, no solo entre Estados, sino entre Grupos del Parlamento Europeo: fijar la edad de acceso a redes sociales sin permiso paterno en 16 años o en 13 años como figuraba en los borradores iniciales, España de entre los Estados, el Grupo conservador, entre los Grupos del Parlamento Europeo, defendían como límite de edad los 16 años para actuar libremente en internet como garantía frente al peligro de los más jóvenes de al acoso, la pedofilia y el adoctrinamiento[15].

Por tanto, España fue uno de los países más conservadores de la Unión Europea para decidir la edad mínima legal y, la máxima sobre los menores o, las menores al hilo, cabe mencionar al autor Reyes que señala:

> En definitiva, pues, se observan varias deficiencias en el Reglamento europeo a la hora de proceder a una adecuada protección de los derechos del menor. En primer lugar, se proyecta un cierto desequilibrio entre los propósitos evidentes formulados en la Exposición de motivos y el mínimo tratamiento que después profesa en el texto articulado. Es consciente de la necesidad de amparo de los niños, pero a la hora de crear una reglamentación coherente y exhaustiva sólo lo hace de un modo muy limitado – escasamente en un solo artículo –. Además, la libertad que deja a los Estados para cambiar la edad mínima a partir de la cual se requiere el consentimiento de los padres – estableciendo un margen de 3 años – debilita la uniformidad

14 UNIÓN EUROPEA. Reglamento (UE) 2016/679, *op. cit.*, p. L.119/37.

15 LÓPEZ CALVO, José. *Comentarios al Reglamento Europeo de Protección de Datos*. Madrid: Editorial Jurídica Sepin, 2017. p. 184.

> del derecho europeo, permitiendo el ejercicio de derechos de modo discriminatorio dentro del Espacio Único, al equiparar la madurez de sujetos en una edad de su desarrollo propensa a sufrir cambios y alteraciones significativas en el entendimiento. Finalmente, deja un margen abierto, y quizás demasiado amplio, a los operadores del servicio de las redes sociales a la hora de verificar el consentimiento requerido. Otras cuestiones como la circulación de los datos o la cancelación de los mismos, ni siquiera han merecido un tratamiento particularizado[16]

Por lo que, en sí deja mucho de entrever el RGPD y, finalmente cabe mencionar el RGPD en su mismo artículo 8 apartado 2º manifiesta: "Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó",[17] por lo tanto en este apartado manifiesta que será licito siempre que exista uno o, los dos progenitores, tutores que autorizaron al menor, al hilo el autor al respecto el autor Reyes manifiesta: "También el Reglamento europeo es consciente de la dificultad de verificar el control hecho por parte de los padres y el consentimiento dado".[18] Por tal razón añade que "El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible", por lo cual, analógicamente el autor respecto al responsable del tratamiento se remite al RGPD a su artículo 6 párrafo 1º letra a) que señala: "El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: el interesado dio su consentimiento

16 REYES MÉNDEZ, Daniel. El acceso del menor a las redes sociales y el problema de su autentificación: la necesidad de una respuesta tecnológica. *Diario La Ley*, Madrid, n. 9335, 2019. p. 3.

17 UNIÓN EUROPEA. Reglamento (UE) 2016/679, *op. cit.*, p. L.119/38.

18 REYES MÉNDEZ, *op. cit.*, p. 3.

para el tratamiento de sus datos personales para uno o varios fines específicos"[19], al respecto cabe mencionar la Sentencia de la Audiencia Provincial de Cantabria en sus Fundamentos de Derecho Tercero (9) que manifiesta:

> Pretende, en fin, la madre de que se prohíba la utilización de la imagen de la menor sin el previo consentimiento de ambos progenitores y de que, del otro lado, la incorporación de la fotografía de un menor, en tanto que sea una persona física identificable, supone difundir un dato de carácter personal[20].

Por lo que, si uno de los padres progenitores no da el consentimiento al menor no será un consentimiento válido, puesto que el consentimiento debe ser expreso o tácito de ambos progenitores del menor, salvo como anteriormente sea visto en la Sentencia, que uno de los progenitores estaba separado y privado de la patria potestad del menor o, la menor.

La protección del menor y del adolescente en la Ley de Protección de Datos del Brasil

La Ley General de Protección de Datos en Brasil en adelante (LGPD) se remite a su artículo 14.1º que menciona: " El tratamiento de datos personales de niños, niñas y adolescentes debe realizarse en su mejor interés, en los términos de este artículo y la legislación pertinente",[21] por lo cual el legislador brasileño no aclara cual es la legislación es la pertinente, al hilo la autora Alejandra manifiesta: "El Estado es

19 UNIÓN EUROPEA. Reglamento (UE) 2016/679, *op. cit.*, p. L.119/36.

20 Audiencia Provincial de Cantabria (Sección 2ª) (Ponente: Arsuaga Cortázar, José) (Sentencia 24/2020 del 13 de enero), Rec. 805/2019. LA LEY 2099/2020.

21 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

responsable y al mismo tiempo garante de la protección, como indican los instrumentos mencionados, lo cual implícitamente lo convierte en el garante de la gobernabilidad del Sistema de Protección de Niñas, Niños y Adolescentes", [22] por lo tanto, cabe remitirse a la Constitución Brasileña de 1988 que su artículo 227 que señala:

> Es deber de la familia, la sociedad y el Estado garantizar que los niños, adolescentes y jóvenes, tengan derecho a la vida, la salud, la alimentación, la educación, a la recreación, la profesionalización, la cultura, la dignidad, al respeto, a la libertad y a la convivencia familiar y comunitaria, con absoluta prioridad, además de protegerlos de toda forma de negligencia, discriminación, explotación, violencia, crueldad y opresión[23].

Por otra parte, cabe destacar que la mayoría de edad en Brasil se alcanza a los dieciocho años, como menciona el Código Civil Brasileño en adelante (CCB) en su artículo 4 que señala: "Son incapaces, en relación con determinados actos y en la forma de ejercerlos: los menores de dieciséis y los menores de dieciocho",[24] lo que implica que antes de esta edad puedan ser adolescentes o, menores. Por otra lado, hay una cierta duda si los menores de edad casados entre dieciséis o, diecisiete años siempre con el consentimiento de los padres, puedan considerarse mayores de edad, por tanto se debe citar el CCB en su artículo 1630 que manifiesta: " Los hijos están sujetos al poder familiar en cuanto sean menores"[25] y, el CCB en su artículo 1631 señala: "Durante el casamiento y la unión estable, compete al poder familiar de los padres, en falta o

22 ALEJANDRA STUCHLIK, Silvia. *El Sistema de Protección Integral de Derechos de Niños, Niñas y Adolescentes de la Ciudad Autónoma de Buenos Aires*. Buenos Aires: Editorial Universidad de San Andrés, 2015. p. 10.

23 BRASIL. Constituição Federal do Brasil. *Mini Código Saraiva*. 21. ed. São Paulo: Saraiva, 2015. p. 140.

24 BRASIL. Código Civil. Lei n° 10.406, de 10 de janeiro de 2012. Mini Código Saraiva. 21. ed. São Paulo: Saraiva, 2015. p. 17.

25 BRASIL. Código Civil, *op. cit.*, p. 165.

impedimento de uno de ellos, el otro ejercerá con exclusividad".[26] Por tanto, aun estando casados los menores dependerán de los padres y, más clarificador es el CCB en su artículo 3º párrafo 1º que menciona: "Son absolutamente incapaces de ejercer personalmente los actos de la vida civil: Los menores de dieciséis años".[27] Por lo cual, como menciona LGPD en su artículo 14 párrafo 1º: "El tratamiento de los datos personales de los menores debe realizarse con el consentimiento específico y destacado prestado por al menos uno de los padres o tutor legal",[28] por tanto, si uno de los padres del menor o, la menor de edad está separado y, le conceden la patria potestad al otro si tendría validez puesto que el otro que no tiene patria potestad, no tendría validez. Por lo cual, el concepto tutor en el CCB se ciñe a su artículo 1637[29] que señala: "cabe al juez que requiera algún pariente, o el Ministerio Público, que adopte alguna medida que le parezca para la seguridad del menor". Por otro lado, la LGPD[30] en su artículo 14 apartado 2º manifiesta: "En el tratamiento de los datos a que se refiere el apartado 1 de este artículo, los responsables del tratamiento mantendrán pública información sobre los tipos de datos recabados, la forma de uso y los procedimientos para el ejercicio de los derechos a que se refiere el art. 18 de esta Ley". Por tanto, la LGPD en su artículo 18 1º señala: "El titular de los datos personales tiene derecho a obtener del responsable del tratamiento, en relación con los datos del titular tratados por él, en cualquier momento y previa solicitud",[31] en este caso serían los progenitores o, el progenitor que tenga la patria potestad o, su tutor. Por otro lado, la LGPD en su artículo 14 párrafo 3º menciona:

26 BRASIL. Código Civil, *op. cit.*, p. 165.

27 BRASIL. Código Civil, *op. cit.*, p. 17.

28 BRASIL. Lei nº 13.709, *op. cit.*, p. 7.

29 BRASIL. Código Civil, *op. cit.*, p. 166.

30 BRASIL. Lei nº 13.709, *op. cit.*, p. 7.

31 BRASIL. Lei nº 13.709, *op. cit.*, p. 10.

> Los datos personales de niños pueden recopilarse sin el consentimiento mencionado en el § 1 de este artículo cuando la recopilación sea necesaria para comunicarse con los padres o el tutor legal, se use solo una vez y sin almacenamiento, o para su protección, y en ningún caso podrá transmitirse a un tercero sin el consentimiento mencionado en el § 1 de este artículo[32].

Lo que implica, que al ser los menores incapaces como expresa el CCB y la LGPD, serán los padres o, tutores a quienes se les comuniquen los actos de los menores y, sin almacenamiento y, al mismo tiempo para proteger a los menores no se transmitirá aún tercero sin el consentimiento de los padres o, el padre que tiene la patria potestad o, tutor. Del mismo modo la LGPD en su artículo 14 párrafo 4º manifiesta:

> Los responsables del tratamiento no condicionarán la participación de los titulares a que se refiere el § 1 de este artículo en juegos, aplicaciones de Internet u otras actividades al suministro de información personal adicional a la estrictamente necesaria para la actividad[33].

Por tanto, queda aclarado que los responsables que realizarán el tratamiento de datos no condicionarán a los menores en el uso de aplicaciones de internet y, otros sobre su información personal, lo que claramente queda en un limbo jurídico. Por otra parte, la LGPD, en su artículo 14. Párrafo 5ª señala: "El responsable del tratamiento debe hacer todos los esfuerzos razonables para verificar que el consentimiento mencionado en el § 1 de este artículo fue otorgado por el responsable del niño, considerando las tecnologías disponibles".[34] Por lo cual, el responsable del tratamiento de los datos de los niños y las niñas, deberán los padres o, el padre, tutor notificar si concedieron

32 BRASIL. Lei nº 13.709, *op. cit.*, p. 8.

33 BRASIL. Lei nº 13.709, *op. cit.*, p. 8.

34 BRASIL. Lei nº 13.709, *op. cit.*, p. 8.

los permisos necesarios para la utilización de las herramientas de internet, aplicaciones etc. Por otro lado, la LGPD, está muy avanzada puesto que en su artículo 14 párrafo 6º menciona:

> La información sobre el tratamiento de los datos a que se refiere este artículo deberá facilitarse de forma sencilla, clara y accesible, considerando las características físico-motoras, perceptivas, sensoriales, intelectuales y mentales del usuario, utilizando los recursos audiovisuales cuando proceda, de forma para proporcionar la información necesaria a los padres o tutor legal y apropiada a la comprensión del niño[35].

Por lo que, el legislador brasileño está pensando en las niñas y, los niños con ciertas discapacidades físicas, intelectuales que alteren su comprensión. Por otra parte, la Autoridad Nacional de Protección de Datos la ANPD en su artículo 33 párrafo I manifiesta: "La transferencia internacional de datos personales soló ésta permitida en los siguientes casos: para países u organismos internacionales que blinden un grado de protección de datos personales adecuado al previsto en la Ley".[36] Por lo cual, puede existir una conexión con el RGPG de Europa como manifiesta en su artículo 40 párrafo 1º apartado j:

> Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas: la transferencia de datos personales a terceros países u organizaciones internacionales[37].

35 BRASIL. Lei nº 13.709, *op. cit.*, p. 8.

36 BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, 9 jul. 2019. p. 8.

37 UNIÓN EUROPEA. Reglamento (UE) 2016/679, *op. cit.*, p. L.119/57.

Lo que implica, en materia penal así, como la pornografía infantil, ambos pueden estar concatenados para la aplicación en materia penal en el país donde se haya cometido el acto delictivo, siempre que Brasil tenga un acuerdo con los países de la Unión Europea.

La protección de los menores y adolescentes en la Ley Protección de Datos en Colombia

Según la Constitución Política de la República de Colombia en su artículo 15 señala:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas[38]

Al respecto la autora Galvis menciona:

> En la Carta Constitucional se parte de un reconocimiento a los efectos de la informática y otros avances tecnológicos que facilitan la recolección, clasificación, almacenamiento y circulación de datos referentes a todos los aspectos de la vida de las personas[39]

Por tanto, analógicamente defiende la Constitución Colombiana el derecho a la protección de los niños y niñas en la utilización de internet, al hilo cabe mencionarse la Ley Estatutaria 1581 de 2012 en su artículo 7 señala:

38 COLOMBIA. Constitución Política de la República de Colombia. 2. ed. corregida de la Constitución Política de Colombia. *Gaceta Constitucional*, Bogotá, n. 116, 20 jul. de 1991. p. 3.

39 GALVIS CANO, Lucero. Protección de datos en Colombia, avances y retos. *Revista Lebret*, Bucaramanga, n. 4, p. 195-214, 2012. p. 199.

> Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública. Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás[40]

A lo que menciona la autora Galvis:

> ha significado un adelanto importante en torno a la protección de cualquier dato personal que sea administrado por entidades públicas y privadas, de acuerdo con los principios generales establecidos en la Constitución. Esta última ley estableció dos categorías de datos que requieren de protección especial y cuyo tratamiento está, en términos generales, prohibido: los llamados datos sensibles que son los que afectan la intimidad de las personas o cuyo uso indebido puede generar discriminación, y los datos personales de los niños, niñas y adolescentes. La norma designó la autoridad competente en términos de protección de datos y prohibió la transferencia de datos a países que no tengan un nivel adecuado de protección de los mismos[41]

Al hilo en la Sentencia del Tribunal Constitucional Colombiano[42] en sus II Consideraciones 3.4.1 manifiesta: "En reiterada jurisprudencia, citada anteriormente, la Corte ha establecido que uno de los límites admisibles del derecho constitucional a la privacidad es la existencia

40 COLOMBIA. Ley Estatutaria 1581, de 17 de octubre de 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013 Por la cual se dictan disposiciones generales para la protección de datos personales. *El Congreso de Colombia*, Colombia, 18 oct. 2012. p. 7-8.

41 GALVIS CANO, *op. cit.*, p. 199.

42 Tribunal Constitucional (Magistrado Responsable: González Cuervo, Mauricio) (Sentencia de Constitucionalidad 640/10) Referencia: D-7999. VIlex Online.

de un interés general en la divulgación de información personal y familiar, estos son de una circunstancia que les otorga relevancia. En este caso -diferente a otros en que la Corte también se ha plantado si existe un registro de la base de datos vulnerable a la intimidad, no es necesario demostrar que el sujeto del Registro aquí analizados y de interés público". Por lo tanto, solamente en Colombia serán de utilidad pública los datos de los niños o, niñas siempre en el ámbito académico o, de estudios. Por tanto, se priva la salida de los datos de los niños y las niñas o, adolescentes a terceros países, tales como la propia imagen.

¿Quiénes serán los responsables de los datos de los niños y las niñas en Colombia?

Como se menciona en el Decreto Número 1377 de 2013 en su artículo 12 manifiesta:

> El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7 de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos: 1. Que responda y respete el interés superior de los niños, niñas y adolescentes. 2. Que se asegure el respeto de sus derechos fundamentales. Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. Todo Responsable y Encargado involucrado en el Tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012 y el presente Decreto[43]

43 COLOMBIA. Ministerio de Comercio, Industria y Turismo. Decreto n° 1377, de 2013. *El Congreso de Colombia*, Colombia, 2013. p. 6.

Por lo cual, como se viene comentando la protección de los niños y las niñas, incluso los adolescentes, el responsable será el encargado del tratamiento de los datos y, siguiendo con el Decreto Número 1377 de 2013 en su artículo 13 párrafo 1 manifiesta: "Los Responsables del Tratamiento deberán desarrollar sus políticas para el Tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas".[44] Por tanto, serán responsables de los datos de los niños y niñas los encargados de los datos. Por otra parte, el Código civil colombiano en su artículo 34 menciona: "Llámase infante o niño, todo el que no ha cumplido siete años; impúber, el varón que no ha cumplido catorce años y la mujer que no ha cumplido doce; adulto, el que ha dejado de ser impúber; mayor de edad, o simplemente mayor, el que ha cumplido veintiún años, y menor de edad, o simplemente menor, el que no ha llegado a cumplirlos"[45] y, al mismo tiempo la Ley 27 de 1977[46] en su artículo 2 manifiesta: "En todos los casos en que la ley señale los 21 años como aptitud legal para ejecutar determinados actos jurídicos, o como condición para obtener la capacidad de ejercicio de los derechos civiles, se entenderá que se refiere a los mayores de 18 años". Por lo cual, en Colombia se adquiere la mayoría de edad a partir de los veintiún años, al mismo, tiempo cabe indicar que la patria potestad de los padres o, alguno de los padres ésta contemplado en el Código civil colombiano en su artículo 62 que señala: "Por los padres, quienes ejercerán conjuntamente la patria potestad sobre sus hijos menores de 21 años. Si falta uno de los padres la representación legal será ejercida por el otro".[47] Por lo

44 COLOMBIA. Ministerio de Comercio, Industria y Turismo. Decreto Número 1377, *op. cit.*, p. 6

45 COLOMBIA. Código Civil Colombiano. Ley 1116 de 2006. *Diario Oficial da Colombia*: Colombia, n. 46.494, 27 dic. 2006. p. 10.

46 COLOMBIA. Ley 27, del 4 de noviembre de 1977. *Diario Oficial da Colombia*: Colombia, n. 34.902, 5 nov. 1977. p. 7.

47 COLOMBIA. Código Civil Colombiano, *op. cit.*, p. 21.

que, estos serán los padres o, en su caso tutor representantes tanto del menor o, adolescentes quienes reclamen al encargado de los datos.

La Ley de Protección de Datos en Argentina sobre la protección de los menores y adolescentes

Como muy bien expresa la Ley de Protección de Datos de Argentina en su artículo 1:

> La presente ley tiene como objeto la protección integral de los datos personales en ficheros, registros, bancos de datos, otros medios técnicos de tratamiento de datos, sistemas públicos y privados destinados a dar información, para garantizar el derecho al honor. la intimidad de las personas[48]

Al hilo cabe mencionar la Constitución Argentina en su artículo 43 párrafo 3 que señala:

> Toda persona puede actuar de manera expedita y rápida para brindar protección, siempre que no exista otro recurso legal más adecuado, frente a cualquier acto de omisión de las autoridades públicas o de los particulares, que en la forma actual el daño inminente[49]

Por lo que, no se especifica sí son menores o, adolescentes y, siguiendo en su artículo 2 de la Ley de Protección de Datos de Argentina manifiesta:

48 ARGENTINA. Ley 25.326, de 4 de octubre de 2000, de Protección de Datos Personales de Argentina. p. 1.

49 ARGENTINA. *Constitución de la Nación Argentina*. Buenos Aires: Editorial Congreso de la Nación, 1994. p. 22.

> El fin de la presente ley se entiende por: Datos personales: Información de cualquier tipo referida a personas físicas o existencia ideal determinada o determinable. Datos sensibles: datos personales que revelen orígenes raciales y étnicos, opiniones políticas, creencias religiosas, filosóficas o morales, afiliación sindical e información sobre la salud de la vida sexual. Usuario de datos: Toda persona, pública o privada[50]

Al hilo los autores Bosque y Villan manifiestan: "si bien se aceptan condiciones de uso de diferentes servicios, en sectores vulnerables como en los niños, niñas y adolescentes el impacto a la privacidad de aún mayor".[51] Por otro lado, no incluye a los niños y las niñas y, adolescentes en la Ley de Protección de Datos de Argentina, sino que es una norma a efectos generales, siempre que se afecte entre otros datos como los raciales, étnicos y especialmente contra la información de la salud. Por otro lado, la Ley de Protección de Datos de Argentina señala en su artículo 11 párrafo 1º:

> Los responsables y las personas que intervienen en cualquier etapa del tratamiento de los datos personales están obligados al secreto profesional respecto a los mismos. Dicha obligación perdurará hasta que finalice su relación con el titular del fichero de datos[52]

Lo que analógicamente se aplicará también a los menores y, adolescentes hasta que se acabe la relación con respecto a los ficheros automatizados. Otro elemento, a destacar en la Ley de Protección de Datos de Argentina en su artículo 12 que manifiesta:

50 ARGENTINA. Ley 25.326, *op. cit.*, p. 1.

51 BOSQUE, Lia; VILLAN, Marco Antonio. Datos personales. Marketing digital y los derechos de los ciudadanos en América Latina. Estado de protección de los datos de los ciudadanos. *In*: CONGRESO INTERNACIONAL DE CIENCIAS SOCIALES, 6., 2018, Ciudad Autónoma de Buenos Aires. *Anales* [...]. Ciudad Autónoma de Buenos Aires: Editorial Universidad Argentina de la Empresa, 2018. p. 2.

52 ARGENTINA. Ley 25.326, *op. cit.*, p. 15.

> Está prohibido transferir datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no brinden niveles adecuados de protección La prohibición no regirá en las siguientes secuencias: La prohibición no regirá en las siguientes secuencias: a. Colaboración judicial internacional; b. Intercambio de datos de carácter médico, cuando así lo requiera el tratamiento de la persona afectada, investigación epidemiológica[53]

Por lo cual, el legislador argentino solamente se refiere a las enfermedades que puedan tener los menores, adolescentes incluso los adultos y, la mención indirecta a la pornografía infantil que puede ser investigada por la vía judicial.

Conclusiones

1. La Ley de protección de datos española de 2018, es muy expresiva respecto a la minoría y mayoría de edad de los menores y las menores de edad y, al mismo tiempo respecto a los adolescentes conjuntamente mediante la Agencia Española de Protección de Datos.
2. Respecto al Reglamento de Protección de Datos Europeo de 2016, limita la edad tanto a los niños y las niñas así, como a los adolescentes, por lo cual, simplemente es una recomendación, puesto que cada país puede adoptar la edad tanto de los niños y, las niñas, así como los adolescentes.
3. Atendiendo, a la legislación del Brasil se tiene que recurrir a su Código Civil, sobre lo que respecta a la minoría y mayoría de edad, puesto que la Ley de Protección de Datos de 2018, no aclara nada al respecto. Por otro lado, la ANPD intenta proteger a los menores y, adolescentes en caso que terceras personas atenten

53 ARGENTINA. Ley 25.326, *op. cit.*, p. 15.

contra el honor y la intimidad mediante su propia imagen, por lo que, que puede haber un nexo de unión según los tratados existentes con el Reglamento Europeo, en este caso contra la pornografía infantil y adolescente.

4. Por otro lado, la Ley Estatutaria 1581 de 2012, Ley de Protección de Datos en Colombia, es sumamente cerrada puesto que su aplicación sobre Protección de Datos es estrictamente para asuntos de índole académico de los niños, niñas y adolescentes. Por tanto, el legislador colombiano debería modificar la norma, puesto que estamos en un mundo globalizado por las nuevas tecnologías. Otro elemento a distinguir es la edad de los menores y adolescentes se tiene que recurrir al Código Civil Colombiano donde la mayoría de edad para ejercer sus derechos es de veintiún años, aunque analógicamente se refiere a los dieciocho años.
5. La Ley de Protección de datos de Argentina, es muy ambigua se refiere a todos los ciudadanos argentinos sin aclarar la edad, solamente se refiere el ámbito en materia de salud, sobre la transferencia de datos, al respecto esta norma es cerrada en cuanto a transferencia a terceros países. Por lo que, en mi opinión debería modificarla el legislador argentino.

Referencias

Autores

ALEJANDRA STUCHLIK, Silvia. *El Sistema de Protección Integral de Derechos de Niños, Niñas y Adolescentes de la Ciudad Autónoma de Buenos Aires. Buenos Aires*: Editorial Universidad de San Andrés, 2015.

BOSQUE, Lia; VILLAN, Marco Antonio. Datos personales. Marketing digital y los derechos de los ciudadanos en América Latina. Estado de protección de

los datos de los ciudadanos. *In*: CONGRESO INTERNACIONAL DE CIENCIAS SOCIALES, 6., 2018, Ciudad Autónoma de Buenos Aires. *Anales* [...]. Ciudad Autónoma de Buenos Aires: Editorial Universidad Argentina de la Empresa, 2018.

DÍAZ, Jesús. Redes sociales: incumplimiento sistemático de los controles técnicos versus vulneración reiterada de los derechos del menor. *Diario La Ley*, Madrid, n. 9326, 2018.

GALVIS CANO, Lucero. Protección de datos en Colombia, avances y retos. *Revista Lebret*, Bucaramanga, n. 4, p. 195-214, 2012.

LÓPEZ CALVO, José. *Comentarios al Reglamento Europeo de Protección de Datos*. Madrid: Editorial Jurídica Sepin, 2017.

REYES MÉNDEZ, Daniel. El acceso del menor a las redes sociales y el problema de su autentificación: la necesidad de una respuesta tecnológica. *Diario La Ley*, Madrid, n. 9335, 2019.

Constituciones

ARGENTINA. *Constitución de la Nación Argentina*. Buenos Aires: Editorial Congreso de la Nación, 1994.

BRASIL. Constituição Federal do Brasil. *Mini Código Saraiva*. 21. ed. São Paulo: Saraiva, 2015.

COLOMBIA. Constitución Política de la República de Colombia. Corregida de la Constitución Política de Colombia. *Gaceta Constitucional*, Colombia, n. 116, 20 jul. de 1991.

ESPAÑA. *Constitución Española*. Navarra: Aranzadi Cizur Menor, 2003.

Códigos Civiles

COLOMBIA. Código Civil Colombiano. Ley 1116 de 2006. *Diario Oficial da Colombia*: Colombia, n. 46.494, 27 dic. 2006. Disponible en: https://www.oas.org/dil/esp/codigo_civil_colombia.pdf. Acceso en: 17 dic. 2021.

BRASIL. Código Civil. *Mini Código Saraiva*. 21. ed. São Paulo: Saraiva, 2015.

Legislación española, europea e internacional

ARGENTINA. Ley 25.326, de 4 de octubre de 2000, de Protección de Datos Personales de Argentina. *Boletín Oficial de la República Argentina*: Argentina, 30 oct. 2000.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, p. 8, 9 jul. 2019.

COLOMBIA. Ley Estatutaria 1581, de 17 de octubre de 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013 Por la cual se dictan disposiciones generales para la protección de datos personales. *El Congreso de Colombia*, Colombia, p. 7-8, 18 oct. 2012.

COLOMBIA. Ley 27, del 4 de noviembre de 1977. *Diario Oficial da Colombia*: Colombia, n. 34.902, p. 7, 5 nov. 1977. Disponible en: Monograma.info/men/docs/pdf/ley_0027_1977. Acceso en: 8 jul. 2021.

COLOMBIA. Ministerio de Comercio, Industria y Turismo. Decreto n° 1377, de 2013. *El Congreso de Colombia*, Colombia, p. 6, 2013. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf. Acceso en: 8 jul. 2021.

ESPAÑA. Convención sobre los Derechos del Niño. I Disposiciones generales. Jefatura del Estado. *Boletín Oficial del Estado* (BOE), Madrid, n. 313. Disponible en: https://www.boe.es/boe/dias/1990/12/31/pdfs/A38897-38904.pdf. Acceso en: 5 dic. 2021.

ESPAÑA. Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil. Jefatura del Estado. *Boletín Oficial del Estado (BOE)*: Madrid, seción 1, n. 15, 16 ene. 1996. (Texto consolidado). Disponible en: www.boe.es. Acceso en: 5 dic. 2021.

ESPAÑA. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Jefatura del Estado. Boletín Oficial del Estado (BOE): Madrid, seción 1, n. 294, p. 17, 6 dez. 2018. (Legislación Consolidada). Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673. Acceso en: 5 dic. 2021

PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS. Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966. Entrada en vigor: 23 de marzo de 1976, de conformidad con el artículo 49 Lista de los Estados que han ratificado el pacto. [*S. l.: s. n.*], 1966. Disponible en: https://www.ohchr.org/sites/default/files/ccpr_SP.pdf. Acceso en: 6 jul. 2021.

UNIÓN EUROPEA. *Declaración Universal de Derechos Humanos*. [República del Paraguay]: Unión Europea, 1948. Adoptada y proclamada por la Asamblea General en su resolución 217 A (III), de 10 de diciembre de 1948. Disponible en: https://www.un.org/es/universal-declaration-human-rights/. Acceso en: 5 dic. 2021.

UNIÓN EUROPEA. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*: Luxemburgo, p. L.119/38, 2016.

Jurisprudencia

Tribunal Supremo (Sala Primera de lo Civil) (Ponente: O´Callaghan Muñoz, Xavier) (Sentencia 774/2006 de 13 de Julio). Rec. 2947/2000. LA LEY 70229/2006.

Audiencia Provincial de Cantabria (Sección 2ª) (Ponente: Arsuaga Cortázar, José) (Sentencia 24/2020 del 13 de enero), Rec. 805/2019. LA LEY 2099/2020.

Tribunal Constitucional (Magistrado Responsable: González Cuervo, Mauricio) (Sentencia de Constitucionalidad 640/10) Referencia: D-7999. VIlex Online.

A NECESSIDADE COMO ELEMENTO MODULADOR DA VALIDADE DOS ATOS DE TRATAMENTO DE DADOS PESSOAIS

Rafael da Silva Santana

Introdução

A vigente Lei Geral de Proteção de Dados (LGPD) representou a fagulha que tornou possível, e necessário, discutir temas de primeira ordem há muito arrefecidos. Alguns destes temas somente tangenciam o objeto primário da legislação, mas que, sem a adequação necessária das bases teóricas, colocam em risco a potencialidade esperada do novo diploma.

Muito se fala do conteúdo normativo da autodeterminação informativa e como ela afeta as disposições contratuais oriundas de instrumentos de massa, mas ainda carece de espaço uma abordagem que transponha o que o titular concordou sem desejar concordar, e passe a analisar os elementos que transformam em ilícito o tratamento de dados ainda que tenha havido prévio esboço de anuência.

Em razão da limitação técnica do capítulo, o problema a ser apresentado neste trabalho representa somente um corte do todo, mas que se mostra de muita valia na superação da crise em que o modelo contratual destacado está inserido.

Assim, não é a falibilidade da utilização do contrato de adesão o objeto desta pesquisa, mas o enfoque será conferido a um dos

elementos que podem representar a escolha jurídica de substituição do modelo vigente ou como adaptá-lo à sociedade de dados em que vivemos. Este elemento é a "necessidade".

O componente em destaque que, assim como muitos outros, foi importado da *General Data Protection Regulation*, equivalente normativo europeu da nossa LGPD, representa um dos pontos focais mais importantes da regulação, na medida em que restringe o tratamento de dados ao mínimo necessário à obtenção dos resultados propostos. Deste modo, se torna salutar entender como este limite impacta no ato de tratamento de dados e quais as repercussões jurídicas da sua não observância.

Com efeito, na segunda seção será analisada a influência da inclusão da necessidade como um dos princípios norteadores das atividades de tratamento de dados, bem como serão exploradas as demais acepções que a necessidade já desempenha no nosso ordenamento e, ao final, investigar-se-á, de fato, dentro do sistema de proteção de dados pessoais, se este instituto representa um princípio, outra espécie normativa ou se consegue se apresentar, concomitantemente, de forma multifacetada.

Na terceira seção, serão abordadas as repercussões jurídicas de se admitir que a necessidade exerce uma influência normativa concreta sobre a análise de licitude dos atos de tratamento de dados, notadamente sobre o prisma da validade, bem como investigar como este elemento contribui para uma adequada compreensão do controle destes atos jurídicos, para além do contrato de adesão.

Não se trata, portanto, de trabalho exaustivo, mas que se propõe a iniciar discussão sobre a adequação dos suportes legais à proteção de dados pessoais por meio de um dos seus institutos mais relevantes, com vistas a buscar interpretação que consagre a maior eficiência protetiva esperada da LGPD.

Feições da necessidade no ordenamento jurídico brasileiro

De início, se revela oportuno destacar que o estudo da necessidade ora proposto não se relaciona com uma característica de um estado pessoal do sujeito. Não se compreenderá o instituto conforme descrito no estado de perigo, ou na lesão, ambos do Direito Civil, ou o próprio estado de necessidade, previsto no Código Penal, ou ainda a necessidade pública de matriz constitucional, e tantos outros correlatos na legislação extravagante.[1]

Em verdade, ao abordar a necessidade, está a se investigar ontologicamente o instituto, cujas bases vão além de uma mera adjetivação de uma situação de fato.

Há muito a doutrina estuda a necessidade enquanto elemento de fundamentação e estruturação normativa.

Aprioristicamente tratada como conteúdo do postulado normativo da proporcionalidade, é amplamente conceituada como o exame da existência de meios alternativos àquele inicialmente escolhido pelo legislador ou governante, que satisfaça a obrigação imposta por um meio menos gravoso ou menos oneroso, contudo igualmente eficiente.

> Nesse sentido, o exame da necessidade envolve duas etapas de investigação: em primeiro lugar, o exame da igualdade de adequação dos meios, para verificar se os meios alternativos promovem igualmente o fim; em segundo lugar, o exame do meio menos restritivo, para examinar se os meios alternativos restringem em menor medida os direitos fundamentais colateralmente afetados.[2]

1 Tais dispositivos estão previstos, respectivamente, nos artigos 156 e 157, ambos do Código Civil, no artigo 24 do Código Penal e no artigo 5°, XXIV, da Constituição Federal.

2 ÁVILA, Humberto. *Teoria dos princípios*: da definição à aplicação dos princípios jurídicos. 18. ed. rev e atual. São Paulo: Malheiros, 2018. p. 217.

Em sentido próximo, Robert Alexy também inclui a necessidade como elemento da máxima da proporcionalidade, dispondo que o conteúdo daquela se traduz em um "mandamento do meio menos gravoso"[3] na aplicação e materialização de direitos.

Assim, como arremata Luiz Guilherme Marinoni, o conteúdo da necessidade sob este prisma se relaciona intrinsecamente com aspectos hermenêuticos voltados à aplicação de normas jurídicas.

Ainda que tenha adotado classificação peculiar, inserindo o postulado normativo como uma categoria de metanorma jurídica, o jurista em comento ensina que estas se situam em um plano acima de outras normas, cuja finalidade é fundamentar a "aplicação de determinada alternativa de aplicação normativa em detrimento de outra", donde inclui a proporcionalidade, e, portanto, a necessidade, como elemento desta classificação.[4]

Destarte, o campo fértil onde floresceu o estudo da necessidade foi no ramo constitucional, exercendo relação mutualista com o postulado normativo da proporcionalidade, sendo um dos três exames necessários para aferir a aplicação proporcional de normas colidentes.[5]

Com a promulgação da LGPD, o instituto em voga ganhou novas cores. A necessidade passou a figurar expressamente no rol do artigo 6º do diploma em comento,[6] sendo atribuído o status de princípio, cujo escopo é impor limite ao tratamento de dados.

Assim, se tornou obrigação daqueles que irão operar com os dados que se valham de uma exata proporção entre o que será tratado e o

3 ALEXY, Robert. *Teoria dos direitos fundamentais*. São Paulo: Malheiros, 2008. p. 117.

4 MARINONI, Luiz Guilherme. *Novo curso de processo civil*: teoria do processo civil. São Paulo: Revista dos Tribunais, 2017. v. 1, p. 65-66.

5 ALEXY, *op. cit.*, p. 117.

6 Art. 6° da Lei n° 13.709/2018: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; [...]".

resultado proposto, guardando a máxima eficiência de modo que se opere com a menor quantidade de dados possível.

Rita Peixoto Ferreira Blum defende que esta norma, fruto do direito à segurança de origem consumerista, além da necessária limitação já mencionada, implica em uma preferência pela adoção de dados anonimizados em relação aos dados com os quais seja possível identificar o titular.[7]

No mesmo sentido, Paulo Marcos Rodrigues Brancher, Fabio Ferreira Kujawski e Ana Carolina Heringer Costa Castellano lecionam que:

> Assim, a partir de uma interpretação teleológica da LGPD, percebe-se que dados pessoais só devem ser processados quando não houver outros meios razoáveis de realizar a atividade e, quando possível, é preferível que se utilizem dados anominizados. É responsabilidade do controlador verificar a quantidade de dados que é necessária para determinado fim e assegurar que nenhuma informação irrelevante será coletada.[8]

Ao tomar como ponto de partida o dispositivo legal da LGPD em comento e as lições doutrinárias retro, é possível formular alguns relevantes questionamentos sobre a exata interpretação do instituto, dentre os quais serão ora sobrelevados: 1. O conteúdo do artigo 6º, inciso III, da LGPD, se trata verdadeiramente de um princípio?; 2. A necessidade abordada na LGPD tem aplicação semelhante à necessidade enquanto conteúdo da proporcionalidade?

7 BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor*. São Paulo: Almedina, 2018.

8 BRANCHER, Paulo Marcos Rodrigues; KUJAWSKI, Fabio Ferreira; CASTELLANO, Ana Carolina Heringer Costa. Princípios Gerais de Proteção de Dados Pessoais: uma análise dos princípios elencados no art. 6° da Lei 13.709/2018 (LGPD). *In*: BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Cláudia (org.). *Proteção de dados pessoais no Brasil*: uma nova visão a partir da Lei 13.709/2018. Belo Horizonte: Fórum, 2019. p. 72-73.

A resposta ao primeiro tende a ser negativa e ao segundo, taxativamente negativa.

No primeiro caso, seria possível, com algum esforço, sustentar que tal dispositivo carrega consigo uma dupla feição, tanto de regra como de princípio. Dworkin relata que, por vezes, a diferença entre estes tipos normativos é tão tênue que é possível dizer que o que os separa é um aspecto meramente formal,[9] assim, ainda que possa causar certa estranheza, não soaria teratológico sustentar um eventual princípio da necessidade tal qual esposado na Lei.

Todavia, a interpretação teleológica da norma carrega tamanha carga decisória que parece de impossível convivência no sistema com outra norma que flexibilize este comando. Se analisada a Lei de forma holística, a pecha da ilegalidade acompanharia o ato de tratamento que fosse realizado coletando dados desvinculados da finalidade proposta, tal qual prevê o artigo 40 da LGPD.

Nesse sentido, seja quanto ao grau de generalidade,[10] seja quanto à acepção ontológica[11] ou ainda sob o critério teleológico,[12] a norma ali insculpida se liga à concepção corrente de norma-regra e não norma-princípio, justamente porque, de acordo com a dinâmica da LGPD e demais leis extravagantes menos específicas, a exemplo do Código de Defesa do Consumidor (CDC), o sistema não se adequa com norma

9 DWORKIN, Ronald. *Levando os direitos a sério*. Tradução de: Nelson Boeira. São Paulo: WWF Martins Fontes, 2010. p. 44-45.

10 Robert Alexy atribui alguns critérios para diferenciar regras de princípios. Com base no critério da generalidade, os princípios são normas com grau de generalidade relativamente alto, enquanto o grau de generalidade das regras é relativamente baixo.

11 Com base neste critério, Alexy ensina que princípios e regras são diferenciados também com base no fato de serem razões para regras ou serem eles mesmos regras, ou, ainda, no fato de serem normas de argumentação ou normas de comportamento.

12 Por esta acepção, os princípios são mandamentos de otimização, ou seja, que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes, podendo ser satisfeitos em graus variados, enquanto as regras são normas que devem ser sempre satisfeitas em sua integralidade ou então não serão satisfeitas.

que mitigue esta regra, de modo que ela é aplicada no modelo tudo-ou-nada e não no sistema de graus de incidência.

Ainda que não tenha sido o objeto detido da análise, Rita Peixoto Ferreira Blum também descreve a norma em destaque como do tipo norma-regra.[13]

Destarte, a ideia de que o controlador e o operador que irão realizar o tratamento de dados devem guardar uma justa relação entre o material examinado e o fim proposto pela investigação não se trata de uma mera faculdade ou comando passível de ser sopesado com outras normas no ordenamento. É, em verdade, regra cogente e aplicável a todo aquele que se proponha a realizar tratamento de dados. Nesse sentido:

> A máxima da proporcionalidade é com frequência denominada 'princípio da proporcionalidade'. Nesse caso, no entanto, não se trata de um princípio no sentido aqui empregado. A adequação, a necessidade e a proporcionalidade em sentido estrito não são sopesadas contra algo. Não se pode dizer que elas às vezes tenham precedência e às vezes não. O que se indaga é, na verdade, se as máximas parciais foram satisfeitas ou não, e sua não-satisfação tem como consequência uma ilegalidade. As três máximas parciais devem ser, portanto, consideradas como regras.[14]

De mais a mais, a negativa ao segundo questionamento tem origens hermenêuticas e que carecem de análise igualmente detida.

Em um sistema harmônico e complementar, não é salutar que conceitos jurídicos tenham significados diversos e que não carreguem consigo, ao menos, linha tangente que os aproxime.

13 A autora o faz justamente quando vai descrever o que vem a ser o princípio da necessidade ao falar que: "Necessidade – limitação do uso de dados pessoais que permitam identificar o mínimo necessário, de forma a adotar no seu tratamento sempre que possível a técnica de anonimato, retirando o vínculo da informação atinente à identidade do consumidor a que se refere. Esta regra, de certa forma, tem relação com o direito básico do consumidor à segurança". BLUM, *op. cit.*, p. 160-161.

14 ALEXY, *op. cit.*, p. 117.

Em outras palavras, se já é prejudicial ao sistema jurídico que um signo tenha mais de um significado, ainda que próximos, se revela contraproducente, para dizer o mínimo, quando um símbolo é traduzido de formas absolutamente isoladas.

Pietro Perlingieri, acerca do caráter problemático da variabilidade dos significados das palavras e das proposições linguísticas, leciona que:

> O equívoco maior que se aninha no brocardo *in claris non fit interpretatio* é o pressuposto no qual se funda, ou seja, a 'clareza' do texto. A qualificação de 'clara', reservada a uma palavra, ainda mais uma proposição linguística, é somente relativa, sobretudo quando a mensagem tem, em relação ao momento da sua recepção por parte do destinatário, uma diversidade temporal. As palavras assumem no tempo significados mesmo qualitativamente diversos, segundo a cultura e a sensibilidade do destinatário. O 'significado próprio das palavras', de acordo com a lei, frequentemente não corresponde ao significado comum e, por outro lado, cada vez mais se acentuam as diferenças de uso das palavras por parte do legislador, quando isso não é nem mesmo almejado. [...][15]

Conforme visto, o conceito predominante de necessidade, enquanto elemento da proporcionalidade, se relaciona com alternativas eficientes que são encontradas na aplicação prática de determinada norma posta, seja pelo legislativo seja pelo executivo. Já a necessidade, para a LGPD, se relaciona com a utilização mínima dos dados pessoais para alcançar determinado fim. Assim temos um signo com duas traduções evidentemente distintas.

15 PERLINGIERI, Pietro. *Perfis do direito civil*. Tradução de: Maria Cristina De Cicco. Rio de Janeiro: Renovar, 2002. p. 73-74.

Melhor teria andado a legislação se tivesse se valido de significação próxima daquela utilizada na GDPR, qual seja, *data minimisation*.[16]

Isso porque o que pretende a Lei é que a informação que não será utilizada, ou seja, aquela que extrapola ao mínimo necessário destinada ao alcance da finalidade pretendida, não possa ser nem coletada nem tratada.[17]

Assim, na sistemática europeia, a opção legislativa foi pela criação de um novo símbolo legal que caracterize a ideia de utilização mínima dos dados pessoais coletados afetos a uma finalidade.[18] Na contramão, o ordenamento pátrio se valeu de uma apropriação terminológica ineficiente e imprópria, atraindo um ponto de divergência semântica para o interior do sistema.

Deste modo, se a escolha pela não adoção de um conceito próprio é duvidosa, ao menos dever-se-ia ter sido empregado conceito jurídico compatível com o signo pretendido. Com efeito, há no sistema conceito jurídico que exprime uma ideia correlata com o quanto previsto

16 ANTIGNAC, Thibaud; SANDS, David; SCHNEIDER, Gerardo. Data-minimisation: a language-based approach. *In*: INTERNATIONAL CONFERENCE ON ICT SYSTEMS SECURITY AND PRIVACY PROTECTION – IFIP SEC'17, 32., 2017. *Annals* [...]. [*S. l.*]: IFIP, 2017.

17 A íntegra do texto: "*According to the article 5 of the EU General Data Protection Regulation proposal 'Personal data must be [...] limited to what is necessary in relation to the purposes for which they are processed'. This principle is called data minimisation. From a software perspective, data minimisation requires that the input data not semantically used by a program should neither be collected nor processed. The data processor could be seen in this context as to be the adversary (or attacker), as she knows all the information available after the input is collected (before the program execution) and thus can exploit the inputs*". Em tradução livre, significa: "De acordo com o artigo 5 da proposta de Regulamento Geral de Proteção de Dados da União Europeia 'Os dados pessoais devem ser [...] limitados ao necessário em relação aos fins para os quais são processados'. Este princípio é chamado de minimização de dados. De uma perspectiva de software, a minimização de dados requer que os dados que não sejam necessários à finalidade prevista não sejam coletados nem processados. O operador de dados pode ser visto neste contexto como o adversário (ou atacante), pois ele conhece todas as informações disponíveis depois que a coleta é feita (antes da execução do programa) e, ainda assim, explora as informações".

18 Tal conceito continua previsto no artigo 5°, alínea c, da GDPR, cujo conceito é: "quate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')". Ver em: https://gdpr-info.eu/art-5-gdpr/.

no dispositivo legal em comento, que é o da proporcionalidade em sentido estrito, outro dos componentes do postulado normativo da proporcionalidade, que se alinha perfeitamente com a ideia de interconexão dos princípios previstos no artigo 6º da LGPD.[19]

De acordo com a lição de Humberto Ávila, a proporcionalidade em sentido estrito é justamente a última aferição de encaixe entre a finalidade e a adequação,[20] assim como a necessidade, para a LGPD, é o exame de validade entre a finalidade e a adequação, ambos presentes no indigitado artigo 6º. Este conceito se relaciona de forma muito mais sinérgica com a pretensão teleológica da norma, ainda que se reconheça uma insuficiência no que tange a exigência da utilização do material mínimo.

Diante do exposto, não há só uma má interpretação da espécie normativa que identifica a necessidade como um princípio, visto que exerce, majoritariamente, força de regra, mas há, também, um problema de ordem hermenêutica, atraindo significado divergente e não sinérgico para um único instituto jurídico.

A necessidade como elemento modulador da validade dos atos de tratamento de dados pessoais

Em consonância com a posição adotada neste capítulo, que passa a ser premissa para este tópico, a necessidade mencionada no artigo 6º, inciso III, da LGPD, será entendida como equivalente normativo da *data minimisation* previsto na *General Data Protection Regulation*, bem

19 OLIVEIRA, Marco Aurélio Bellize; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei nº 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 53-84.

20 ÁVILA, *op. cit.*, p. 210.

como, ao revés da aderência à nomenclatura adotada nos regramentos nacional e internacional, ser tratada como uma norma-regra.

Ao adotar estes marcos, é possível sugerir que a utilização mínima dos dados necessários é um comando destinado indistintamente a todos que realizem tratamento de dados pessoais e, *mutatis mutandis*, que o armazenamento e o uso de elementos que extrapolem o extremamente necessário ao alcance da finalidade proposta se revelam atos contrários ao comando normativo.

Com efeito, o ordenamento passa a admitir, ainda que implicitamente, uma regra cogente, cujo destinatário imediato é o ordenador ou o operador dos dados, de tal modo que disposição em contrário na generalidade dos instrumentos contratuais seria eivada de nulidade.[21]

Em legislações tipicamente protetivas, a exemplo do CDC, há regras que se amoldam ao modelo ora proposto, como é o caso das hipóteses não exaustivas previstas no artigo 51[22] da Lei em comento. A Lei

21 Diz-se generalidade posto que, ao tempo em que este capítulo está sendo escrito, o autor desconhece publicação que tenha enfrentado a possível coexistência de um direito irrestrito de cessão de direito de uso de dados pessoais com a regra da necessidade.

22 Art. 51 da Lei nº 8.078/90. Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que: I – impossibilitem, exonerem ou atenuem a responsabilidade do fornecedor por vícios de qualquer natureza dos produtos e serviços ou impliquem renúncia ou disposição de direitos. Nas relações de consumo entre o fornecedor e o consumidor pessoa jurídica, a indenização poderá ser limitada, em situações justificáveis; II – subtraiam ao consumidor a opção de reembolso da quantia já paga, nos casos previstos neste código; III – transfiram responsabilidades a terceiros; IV – estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a eqüidade; V – (Vetado); VI – estabeleçam inversão do ônus da prova em prejuízo do consumidor; VII – determinem a utilização compulsória de arbitragem; VIII – imponham representante para concluir ou realizar outro negócio jurídico pelo consumidor; IX – deixem ao fornecedor a opção de concluir ou não o contrato, embora obrigando o consumidor; X – permitam ao fornecedor, direta ou indiretamente, variação do preço de maneira unilateral; XI – autorizem o fornecedor a cancelar o contrato unilateralmente, sem que igual direito seja conferido ao consumidor; XII – obriguem o consumidor a ressarcir os custos de cobrança de sua obrigação, sem que igual direito lhe seja conferido contra o fornecedor; XIII – autorizem o fornecedor a modificar unilateralmente o conteúdo ou a qualidade do contrato, após sua celebração; XIV – infrinjam ou possibilitem a violação de normas ambientais; XV – estejam em desacordo com o sistema de proteção ao consumidor; XVI – possibilitem a renúncia do direito

do Marco Civil da Internet, em seu artigo 16, II, também se vale do princípio da *data minimisation* para tachar eventuais abusos de armazenamento de dados de ilícitos.[23]

Assim, ao se valer da regra em voga, restou inserido no ordenamento jurídico brasileiro um limite ao tratamento de dados pessoais, que se traduz em um controle de conteúdo, ancorado em princípios maiores tais quais o da dignidade da pessoa humana, da boa-fé e da probidade.[24]

Deste modo, a análise do elemento da necessidade atua como um vetor racional e inerente a cada ato de tratamento, atraindo a incidência obrigatória de controle de legalidade simultânea com a operação desenvolvida.

O que se pretende afirmar é que o armazenamento e o tratamento de dados em espécie que exacerbem a exata adequação entre quantidade/qualidade e a finalidade proposta já é, *de per si*, ilícita.

Despicienda, portanto, qualquer manifestação judicial neste sentido, ou, se houver, os efeitos dela decorrentes serão meramente declaratórios, podendo vir a ser sentenciada a nulidade ainda de forma

de indenização por benfeitorias necessárias. § 1° Presume-se exagerada, entre outros casos, a vantagem que: I – ofende os princípios fundamentais do sistema jurídico a que pertence; II – restringe direitos ou obrigações fundamentais inerentes à natureza do contrato, de tal modo a ameaçar seu objeto ou equilíbrio contratual; III – se mostra excessivamente onerosa para o consumidor, considerando-se a natureza e conteúdo do contrato, o interesse das partes e outras circunstâncias peculiares ao caso. § 2° A nulidade de uma cláusula contratual abusiva não invalida o contrato, exceto quando de sua ausência, apesar dos esforços de integração, decorrer ônus excessivo a qualquer das partes. § 3° (Vetado). § 4° É facultado a qualquer consumidor ou entidade que o represente requerer ao Ministério Público que ajuíze a competente ação para ser declarada a nulidade de cláusula contratual que contrarie o disposto neste código ou de qualquer forma não assegure o justo equilíbrio entre direitos e obrigações das partes.

23 Art. 16 da Lei n° 12.965/2014. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: [...] II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

24 MARQUES, Cláudia Lima. *Comentários ao código de defesa do consumidor*. São Paulo: Thomson Reuters Brasil, 2019. p. 1315.

acessória à matéria principal, de ofício ou mediante provocação, com efeitos *ex tunc*.[25]

Oportuno destacar que está a se falar repetidas vezes em validade, uma vez que, ancorado na doutrina de Marcos Bernardes de Mello, o problema a ser enfrentado se relaciona intrinsecamente com um dos elementos componentes do ato jurídico atrelado à legitimação do agente para realizar tal tratamento.

Assim, não há dúvidas de que há agente (operador ou controlador), objeto (dados pessoais cedidos ou coletados) ou forma, tampouco inexistem, na análise da necessidade, outros elementos que condicionem e imponham termo aos atos de tratamento de dados, mas, em realidade, o que está a ser investigado ao estudar a *data minimisation* é uma especificidade do elemento objeto, qual seja, a licitude ou seu antônimo.

Rodrigo Rebouças, ao tratar sobre contratos eletrônicos, enfrentou questão semelhante e, partindo da premissa que os requisitos do plano da validade são qualificadores dos requisitos de existência, atribui ao agente o ônus de, além da capacidade, operar com legitimação.[26]

Assim, a legitimação, que tem conteúdo diverso da capacidade, consiste "em uma posição do sujeito relativamente ao objeto do direito, que se traduz, em geral, na titularidade do direito, posição esta que tem como conteúdo o poder de disposição, bem assim o poder de aquisição. [...]".[27]

25 Marcos Bernardes de Mello leciona que, quanto aos atos nulos, "a sua desconstituição somente será necessária quando: (i) há dúvida em relação à nulidade, impondo-se o seu conhecimento pelo juiz, ou, (ii) necessariamente quando há registro público do ato jurídico, de que são exemplos o casamento e o acordo de transmissão de bem imóvel. Caso seja evidente, indiscutível a nulidade e não haja registro público do ato jurídico, é despicienda sua desconstituição judicial, uma vez que esta se refere, tão somente, ao ato em si, para expulsá-lo do mundo jurídico, pois não há efeitos a desfazer". MELLO, Marcos Bernardes. *Teoria do fato jurídico*: plano da validade. São Paulo: Saraiva, 2019, p. 50.

26 REBOUÇAS, Rodrigo Fernandes. *Contratos eletrônicos*: formação e validade. São Paulo: Almedina, 2018. p. 82.

27 MELLO, *op. cit.*, p. 76.

Com efeito, ao adotar a *data minimisation* como uma norma-regra cogente de aplicação imediata a todos os atos de tratamentos de dados, cujo ato jurídico praticado em sentido contrário importará na declaração de nulidade destes, é coerente afirmar que a necessidade tal qual prevista na LGPD é um elemento modulador da validade dos atos de tratamento previstos naquele diploma.

Como consequência deste exame, algumas conclusões são decorrentes e alcançam as searas extracontratual e contratual.

Com relação ao primeiro campo, ao tomar como premissa que a utilização de dados deve ser pautada na utilização da menor quantidade de dados possíveis, se mostra assertivo afirmar que a *data minimisation* afeta a esfera jurídica do controlador e do operador de dados de uma forma direta, impondo limitações ao tratamento de dados, mas também veda o "reter tudo", ou alinhado com o quanto disposto na GDPR, restringe o armazenamento de dados desvinculados à finalidade proposta (*storage limitation)*.[28]

> (Storage limitation) That is, we can never collect or store data that we will not subsequently use for a legitimate purpose (1c). Moreover, not only must we delete that data once it has outlived its purpose, with some exceptions, perpetual storage is prohibited outright (1e).[29]

28 O artigo 5°, alínea e, da GDPR assim prevê: "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')".

29 ARFELT, Emma; BASIN, David; DEBOIS, Soren. Monitoring the GDPR. *In*: EUROPEAN SYMPOSIUM ON RESEARCH IN COMPUTER SECURITY, 24., 2019, Luxembourg. ANNALS [...]. Luxembourg: Springer, 2019.

Assim, em uma leitura apressada, poder-se-ia admitir que o "princípio da necessidade" tem como efeito a obrigação de não processar o tratamento de dados além dos necessários a uma finalidade, atuando de forma ativa.

Contudo, de acordo com a própria redação da LGPD, em interpretação conjunta do artigo 5º, inciso X,[30] que dispõe que tratar dados também é armazená-los, com o conteúdo do artigo 6º, inciso III do diploma em voga, é de todo perceptível que o dito princípio também dispõe de acepção negativa, que é a da vedação ao armazenamento de material desnecessário à finalidade indicada no momento da coleta.

Deste modo, a restrição, quando ativa, se relaciona com o uso efetivo dos dados coletados, enquanto a barreira omissiva, aqui designada pela limitação ao armazenamento, está vinculada à latência. Ambos ilícitos, desde que não observadas as regras da menor utilização e da vinculação à finalidade específica.

Em linha simétrica ao quanto dissertado, Rony Vainzof leciona[31] que limitação ao armazenamento "significa que o *controller* deve limitar a coleta de dados pessoais ao que é diretamente relevante e necessário para atingir um propósito específico, retendo tais dados apenas pelo tempo que for necessário para cumprir este propósito". Em arremate, conclui que o reter tudo, indistintamente e desvinculado ao fim proposto, possivelmente será tido como ilícito.

Neste sentido, e de acordo com as outras premissas já adotadas neste trabalho, atos de coleta de dados em massa, tal qual o famoso

30 Art. 5°. Para os fins desta Lei, considera-se: [...] X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; [...]"

31 VAINZOF, Rony. Dados pessoais, tratamento e princípios. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *Comentários ao gdpr*: regulamento geral de proteção de dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 61-62.

caso do *FaceApp*,[32] independentemente de qualquer ação comissiva futura, a simples coleta de dados além dos mínimos já representa um ilícito, ao menos na seara civil.

Destarte, e esta é uma das possíveis conclusões que se extrai do processo de dissecar o "princípio da necessidade" e reconhecer a existência desta característica omissiva desta regra, eventual ilícito civil não decorre somente da síntese do tratamento comissivo de dados, ou seja, após a transformação de dados em informação. O marco inicial do fato lesivo é a própria captura e armazenamento de dados alheios à finalidade proposta ao titular, ainda que permaneçam perenemente em estado de latência.

Sob o prisma contratual, dinâmica similar se impõe.

Uma vez assimilada a ideia de que o ato de realizar o tratamento de dados desnecessários ou desvinculados ao propósito indicado se traduz em infração à norma-regra cogente, a autorização requerida para que se realize coleta indiscriminada de dados pessoais, é de todo ilegal.

A um, porque os comandos normativos já destacados são claros quanto à relação íntima que o tratamento tem com a finalidade indicada, cuja interpretação semântica pressupõe um objetivo específico, e não algo genericamente concebido.

A dois, o exame objetivo da "necessidade" não fica limitado ao fim específico narrado, mas que se relaciona intimamente com a própria atividade empresarial do controlador. Assim, ainda que um escritório de advocacia indique que necessitará que aqueles que recorrem a seus serviços precisem indicar seu tipo sanguíneo para que os clientes possam ser alertados em futuras campanhas de doação, a atividade técnica desenvolvida naquele ambiente se distancia da finalidade narrada. Deste modo, ainda que haja uma relação íntima entre a informação requerida e a finalidade indicada, a inexistência de liame entre o fim

32 Fato amplamente noticiado. Tem-se como exemplo o seguinte canal. Ver em https://canaltech.com.br/apps/faceapp-rastreia-navegacao-e-compartilha-dados-do-usuario-com-terceiros-144235/.

narrado e a atividade intelectual finalística desenvolvida pelo escritório desautoriza tal tratamento.

Muitos outros exemplos práticos poderiam surgir da aplicação das regras ora trabalhadas, mas, em plano abstrato, o que carece de atenção dos operadores do Direito é o fato de os amplos e imprecisos contratos de adesão, hodiernamente apresentados como termos de uso no mercado de dados, conterem cláusulas de coleta igualmente inespecíficas.

Para além das críticas comumente ofertadas ao modelo contratual *suso* aludido, as quais são endossadas por este trabalho,[33] a inserção de cláusula em termos de uso que exija, para a utilização do serviço prestado, o tratamento de dados que extrapolem o quanto necessário à finalidade pretendida, já é elemento mais do que suficiente para que o ilícito esteja configurado.

Nesse sentido, em eventuais demandas judiciais, além da finalidade indicada no termo de uso, é necessário que o julgador se debruce especificamente sobre a relação existente entre a natureza do serviço proposto e a essencialidade da informação colhida, tal qual o exemplo do escritório de advocacia acima ofertado.

Não paira sobre o titular o ônus de provar a destinação dos seus dados, assim como ao controlador não cabe alegar anuência do usuário. Neste aspecto, a anuência é irrelevante para a aferição do ilícito.

O ônus de provar que a finalidade para qual os dados do titular estão sendo tratados é condizente com o serviço prestado e se relaciona intimamente com a atividade-fim da empresa controladora, é exclusivo desta.

Assim, é mantida incólume a máxima de que os atos nulos não se convalidam,[34] cuja asserção ratifica a natureza jurídica da invalidade que acomete a não observância da *data minimisation*.

33 Vide crítica aludida em: MARQUES, Cláudia Lima. *Contratos no código de defesa do consumidor*: o novo regime das relações contratuais. São Paulo: Thomson Reuters Brasil, 2019.

34 Assim está disposto no art. 169 do Código Civil. O negócio jurídico nulo não é suscetível de confirmação, nem convalesce pelo decurso do tempo.

Igualmente interessante é a abrangência da gama de proteção que decorre da acepção de regra cogente imputada ao "princípio da necessidade".

Ao assumir que não existem graus variados de aderência entre o tratamento de dados e a finalidade elencada, como decorreria se interpretada como princípio, mas como uma relação direta e imediata entre finalidade e adequação, aproximando-a de uma regra analítica da proporcionalidade em sentido estrito, ainda que conste no termo de uso que o aceite àquelas condições é individual, a infração contratual a uma norma de observância obrigatória amplia sobremaneira o espectro de proteção a ela garantida.

Isso porque quando se trata de nulidade de pleno direito, cominado com o fato de ser indeterminado o número de pessoas passíveis de serem atingidas por tal ilegalidade, a nulidade não alcança somente uma relação contratual, mas toda uma coletividade.

> A nulidade *de pleno iure* não alcança, apenas, determinados interesses pessoais e privados, certas pessoas interessadas, direta ou indiretamente, no ato jurídico e suas consequências; afeta a todos. Por isso, a decisão que desconstitui o ato jurídico nulo tem eficácia *erga omnes.* Por essa razão, se há vários *interessados* na decretação da nulidade, qualquer deles estará legitimado para argui-la, e a desconstituição do ato nulo terá eficácia em relação a todos.[35]

Destarte, assumir que o conteúdo do indigitado "princípio da necessidade" desempenha papel central na aferição da validade do tratamento de dados é avançar em sentido da maior eficiência normativa, conferindo harmonia ao sistema, conjugando as acepções atômicas ora trabalhadas com preceitos específicos e nucleares da LGPD, a exemplo da *accountability*.

35 MELLO, *op. cit.*, p. 303-304.

Considerações finais

Por tudo quanto exposto, a despeito do *nomen iuris* conferido pela LGPD, a aplicação do que se convencionou chamar de princípio da necessidade se distancia do modelo de graus de incidência e se materializa no ordenamento enquanto regra, de modo tal que seria questionável a coexistência com outra regra em sentido contrário do indigitado "princípio" no mesmo sistema, sem que representasse uma exceção a ele.

Em verdade, conforme amplamente demonstrado, é salutar que a interpretação ora conferida à norma em destaque prevaleça. Seja enquanto elemento de harmonização do sistema, seja enquanto componente hermenêutico que compatibilize a maior eficiência viabilizando alcançar as potencialidades pretendidas pela legislação em comento, a compreensão da necessidade como regra cogente, e, portanto, elemento modulador da validade dos atos de tratamento de dados pessoais, é peça central no arcabouço protetivo do titular, que é a finalidade maior da LGPD.

Dessarte, adotadas estas premissas como ponto de partida, é facilitada a efetiva proteção do meio digital, já que a responsabilidade dos agentes de tratamento começa em momento anterior à coleta, qual seja, o da própria confecção da ficha cadastral do serviço a ser posto em circulação, já que a mera requisição de informações incompatíveis com a finalidade proposta pelo serviço, *de per si*, representa um ilícito.

Mas não só. Há muito se discute a influência positiva que as ações coletivas podem exercer na sociedade atual, notadamente nos campos em que os contratos de massa reinam. Não é à toa que está em discussão um Código Brasileiro de Processo Coletivo. Neste viés, a LGPD pode dar um salto de importância e abrangência se a interpretação conferida aos institutos nela previstos passem a ser vistos não por um modelo atomizado e de difícil penetração, mas, como efetivamente deve ser, uma legislação voltada a proteger os milhões de titulares, estes incomensuráveis.

Em recuperação ao preâmbulo do presente trabalho, este capítulo tem como finalidade representar um ponto de partida para discussões outras que extrapolam o limite material da via eleita, mas que, de certa maneira, perscrutam uma fenda em meio ao imobilismo que uma inadequada nomenclatura poderia causar.

Referências

ALEXY, Robert. *Teoria dos direitos fundamentais.* São Paulo: Malheiros, 2008.

ANTIGNAC, Thibaud; SANDS, David; SCHNEIDER, Gerardo. *Data-minimisation*: a language-based approach. *In*: INTERNATIONAL CONFERENCE ON ICT SYSTEMS SECURITY AND PRIVACY PROTECTION – IFIP SEC'17, 32., 2017. *Annals* [...]. [*S. l.*]: IFIP, 2017. Disponível em: http://www.cse.chalmers.se/~gersch/ifip-sec17-data_min.pdf. Acesso em: 30 nov. 2020.

ARFELT, Emma; BASIN, David; DEBOIS, Soren. Monitoring the GDPR. *In*: EUROPEAN SYMPOSIUM ON RESEARCH IN COMPUTER SECURITY, 24., 2019, Luxembourg. *Annals* [...]. Luxembourg: Springer, 2019. Disponível em: https://core.ac.uk/download/pdf/286340939.pdf. Acesso em: 2 dez. 2020.

ÁVILA, Humberto. *Teoria dos princípios*: da definição à aplicação dos princípios jurídicos. 18. ed. rev. e atual. São Paulo: Malheiros, 2018.

BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor.* São Paulo: Almedina, 2018.

BRANCHER, Paulo Marcos Rodrigues; KUJAWSKI, Fabio Ferreira; CASTELLANO, Ana Carolina Heringer Costa. Princípios Gerais de Proteção de Dados Pessoais: uma análise dos princípios elencados no art. 6º da Lei 13.709/2018 (LGPD). *In*: BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Cláudia (org.). *Proteção de dados pessoais no Brasil*: uma nova visão a partir da Lei 13.709/2018. Belo Horizonte: Fórum, 2019. p. 72-73.

DWORKIN, Ronald. *Levando os direitos a sério.* Tradução: Nelson Boeira. São Paulo: WWF Martins Fontes, 2010.

MARINONI, Luiz Guilherme. *Novo curso de processo civil*: teoria do processo civil. São Paulo: Revista dos Tribunais, 2017. v. 1.

MARQUES, Cláudia Lima. *Comentários ao código de defesa do consumidor.* São Paulo: Thomson Reuters Brasil, 2019.

MARQUES, Cláudia Lima. *Contratos no código de defesa do consumidor*: o novo regime das relações contratuais. São Paulo: Thomson Reuters Brasil, 2019.

MELLO, Marcos Bernardes. *Teoria do fato jurídico*: plano da validade. São Paulo: Saraiva, 2019.

OLIVEIRA, Marco Aurélio Bellize; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 53-84.

PERLINGIERI, Pietro. *Perfis do direito civil.* Tradução: Maria Cristina De Cicco. Rio de Janeiro: Renovar, 2002.

REBOUÇAS, Rodrigo Fernandes. *Contratos eletrônicos*: formação e validade. São Paulo: Almedina, 2018.

VAINZOF, Rony. Dados pessoais, tratamento e princípios. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *Comentários ao gdpr*: regulamento geral de proteção de dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 61-62.

TUTELA JURÍDICA DOS DADOS PESSOAIS: UMA RELAÇÃO COM OS DIREITOS DE PERSONALIDADE

Lorena Esquivel de Brito

Introdução

A proteção de dados se apresenta na atualidade como um dos mais relevantes segmentos que têm interferências, sociais, econômicas e políticas. A necessidade de tutela jurídica ganha maior relevância diante das novas relações sociais com as facilidades de acesso aos aparelhos de tecnologia através da internet.

O paradoxo existente entre a exposição deliberada da vida privada e a necessidade proteção dos direitos de personalidade impõe uma reflexão sobre novas manifestações da privacidade e da disponibilidade dos dados pessoais. Assim, questiona-se, em que se fundamenta a proteção de dados pessoais?

Para responder a esta questão, é necessário levar em consideração a tutela jurídica concedida aos direitos de personalidade e o fato de que os dados pessoais representam as características individuais de cada ser humano. Assim, dados coletados massivamente por grandes empresas alimentam um sistema que propicia o capitalismo, tendo em vista que é possível traçar um perfil do cidadão dentro de expectativas do mercado de consumo em desrespeito aos direitos de personalidade do ser humano.

Diante disso, este capítulo tem como objetivo geral analisar como se estabelece a tutela concedida pelo ordenamento jurídico brasileiro

no que diz respeito à proteção da privacidade e dos dados pessoais tendo em vista novas relações sociais estabelecidas com o advento da era digital.

Para isso, tem-se como objetivos específicos pesquisar a legislação e a doutrina no que se refere aos direitos de personalidade, em seguida analisar a relação da privacidade com a proteção dos dados pessoais e, por fim, compreender a resposta dada pelo ordenamento jurídico brasileiro no que diz respeito à proteção de dados pessoais.

O trabalho está estruturado em três seções. Na primeira seção propõe-se realizar um estudo sobre a tutela jurídica da personalidade no ordenamento jurídico brasileiro. Na segunda seção busca-se compreender os aspectos principais da privacidade e sua relação com a proteção de dados pessoais. Na terceira seção tem-se uma abordagem sobre a tutela jurídica dos dados pessoais no ordenamento jurídico brasileiro.

A metodologia utilizada se baseia no método de revisão de literatura e pesquisa documental como a Constituição Federal, Código Civil, Lei Geral de Proteção de Dados (LGPD), a doutrina e artigos científicos a respeito do tema abordado.

A pesquisa do presente tema se justifica diante do fato de que as novas tecnologias trouxeram e continuam trazendo verdadeiras revoluções no modo de pensar e agir das pessoas, desencadeando alterações profundas nas relações sociais e na proteção que deve ser concedida a valores como liberdade, intimidade e privacidade. Assim, o referido trabalho pode permitir uma compreensão sobre os direitos de personalidade e sua relação com a proteção de dados pessoais.

Tutela jurídica da personalidade no ordenamento jurídico brasileiro

Os direitos de personalidade se manifestam sob a análise dos aspectos históricos, da Constituição Federal de 1988 e do Código Civil de 2002,

levando em consideração o fato de que as diversas mudanças sociais impuseram o reconhecimento da autonomia e da individualidade como forma de proteção da personalidade da pessoa natural.

Dentro de uma perspectiva histórica, sobre a proteção da personalidade da pessoa natural, Roxana Borges[1] destaca a importância do momento pós Revolução Francesa, na Europa, com a luta contra o poder absolutista e a busca pelos direitos individuais, nomeadamente a liberdade. No Brasil, o ordenamento civilista seguia as Ordenações Filipinas e, por isso, verifica-se que a razão de não ter sido elaborado o Código Civil pátrio ainda no século XIX tenha sido tão somente a tentativa de preservação da tradição jurídica lusitana no ordenamento brasileiro.

No entanto, segundo Orlando Gomes, tratava-se de um trabalho preparatório da codificação, constituindo, na opinião do civilista, um "marco decisivo na evolução do Direito Civil brasileiro"[2] que, em verdade, em muito facilitou o trabalho posterior do codificador. Isso porque, na época, a cultura do individualismo jurídico e do liberalismo econômico era predominante, o que serviu de inspiração para o conteúdo do Código Civil de 1916.

Com fundamento na liberdade e na autonomia privada, a intervenção do Estado era mínima, apenas para garantir que o acordado entre as partes fosse cumprido, nomeadamente a propriedade privada e o cumprimento dos contratos.

Neste sentido, afirma Roxana Borges que "no Estado liberal, para reduzir os abusos do absolutismo, a distinção entre direito público e privado foi nítida e muito importante, pois se buscou delimitar ao máximo os espaços de intervenção do Estado e os espaços de atuação

1 BORGES, Roxana Cardoso Brasileiro. *Direitos de personalidade e autonomia privada*. 2. ed. rev. São Paulo: Saraiva, 2007. p. 73.

2 GOMES, Orlando. *Raízes históricas e sociológicas do Código Civil brasileiro*. São Paulo: Martins Fontes, 2006. p. 12.

privada".[3] Por isso, por muito tempo, o Estado precisou se manter distante e sem atuar de forma intervencionista nessas relações privadas, deixando a legislação civilista responsável por regular as regras mínimas a serem atendidas nessas relações.

No entanto, diante de abusos de direitos, desrespeitos e com a complexidade das relações entre os indivíduos, foi necessário a retomada do Estado com intuito de traçar regras mínimas a serem observadas nas relações privadas, de modo a proteger os indivíduos contra possíveis abusos praticados no desenvolvimento das relações jurídicas.

As experiências compartilhadas por diversos ordenamentos jurídicos fazem com que exista uma confluência de ideias e valores a serem protegidos em momentos semelhantes, mas isso não significa uma uniformidade internacional. Por isso, um aspecto que merece destaque no que se refere à proteção da personalidade da pessoa natural é a sua proteção através da internacionalização de direitos humanos. Após as atrocidades cometidas durante a Segunda Guerra Mundial, a comunidade internacional entendeu a necessidade e importância de proteger o ser humano, a partir da sua compreensão enquanto sujeito de direitos. Assim, em 1945, os países vencedores da guerra criaram a Organização das Nações Unidas (ONU) e trouxeram o rol de direitos do ser humano através da criação da Declaração Universal de Direitos Humanos de 1948 (DUDH). Sobre este assunto, André Ramos explica:

> Como marco dessa nova etapa do Direito Internacional, foi criada, na Conferência de São Francisco em 1945, a Organização das Nações Unidas (ONU). O tratado institutivo da ONU foi denominado 'Carta de São Francisco' ou 'Carta das Nações Unidas'. Porém, a Carta da ONU não listou o rol dos direitos que seriam considerados essenciais. Por isso, foi aprovada, sob a forma de Resolução da Assembleia Geral da ONU, em 10 de dezembro de 1948, em Paris,

3 BORGES, *op. cit.*, p. 74.

> a Declaração Universal de Direitos Humanos (também chamada de 'Declaração de Paris'), que contém 30 artigos e explicita o rol de direitos humanos aceitos internacionalmente.[4]

A DUDH traz um rol de direitos considerados como essenciais para o livre desenvolvimento do ser humano e da sua personalidade, dentre esses direitos, merece destaque a proteção aos direitos de personalidade descritos no art. 12, que diz:

> Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.[5]

Desse modo, com as modificações ocorridas, o ordenamento jurídico brasileiro passou a ter uma preocupação em atuar de forma que os cidadãos pudessem exercer os seus direitos livremente, com respeito à dignidade e propiciando o livre desenvolvimento da personalidade da pessoa natural.

Para Sarlet, Marinoni e Mitidiero "é o Estado que existe em função da pessoa humana, e não o contrário, já que o ser humano constitui a finalidade precípua, e não meio da atividade estatal".[6] Assim, a proteção à personalidade jurídica da pessoa natural tem forte relação com a dignidade da pessoa humana.

Nesse sentido, o ordenamento jurídico brasileiro a Constituição Federal de 1988 (CF/88) traz no seu art. 1º os fundamentos da República Federativa do Brasil, dentre eles encontra-se a "dignidade da pessoa humana". Esta pode ser considerada como essencial para a proteção

4 RAMOS, André de Carvalho. *Curso de Direitos Humanos*. 5. ed. São Paulo: Saraiva, 2018. p. 49-50.

5 NAÇÕES UNIDAS (Brasil). *Declaração Universal de Direitos Humanos*. Brasília, DF: Nações Unidas, 1948.

6 SARLET, Ingo Wolfgang; MARINONI, Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 8. ed. São Paulo: Saraiva, 2019. p. 268.

dos direitos fundamentais dos seres humanos e, portanto, dos seus direitos de personalidade.

Os direitos de personalidade recebem tratamento na CF/88, na categoria de "direitos fundamentais", conforme transcrição do inciso X do art. 5º, que diz "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".[7] Dentro da perspectiva dos direitos fundamentais, Peixoto e Ehrhardt Júnior defendem que "a inviolabilidade da casa é direito de privacidade, protege o ambiente privado do lar, as relações que ali se desenvolvem livres do julgamento social".[8]

No âmbito infraconstitucional, os direitos de personalidade estão no Código Civil, na parte geral, nos arts. 11 a 21, destacando-se as características extraídas do art. 11 que dizem: "com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis".[9] Por isso, a intransmissibilidade, a inalienabilidade e a indisponibilidade devem se comunicar com a proteção da dignidade humana. Anderson Schreber complementa que os direitos de personalidade "Nascem e morrem com aquela pessoa, não podendo ser cedidos, doados, emprestados, vendidos ou recebidos por herança".[10]

Observa-se, em que pese serem estas as suas características, que os direitos de personalidade dizem respeito à realização pessoal do indivíduo, por isso, caberia à própria pessoa escolher sobre a transmissão ou a comercialização.

7 BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 1988.

8 PEIXOTO, Érick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. *Revista Brasileira de Direito Civil*, Belo Horizonte, v. 16, p. 35-56. 2018. p. 54.

9 BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: seção 1, Brasília, DF, ano 130, n. 8, p. 1-74, 11 jan. 2002.

10 SCHREIBER, Anderson. *Direitos da personalidade*. 3. ed. São Paulo: Atlas, 2014. p. 24.

Além disso, no que diz respeito à classificação dos direitos de personalidade, Farias e Rosenvald trazem uma classificação, levando em consideração os aspectos fundamentais da personalidade:

> a integridade física (direito à vida, direito ao corpo, direito à saúde ou inteireza corporal, direito ao cadáver...), a integridade intelectual (direito à autoria científica ou literária, à liberdade religiosa e de expressão, dentre outras manifestações do intelecto) e a integridade moral ou psíquica (direito à privacidade, ao nome, à imagem etc.).[11]

Sendo assim, a tutela jurídica da personalidade da pessoa natural abrange a proteção da integridade física, intelectual, moral e psíquica, guardando relação com o direito à proteção dos dados pessoais dos indivíduos.

Um caminho a percorrer: da privacidade à proteção de dados pessoais

Com o advento da era digital, mudanças comportamentais foram impostas de forma irrefletida, desaguando na complexidade da sociedade da informação. A produção legislativa não consegue dar respostas com a rapidez necessária para as demandas sociais. E isso se manifesta nitidamente quando o assunto abordado é a proteção dos dados pessoais.

Sobre os aspectos históricos da privacidade, Stefano Rodotà[12] entende que o nascimento da privacidade se dá com o fim do sistema feudal, visto que na organização feudal vivia-se em comunidade e

11 FARIAS, Cristiano Chaves de; ROSENVALD Nelson. *Curso de direito civil*: parte geral e LINDB. 13. ed. rev. ampl. e atual. São Paulo: Atlas, 2015. p. 171.

12 RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 26.

a privacidade só era possível para privilegiados ou para aqueles que viviam afastados da comunidade.

Segundo Roxana Borges, o direito civil muito resistiu, e ainda resiste, em se adaptar às evoluções econômicas, sociais e culturais vivenciadas ao longo do tempo, no entanto, "a inalterabilidade e intangibilidade do direito civil são muito mais fictícias do que reais, são mais uma ilusão do que um fato",[13] principalmente diante das grandes revoluções econômicas e sociais.

Por este motivo, a busca por encontrar o fundamento para a proteção dos dados pessoais conduz aos direitos de personalidade, nomeadamente a privacidade. Para isso, deve-se abordar em conjunto os direitos à intimidade e à privacidade, visto serem indissociáveis da vida privada, da autonomia e da individualidade.

Sobre este assunto, Sarlet, Marinoni e Mitidiero entendem que embora as dimensões (privacidade e intimidade) tenham sido expressamente referidas no art. 5º, X da CF/88, elas devem ser analisadas em conjunto, na medida em que ambas as situações se relacionam com as esferas do direito da vida privada.[14]

Nesse sentido, a proteção à privacidade estaria relacionada ao "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular".[15] Portanto, deve ser tutelado o direito de não sofrer interferências externas, o direito de ter a sua individualidade compartilhando a vida privada apenas com um grupo pequeno de escolha do indivíduo.

Além disso, Peixoto e Ehrhardt Júnior defendem ainda que a noção de privacidade é variável de acordo com cada sociedade e cultura, sendo possível a sua adaptação em decorrência da complexidade social:

13 BORGES, *op. cit.*, p. 74.

14 SARLET; MARINONI; MITIDIERO, *op. cit.*, p. 456.

15 RODOTÀ, *op. cit.*, p. 15.

> Ao longo da história, nas diferentes sociedades e em seus mais diferentes meios, a noção de privacidade foi sentida de uma maneira muito própria em cada círculo social. Daí a razão de se dizer que a privacidade é algo plástico, que varia conforme a época e o local. É adaptável, valorada de um jeito por uma cultura, e até dispensável para outra.[16]

O tratamento conferido à proteção de dados pessoais na Europa e nos Estados Unidos se apresenta de maneiras diferentes, compatíveis com os ideais defendidos pelos europeus e pelos estadunidenses, no que se relacionam à intervenção estatal e às esferas da liberdade. Sobre este aspecto, Peixoto e Ehrhardt Júnior explicam que:

> As raízes da privacidade nos Estados Unidos estão em um direito do indivíduo, de caráter negativo, enquanto que as raízes europeias estão também na sociedade, apresentando características de direito positivo, no qual se exige do Estado que se tomem medidas para garantir a proteção de dados pessoais, como a instalação de órgãos de controle, além de a proteção visar grupos minoritários que podem sofrer discriminações com a exposição de seus dados pessoais. Na Europa se desenvolve o aspecto social da privacidade.[17]

Para os europeus, a intervenção do Estado na tutela dos direitos se apresenta de forma essencial para a ordem jurídica e a justiça, enquanto para os estadunidenses a intervenção deve ser mínima, fundamentada no exercício da liberdade e concretizada na escolha dos indivíduos. Essa perspectiva se reflete na condução da proteção de dados pessoais conferida pelo Estado.

No Brasil, com o aumento da circulação e armazenamento de dados, a atuação do Estado tem fundamental importância. Danilo Doneda

16 PEIXOTO; EHRHARDT JÚNIOR, *op. cit.*, p. 36.

17 PEIXOTO; EHRHARDT JÚNIOR, *op. cit.*, p. 42.

defende que uma proteção específica através da legislação se apresenta de forma essencial:

> Aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo.[18]

O controle se mostra como instrumento necessário para a proteção da privacidade e consequentemente dos dados pessoais, segundo Stefano Rodotà, "a atenção deve passar do sigilo ao controle".[19]

Com base nisso, Danilo Doneda analisa a necessidade de estabelecer a relação entre a proteção de dados pessoais, direitos fundamentais e direitos de personalidade como necessários para a tutela jurisdicional, assim destaca:

> No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada.[20]

Outro aspecto que merece destaque é a existência de um ambiente adequado para o exercício dos direitos de personalidade de forma plena. Isso seria possível, segundo Danilo Doneda, através de "mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus

18 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, 2011. p. 94

19 RODOTÀ, *op. cit.*, p. 15.

20 DONEDA, *op. cit.*, p. 103.

próprios dados – que, no fundo, são expressão direta de sua própria personalidade".[21]

Portanto, o fortalecimento do conhecimento e os mecanismos de exercício da liberdade são basilares para a autonomia privada no âmbito das relações proporcionadas pelas mudanças nas relações sociais estabelecidas ou pelas redes da internet. Para Maurício Requião a autonomia privada está relacionada com a autonomia existencial, pois se dirige à liberdade do sujeito em gerir sua vida e sua personalidade, de forma digna.[22] O exercício da autonomia existencial permitirá ao indivíduo fazer sua escolha de forma refletiva, consciente das consequências jurídicas e compatível com os seus reais interesses.

A proteção de dados pessoais no ordenamento jurídico brasileiro

A utilização das ferramentas tecnológicas trouxe para a sociedade brasileira uma rapidez na comunicação e circulação de informações, aproximando pessoas e encurtando distâncias. É um cenário semelhante ao de outros países, pois trata-se de um fenômeno global que desterritorializa fronteiras.

Nesta linha de pensamento Peixoto e Ehrhardt Júnior[23] observam o grande impacto das tecnologias da informação para a sociedade. A partir disso, é possível presenciar intercâmbios culturais, fomento da economia, crescimento do mercado de consumo e produção de conhecimento.

A preocupação com a proteção dos dados pessoais torna-se mais evidente a partir das modificações nas relações sociais, no século XX, oriundas das diversas conexões em redes proporcionadas

21 DONEDA, *op. cit.*, p. 103.

22 REQUIÃO, Maurício. *Estatuto da Pessoa com Deficiência, Incapacidades e Interdição*. São Paulo: Tirant lo blanch, 2018. p. 32.

23 PEIXOTO; EHRHARDT JÚNIOR, *op. cit.*, p. 36.

pela internet com as inovações introduzidas pelos avanços da ciência no campo da informática.

Segundo os dados do Instituto Brasileiro de Geografia e Estatística (IBGE), atualmente três em cada quatro brasileiros estão de alguma forma conectados à internet. O número representa o equivalente a 79,1% das casas brasileiras com internet.[24]

Diante dessa mudança de perfil da sociedade brasileira, verifica-se a necessidade de uma sistemática de proteção de dados pessoais que parta do pressuposto do direito do indivíduo de escolher quais informações pessoais deseja compartilhar. Por esse motivo, o consentimento é elemento basilar para dar validade ao fluxo dos seus dados pessoais, de modo que o próprio cidadão possa exercer um controle sobre os caminhos e alcance de suas informações.[25]

Em sua análise, Rafael Zanatta[26] destaca que o debate sobre privacidade e proteção de dados guarda profunda relação com concepções democráticas de controle da atividade governamental. Sendo assim, deve haver um equilíbrio para que os cidadãos exerçam controle sobre as informações que são coletadas, seja pelo governo, seja pelas empresas privadas. Neste sentido:

> O modelo teórico da regulação do risco, aplicável à proteção de dados pessoais, está relacionado a autores que analisam a 'reformatação' da proteção de dados pessoais por um prisma mais complexo do direito regulatório, envolvendo mecanismos de contenção de abusividade e técnicas de prevenção e mitigação a riscos a direitos e liberdades em uma perspectiva coletiva.[27]

24 TOKARNIA, Mariana. Um em cada 4 brasileiros não tem acesso à internet, mostra pesquisa. *Agência Brasil*, Rio de Janeiro, 2020.

25 DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (org.). *Direito digital*: direito privado e internet. 2. ed. Indaiatuba: Foco, 2019.

26 ZANATTA, Rafael A. F. *Proteção de dados pessoais como regulação de risco*: uma nova moldura teórica?. *In*: ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1., 2017, Rio de Janeiro. *Anais* [...]. Rio de : [*s. n.*], 2017. p. 180.

27 ZANATTA, *op. cit.*, p. 181.

Além disso, a atuação governamental, conferindo proteção aos cidadãos, cumpre uma função extremamente importante, pois as informações pessoais armazenadas podem ser utilizadas com desrespeito à privacidade. Pois, com essas informações, aquele que armazena dados pessoais poderia vender esses dados para empresas que fariam disso um mercado consumidor, visto que os dados são mapeados e possibilitam traçar crenças, ideologias. Ou, ainda, poderiam ser mapeados e vendidos para atender a interesses do jogo político.

Por esse motivo, a grande quantidade de informações que são armazenadas e que circulam através das *big techs* causa preocupação devido ao desrespeito à privacidade de cada indivíduo e ao controle que pode ser exercido. Esse mapeamento e controle de dados atende aos interesses do capitalismo de vigilância, conduzindo e manipulando os interesses dos indivíduos.

A privacidade e o tratamento dos dados pessoais têm ligação direta, conforme estudo realizado na década de 1970 apontado por Danilo Doneda:

> No início da década de 1970, a *Secretary for health, education and welfare* reuniu uma comissão de especialistas que divulgou, em 1973, um estudo que concluiu pela relação direta entre a privacidade e os tratamentos de dados pessoais, além da necessidade de estabelecer a regra do controle sobre as próprias informações.[28]

Nessa perspectiva, interessa destacar os princípios relacionados à proteção de dados pessoais:[29] princípio da publicidade (ou da transparência); princípio da exatidão; princípio da finalidade; princípio do livre acesso; e princípio da segurança física e lógica. Nesta linha, os princípios cumprem uma importante missão, pois eles representam o alicerce para a elaboração legislativa, sua aplicação e interpretação.

No caminho para a tutela jurídica dos dados pessoais, tramita na Câmara dos Deputados a Proposta de Emenda Constitucional (PEC) nº

28 DONEDA, *op. cit.*, p. 99.

29 DONEDA, *op. cit.*, p. 99.

17 de 2019, que tem por objetivo "incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão".[30]

Nesta senda, o Brasil elaborou a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709 de 14.08.2018,[31] que entrou em vigor no ordenamento jurídico de forma gradativa conforme determinação do seu artigo 65. Apesar de a Constituição Federal não incluir a proteção de dados pessoais como direito fundamental, a LGPD segue uma sistemática similar com as orientações europeias da *General Data Protection Regulation* (GDPR).

Os direitos fundamentais de liberdade e privacidade, destacadas no artigo 1º da LGPD, são compreendidos como direitos individuais do ser humano e, também, como direitos de personalidade. Por esse motivo, devem ser protegidos tanto por pessoa natural quanto por pessoa jurídica, seja de direito público ou privado, de modo que aquele que fizer o tratamento de dados pessoais precisa respeitar a tutela consagrada pela LGPD.

Sobre proteção de dados, existem ainda aqueles que são considerados "dados sensíveis" e, por isso, despertam uma preocupação ainda mais no que diz respeito ao seu uso indiscriminado:

> Por exemplo, uma empresa que pretenda desenvolver tecnologia de reconhecimento facial e coleta de dados biométricos a partir da análise de filmagens feitas por drones em áreas abertas claramente trará risco elevado de lesão a direitos fundamentais, tanto em razão da coleta de dados biométricos (considerados dados

30 BRASIL. *PEC 17/2019*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Senado Federal, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 10 nov. 2020.

31 BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n° 12.965, de 23 de abril de 2014 (Marco Civil da Internet). ***Diário Oficial da União***: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

> sensíveis que só podem ser coletados para finalidades específicos e com consentimento informado dos titulares), quanto em razão da coleta ser feita a partir de áreas geográficas abertas.[32]

Diante da necessidade de proteção dos dados pessoais, regras de controle sobre a manipulação dos dados pessoais são fundamentais. Danilo Doneda defende que:

> Por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais.[33]

Verifica-se, portanto, que os dados coletados massivamente pelo *big data* alimentam um sistema de capitalismo de vigilância, de modo que empresas de *big tech* armazenam dados pessoais, inclusive os sensíveis, para traçarem um perfil do cidadão dentro de expectativas do mercado de consumo, fomentando e fortalecendo o capitalismo em detrimento dos direitos individuais e da liberdade do ser humano.

Considerações finais

O advento da modernidade trouxe mudanças significativas nas relações sociais, seja na forma como a relação é estabelecida, seja no conteúdo objeto das relações, seja também nas consequências jurídicas dessas relações.

A grande exposição da vida privada impõe uma reflexão sobre a tutela jurídica a ser concedida em tempos de rapidez na circulação e armazenamento das informações pessoais. Neste sentido, a tutela

32 ZANATTA, *op. cit.*, p. 184.

33 DONEDA, *op. cit.*, p. 95.

jurídica concedida aos dados pessoais deve se fundamentar na tutela jurídica concedida aos direitos de personalidade, visto que guardam entre si as mesmas características.

Em decorrência das grandes mudanças de comportamento da sociedade brasileira, a PEC nº 17/2019[34] tem como objetivo a inclusão da proteção dos dados pessoais como direito fundamental do ser humano. Essa proposta de modificação na Constituição Federal não significa uma garantia de concretização e efetividade deste direito, mas ao menos cumpre uma função simbólica e importante no que diz respeito à tutela jurídica dos dados pessoais.

Nesse sentido, em âmbito infraconstitucional, o ordenamento jurídico brasileiro, atuando dentro do exercício do poder legislativo, elaborou LGPD buscando trazer uma proteção específica sobre o tratamento de dados pessoais.

Portanto, a sistemática de proteção dos dados pessoais guarda relação direta com os direitos de personalidade, no entanto, não pode se limitar à concepção tradicional, sendo necessário haver uma adequação capaz de atender à proteção dos direitos de personalidade diante das constantes modificações das relações sociais.

Referências

BORGES, Roxana Cardoso Brasileiro. *Direitos de personalidade e autonomia privada*. 2. ed. rev. São Paulo: Saraiva, 2007.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 dez. 2020.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: seção 1, Brasília, DF, ano 130, n. 8, p. 1-74, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 30 out. 2020.

34 BRASIL. PEC n° 17/2019, *op. cit.*

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 nov. 2020.

BRASIL. *PEC 17/2019*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Senado Federal, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 10 nov. 2020.

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

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (org.). *Direito digital*: direito privado e internet. 2. ed. Indaiatuba, Foco, 2019. p. 35-54.

FARIAS, Cristiano Chaves de; ROSENVALD Nelson. *Curso de direito civil*: parte geral e LINDB, 13. ed. rev. ampl. e atual. São Paulo: Atlas, 2015, v. 1.

GOMES, Orlando. *Raízes históricas e sociológicas do Código Civil brasileiro*. São Paulo: Martins Fontes, 2006.

NAÇÕES UNIDAS BRASIL (Brasil). *Declaração Universal de Direitos Humanos*. Brasília, DF: Nações Unidas, 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 17 dez. 2020.

PEIXOTO, Érick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. *Revista Brasileira de Direito Civil*, Belo Horizonte, v. 16, p. 35-56, 2018.

RAMOS, André de Carvalho. *Curso de Direitos Humanos*. 5. ed. São Paulo: Saraiva, 2018.

REQUIÃO, Maurício. *Estatuto da Pessoa com Deficiência, Incapacidades e Interdição*. São Paulo: Tirant lo blanch, 2018.

RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang; MARINONI, Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 8. ed. São Paulo: Saraiva Educação, 2019.

SCHREIBER, Anderson. *Direitos da Personalidade*. 3. ed. São Paulo: Atlas, 2014.

TOKARNIA, Mariana. Um em cada 4 brasileiros não tem acesso à internet, mostra pesquisa. *Agência Brasil*, Rio de Janeiro, 2020. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2020-04/um-em-cada-quatro-brasileiros-nao-tem-acesso-internet. Acesso em: 16 dez. 2020.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?. *In*: ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1., 2017, Rio de Janeiro. *Anais* [...]. Rio de Janeiro [*s. n.*], 2017. Disponível em: http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf. Acesso em: 5 maio 2020.

BREVES NOTAS SOBRE ANONIMIZAÇÃO E PROTEÇÃO DE DADOS PESSOAIS

Marcos Ehrhardt Jr.
Jéssica Andrade Modesto

Introdução

Em 2017,[1] o Centro Médico da Universidade de Chicago realizou uma parceria para compartilhar dados de pacientes com o Google, para o desenvolvimento de novas ferramentas de inteligência artificial voltadas para serviços de saúde, que utilizariam métodos de previsão e análise a fim de organizar o fluxo de um hospital, com um sistema capaz de prever quanto tempo um paciente ficaria internado e o que faria sua saúde deteriorar-se, com base em dados de casos semelhantes.

No ano passado, o Google publicou um trabalho de pesquisa com dados de prontuários eletrônicos de pacientes da Universidade de Chicago Medicine, de 2009 a 2016, que incluíam diagnósticos, procedimentos, medicação e outros dados do paciente. Segundo declara, esses registros médicos foram anonimizados. Também afirma que as datas de serviço foram mantidas e que a Universidade de Chicago forneceu anotações médicas, porém, tais anotações também foram desidentificadas.

Agora, a Universidade de Chicago, o centro médico e o Google estão sendo processados em uma ação coletiva que acusa o hospital

1 WAKABAYASHI, Daisuke. Google and the University of Chicago are sued over data sharing. *The New York Times*, New York, 26 jun. 2019.

de compartilhar com o Google centenas de milhares de registros de pacientes que continham datas de entrada e saída dos pacientes, além de anotações médicas. Isso violaria a privacidade dos pacientes, sobretudo porque o Google poderia combinar esses dados com outras informações que já detém, como dados de localização de *smartphones* com Sistema Operacional Android ou com os *softwares* Google Maps e Waze, para estabelecer a identidade dos pacientes.

Por sua vez, o Google aduz ter seguido todas as diretrizes do *Health Insurance Portability e Accountability Act* (Hipaa), que permitem divulgar informações pessoais de saúde sem autorização, em certas instâncias, para fins de pesquisa. De igual forma, o Centro Médico da Universidade de Chicago também afirma ter cumprido as leis e regulamentos aplicáveis à privacidade do paciente.

O Hipaa, o regulamento federal estadunidense que protege os dados de saúde confidenciais dos pacientes, permite que os provedores médicos tenham permissão para compartilhar registros médicos, desde que os dados sejam desidentificados. Assim, para atender ao padrão Hipaa, os hospitais devem retirar informações individualmente identificáveis, como o nome do paciente e o número da Previdência Social, bem como as datas diretamente relacionadas ao indivíduo, incluindo as datas de admissão e de alta.

Stacey A. Tovino, professora de direito da saúde na Universidade de Nevada, em Las Vegas, observa que o Hipaa foi promulgado em 1996, isto é, antes de a indústria de tecnologia começar a coletar grandes quantidades de informações pessoais. Isso tornou os regulamentos desatualizados, porque a ideia de quais informações são consideradas individualmente identificáveis mudou com os avanços da tecnologia.

Importante dizer, ainda, que a denúncia não ofereceu evidências de que o Google usou indevidamente as informações fornecidas pelo centro médico ou fez tentativas para identificar os pacientes.

Esse caso recente ilustra bem como a preocupação das pessoas com os riscos da reidentificação pode se tornar um grande entrave ao

desenvolvimento tecnológico e de seus benefícios para a sociedade – mesmo se tratando de dados anônimos, uma vez que estas informações estariam em poder de um gigante da tecnologia que armazena diversos outros dados.

A Era da Informação e, mais especificamente, a internet como um de seus mais característicos instrumentos de proliferação da informação, implicam modificações significativas na forma como se regem e se regulam as relações sociais. O Direito não pode ser um instrumento estático, alheio às mudanças inerentes à evolução das relações humanas.

Os dados pessoais tornaram-se valiosos ativos para a economia. Em um país no qual não haja legislação específica atinente à proteção de dados, a coleta, o tratamento e o compartilhamento desses dados acabam sendo regulados pelo próprio mercado, o que, muitas vezes, acarreta abusos por parte dos agentes de tratamento, de modo que a privacidade dos indivíduos não recebe a tutela adequada.

Diante disso, surgem legislações sobre a proteção de dados pessoais, a exemplo do Regulamento Geral de Proteção de Dados (RGPD) e da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD),[2] a qual ainda se encontra em *vacatio legis*. No entanto, trará alterações significativas na atuação daqueles que precisam tratar dados pessoais no desenvolvimento de sua atividade, razão por que se faz necessário o estudo crítico da legislação. Nesse cenário, questiona-se: a proteção dos dados pessoais é sempre um obstáculo à nova economia?

A utilização dos dados pessoais traz inúmeros benefícios não só às grandes organizações que lucram a partir desses dados, mas também à sociedade, haja vista que esses dados são a principal matéria-prima de muitos serviços de utilidade pública. Por outro lado, o tratamento desses dados não pode gerar danos à privacidade dos indivíduos. Dessa forma, privacidade e avanços tecnológicos devem coexistir.

2 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

O presente trabalho se propõe a refletir se a LGPD oferece algum mecanismo que possibilite tal coexistência. Para tanto, será realizada uma pesquisa bibliográfica/documental acerca do tema, em doutrina e legislação nacional e estrangeira, já que a experiência europeia em matéria de proteção de dados pessoais pode servir de guia à compreensão e à efetivação da temática ainda em desenvolvimento no Brasil.

O direito fundamental à proteção de dados pessoais e a sua natureza jurídica

Na sociedade da informação em que estamos, a todo momento, conectados, faz-se necessário que tenhamos ciência de que não agimos apenas passivamente, isto é, recebendo informações; ao contrário, diariamente alimentamos essa rede com dados sobre nosso modo de ser, escolhas, gostos pessoais etc.

Em alguns momentos, o fornecimento desses dados é mais perceptível, como quando utilizamos uma rede social ou enviamos um *e-mail*, no entanto, constantemente estamos fornecendo essas informações de maneira que, muitas vezes, nem nos damos conta, a exemplo de quando utilizamos um mecanismo de busca ou mesmo o serviço de localização por GPS do *smartphone*. Posteriormente, esses dados são compartilhados com os chamados "parceiros" das organizações, muitas vezes até sem nosso consentimento.

Nesse cenário, surgem alguns questionamentos: qual a natureza jurídica dos dados pessoais? Eles seriam uma "coisa", um bem, que pode ser comercializado? Quem os compra poderá usá-los independentemente da vontade da pessoa a que esses dados estão vinculados ou, pelo contrário, os dados pessoais seriam uma extensão da nossa personalidade? Além disso, existiria, no sistema jurídico brasileiro, um direito fundamental à proteção de dados pessoais?

A esse respeito, Schertel Mendes afirma que a informação pessoal possui um vínculo objetivo com a pessoa, revelando aspectos que lhe dizem respeito e, justamente por isso, diferenciam-se das demais informações. Dessa forma, uma vez que têm como objeto a própria pessoa, os dados pessoais "constituem um atributo de sua personalidade".[3]

Nesse sentido, "na Sociedade da Informação, a representação da pessoa em informações é a própria pessoa que se conhece *a priori*, eis que é primeiramente representada por informações",[4] de modo que, ainda que o dado possa dissociar-se do indivíduo e circular pela internet, sendo um dado pessoal e, portanto, permanecendo com a qualidade de identificação de um indivíduo, deve ser entendido como uma extensão da personalidade.[5]

Assim, tutelam-se os dados pessoais para proteger a pessoa que é seu titular, máxime quando se tem em mente que tais dados podem representar os aspectos mais íntimos do indivíduo. Desse modo, aumenta-se a compreensão do direito à proteção de dados pessoais como um pressuposto fundamental das sociedades democráticas, por permitir o livre desenvolvimento da personalidade dos indivíduos.[6]

A Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 1981, é considerada um importante marco no reconhecimento do direito à proteção de dados como fundamental

3 MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 56.

4 PEZZELLA, Maria Cristina Cereser; GHISI, Silvano. A manipulação de dados pessoais nas relações de consumo e o sistema "*crediscore*". *Civilista.com*, [*s. l.*], v. 4, n. 1, p. 1-29, 2015. p. 19.

5 PASSOS, Bruno Ricardo dos Santos. *O Direito à Privacidade e a Proteção aos Dados Pessoais na Sociedade da Informação*: uma abordagem acerca de um novo direito fundamental. 2017. Dissertação (Mestrado em Direito Público) – Programa de Pós-Graduação em Direito da Universidade Federal da Bahia, Salvador, 2017.

6 ARAÚJO, Alexandra Maria Rodrigues. As transferências transatlânticas de dados pessoais: o nível de proteção adequado depois de *Schrems*. *Revista Direitos Humanos e Democracia*, Unijuí, v. 5, n. 9, p. 201-236, 2017. p. 207.

por ser uma das primeiras que, em seu preâmbulo,[7] entende a proteção de dados como um pressuposto do estado democrático e, por isso, relaciona-se com a proteção dos direitos humanos e das liberdades fundamentais.[8]

Muitos instrumentos internacionais de proteção de direitos humanos preveem o direito à proteção de dados como uma extensão do direito à privacidade. Também a jurisprudência do TJUE não faz uma distinção entre esses dois direitos. Contudo, há, na doutrina, uma discussão se o direito à proteção de dados pessoais seria autônomo. Essa corrente diferencia privacidade e proteção de dados por entender que este tutela qualquer informação que diz respeito a uma pessoa, ainda que não se incluam no âmbito do direito ao respeito à vida privada.[9]

Nesse sentido, Rodotà entende que o direito à proteção de dados não deve ser subordinado a nenhum outro. Para o autor, a Carta de Direitos Fundamentais da União Europeia distinguiu, acertadamente, o direito à proteção de dados pessoais do direito à vida privada e familiar. Isso porque este último consiste em impedir a interferência na vida privada e familiar de um indivíduo e, por conseguinte, reflete um componente mais individualista, sendo um tipo de proteção estático, negativo. Já o direito à proteção de dados pessoais estabelece regras sobre os mecanismos de processamento de dados, bem como estabelece a legitimidade para

7 "Os Estados-membros do Conselho da Europa, signatários da presente Convenção: Considerando que a finalidade do Conselho da Europa é conseguir uma união mais estreita entre os seus membros, nomeadamente no respeito pela supremacia do direito, bem como dos direitos do homem e das liberdades fundamentais; Considerando desejável alargar a protecção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado; [...]".
CONSELHO DA EUROPA PARA A PROTEÇÃO DAS PESSOAS SINGULARES. *Convenção nº 108, de 1981*. Tratamento Automatizado de Dados Pessoais. Europa: [União Europeia], 1981.

8 DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, 2011. p. 102.

9 ARAÚJO, *op. cit.*, p. 206-208.

que uma autoridade tome medidas em sua defesa. Este seria um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos.[10]

Por sua vez, Doneda afirma que, no direito brasileiro, o reconhecimento da autonomia do direito à proteção de dados deriva da consideração

> "dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada".[11]

Mendes aduz que, no Brasil, o conceito de privacidade evoluiu, passando a abarcar a proteção de dados pessoais. Dessa feita, reconhece-se o direito fundamental à proteção de dados pessoais como uma dimensão da inviolabilidade dos direitos previstos pelo artigo 5º, X, da Constituição brasileira, quais sejam: intimidade e vida privada.[12] A esse respeito, foi aprovada no Senado Federal, em 2 de julho de 2019, a Proposta de Emenda à Constituição nº 17/2019, que visa incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão elencados no artigo 5º da CF/1988. O texto agora tramita na Câmara dos Deputados.[13]

Também Mulholland entende que, muito embora a Constituição brasileira não preveja, expressamente, o direito à proteção de dados pessoais como uma categoria de direitos fundamentais, o *locus* constitucional desse direito é a tutela da privacidade, que tem seu conceito ampliado em razão de a evolução das formas de divulgação e apreensão

10 RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 16-18.

11 DONEDA, *op. cit.*, p. 102.

12 MENDES, *op. cit.*, p. 170-171.

13 "Art. 1º Inclua-se no art. 5º da Constituição Federal o seguinte inciso XII-A: Art. 5º [...]. XII-A – é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais. [...]". (BRASIL, 2017). Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. (BRASIL, 2017).

de dados pessoais ter expandido as formas potenciais de violação da esfera privada, máxime pelo acesso não autorizado de terceiros a esses dados. Dessa feita, "a tutela da privacidade passa a ser vista não só como o direito de não ser molestado, mas também como o direito de controlar a circulação dos dados pessoais".[14]

Nessa mesma esteira, Anderson Schreiber afirma que, em uma "sociedade caracterizada pelo constante intercâmbio de informações, o direito à privacidade deve se propor a algo mais que àquela finalidade inicial, restrita à proteção da vida íntima",[15] devendo abarcar também o direito do indivíduo de manter o controle sobre seus dados pessoais.

Diante de toda a discussão exposta, comunga-se, neste trabalho, do entendimento de que a privacidade seria uma palavra guarda-chuva que abriga distintos direitos da mesma família,[16] como o direito ao sigilo, o direito à intimidade, o direito à imagem, o direito à honra, o direito à proteção dos dados pessoais.

Dessa forma, entende-se que, na sociedade da informação, a privacidade não mais se limita ao direito de ser deixado só, alcançando novos contornos, alicerçados na autodeterminação informativa e no direito de cada indivíduo decidir quando e como dispor de suas informações. É nesse contexto que o direito à proteção de dados é reconhecido como um direito fundamental.

Feitas essas considerações, passa-se agora às questões conceituais relacionadas aos dados pessoais, porquanto indispensáveis à temática ora estudada.

14 MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (13.709/18). *Revista Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, p. 159-180, 2018. p. 171-172.

15 Apud ROCHA, Luiz A. C. B. L. M. da; FILPO, Klever P. L. Proteção do direito à vida privada na sociedade da hiperexposição: paradoxos e limitações empíricas. *Civilista. com*, Rio de Janeiro, ano 7, n. 1, p. 1-31, 2018, p. 7.

16 PEIXOTO, Erick L. C. EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. *Revista Brasileira de Direito Civil*, Belo Horizonte, v. 16, p. 35-56, 2018.

Dados pessoais

A compreensão do conceito de dado pessoal[17] é fundamental para se verificar a abrangência material das legislações sobre proteção de dados pessoais, pois as leis sobre a matéria podem adotar uma concepção ampla ou restrita de dado pessoal, o que, por conseguinte, impacta diretamente sobre quais dados são protegidos por cada legislação.

Numa definição restrita, são dados pessoais apenas aquelas informações que se relacionam a uma pessoa identificada, específica, isto é, o vínculo entre o dado e a pessoa a quem esse dado está associado é estabelecido de forma direta, imediata.[18]

Já a acepção ampla abrange também os dados que potencialmente permitam a identificação do titular da informação, ou seja, um dado será considerado pessoal se a partir dele existir a possibilidade de se individualizar a pessoa a quem ele se refere, ainda que indiretamente.[19] Nesse sentido, o conceito de dado pessoal pode ser entendido como os fatos, comunicações e ações que se referem a um indivíduo identificado ou identificável.[20]

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), assim como o Regulamento Geral de Proteção de Dados da União Europeia (RGPD), adotou a concepção mais extensa de dado pessoal, definindo-o como a informação relacionada à pessoa natural identificada ou identificável.[21]

17 Apesar de parcela da doutrina distinguir os conceitos de dado pessoal e informação, neste trabalho as expressões serão utilizadas como sinônimas.

18 BIONI, Bruno R. Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. *Privacidade e Vigilância*, São Paulo, 2015. p. 17.

19 MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*, São Paulo, v. 998, p. 99-128, 2018. p. 106, Caderno Especial.

20 MENDES, *op. cit.*, p. 55-56

21 Artigo 5°, I, da Lei n° 13.709/2018.

O RGPD, por sua vez, em seu artigo 4º, diz que é identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.

Pelos exemplos trazidos pelo RGPD percebe-se mais claramente como informações que só permitam a identificação do titular pela via indireta podem ser consideradas como dados pessoais, como no caso do IP de computador, pelo qual se pode chegar à identificação de alguém, ainda que seja necessária autorização judicial para isso.

Assim, estar-se-á diante de um dado pessoal quando a informação for relativa a uma pessoa singular identificada ou identificável, independentemente do suporte, incluindo som e imagem.[22]

Dados pessoais sensíveis e as dificuldades de sua delimitação

Existem dados pessoais que podem ser utilizados com finalidades discriminatórias e que, por isso, merecem ser especialmente protegidos contra os riscos da circulação dessas informações, estabelecendo-se regras mais rigorosas para sua coleta, tratamento e armazenamento. Esses dados são classificados como "dados sensíveis".[23]

A esse respeito, o RGPD estabelece que merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais,

22 RIBEIRO, Florbela da Graça Jorge da Silva. *O tratamento de dados pessoais de clientes para marketing*. 2017. Dissertação (Mestrado em Direito, Especialidade em Ciências Jurídico-Políticas) – Departamento de Direito, Universidade Autónoma de Lisboa, Lisboa, 2017. p. 48.

23 RODOTÀ, *op. cit.*, p. 96.

dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais, estabelecendo-se, como regra geral, a proibição de tratamento desses dados.[24]

No Brasil, o artigo 5º, II, da LGPD dispõe que são sensíveis os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

A Lei nº 13.709/2018 traz uma seção específica acerca das particularidades no tratamento desses dados, tornando mais restritas as hipóteses de tratamento dos dados pessoais e exigindo que o consentimento do titular seja fornecido de forma específica e destacada, para finalidades específicas.

No que diz respeito aos dados sensíveis, surgem algumas questões relevantes, máxime na atualidade, em que uma vasta quantidade de dados é tratada e analisada por algoritmos: um dado pessoal é sensível em si, isto é, apenas por se relacionar à origem étnica ou convicção religiosa de um indivíduo, por exemplo, ou pela função que exerce? Um dado deve ser considerado sensível pelo simples fato de se encaixar no rol do artigo 5º, II, da LGPD, independentemente do contexto em que está inserido e da finalidade para que será utilizado? E se o dado pessoal, isoladamente, não disser respeito ao referido rol, contudo, ao ser combinado com outros dados, for capaz de revelar informações sensíveis sobre seu titular, este dado deverá ser considerado sensível e, portanto, receber o tratamento diferenciado previsto na LGPD, ou não?

No escândalo da Cambridge Analytica que foi tão noticiado em razão de supostamente ter influenciado as eleições estadunidenses, os usuários do *Facebook* respondiam ao teste de personalidade "This is Your Digital Life", que consistia em perguntas sobre se os usuários eram ou não extrovertidos, vingativos, se concluíam os projetos

24 Considerando 51 do RGPD.

que começavam, se se preocupavam constantemente, se gostavam de arte, entre outras questões acerca dos gostos e hábitos pessoais. Posteriormente, os resultados obtidos eram combinados com os dados extraídos dos perfis e amizades do *Facebook*,[25] que incluíam detalhes sobre a identidade das pessoas, como o nome, a profissão e o local de moradia, além da rede de contatos.

Segundo informações divulgadas na mídia, esse teste foi respondido por mais de 270 mil pessoas. Como os dados dos amigos dos participantes também foram coletados, mais de 50 milhões de usuários foram afetados. Esses dados, então, foram vendidos à Cambridge Analytica e utilizados para criar e catalogar perfis das pessoas, a fim de se direcionar, de forma mais personalizada, materiais pró-Trump e mensagens contrárias à adversária dele.[26] Assim, os dados coletados, se considerados individualmente, não eram classificados como sensíveis, entretanto, foi possível fazer inferências sensíveis dos usuários do *Facebook* pelo contexto em que tais dados estavam inseridos.[27]

Nesse mesmo caminho, um estudo que analisou as interações dos usuários do Facebook por meio de curtidas em fotos, atualizações de *status* de amigos, páginas de produtos, esportes, músicos, livros e restaurantes, concluiu que é possível inferir diversas informações sensíveis que os usuários acreditam ser privadas, como orientação sexual, etnia, opiniões religiosas e políticas e traços de personalidade, por meio de tais interações.[28]

25 PSICÓLOGO que criou aplicativo da Cambridge Analytica acreditava que sistema era legal. *O Globo*, São Paulo, 21 mar. 2018.

26 ENTENDA o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. *BBC News*, Londres, 20 mar. 2018.

27 Sobre o caso da Cambridge Analytica, a Netflix lançou o documentário original "Privacidade Hackeada", o qual se encontra disponível na referida plataforma: https://www.netflix.com/br/title/80117542.

28 KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. *PNAS*, [s. *l.*], v. 110, n. 15, 2013.

Outro estudo, realizado por pesquisadores da Universidade de Stanford, demonstrou que os metadados do telefone de cada pessoa podem ser extremamente reveladores, permitindo uma série de inferências sensíveis a respeito das associações familiares, políticas, profissionais, religiosas e sexuais.[29] Metadados são dados sobre os dados[30].

Nesse estudo, os participantes instalavam um aplicativo chamado MetaPhone, que enviava para os pesquisadores informações sobre o histórico de chamadas dos usuários: números de telefone para quem os participantes ligaram, dia e horário das chamadas, quantas vezes ligaram para determinado número e as durações das chamadas. Em seguida, os pesquisadores combinaram os números de telefone destinatários da chamada com os diretórios públicos do Yelp e do Google Places para identificá-los. A partir disso, os pesquisadores conseguiram realizar uma série de inferências sensíveis acerca dos participantes.

Assim, por exemplo, se uma pessoa conversa durante muito tempo com uma instituição religiosa, é bem provável que ela professe determinada fé. Em outro exemplo, um participante conversou por muito tempo com o cardiologista, comunicou-se brevemente com um laboratório médico, recebeu ligações de uma farmácia e fez breves telefonemas para um serviço relacionado a um dispositivo médico usado para monitorar a arritmia cardíaca. Os pesquisadores puderam confirmar que esse paciente realmente possuía um problema de saúde.[31]

Os casos acima expostos demonstram que dados que, se considerados isoladamente, por si mesmos não são dados sensíveis, ao serem

29 MAYER, Jonathan; MUTCHLER, Patrick. MetaPhone: The Sensitivity of Telephone Metadata. *Web Policy*, [*s. l.*], 12 mar. 2014. No mencionado estudo, os dados seriam o conteúdo das ligações, os metadados seriam as informações sobre a chamada, como data e duração da ligação.

30 MENEZES NETO, Elias J.; MORAIS, José Luis B.; BEZERRA, Tiago José S. L. O projeto de Lei de Proteção de Dados Pessoais (PL 5.276/2016) no mundo do Big Data: o fenômeno da Dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. *Revista Brasileira de Políticas Públicas*, Brasília, DF, v. 7, n. 3, p. 185-200, 2017. p. 191.

31 MAYER; MUTCHLER, *op. cit.*

analisados em conjunto desempenham a função de dados sensíveis. Entretanto, a LGPD traz uma definição de dados sensíveis que não leva em consideração a função que o dado exerce no contexto em que está inserido. Ao contrário, traz um rol de dados que, historicamente e pela sua natureza, são informações que podem gerar discriminação.

Essa técnica legislativa falha tanto por deixar de fora outros dados que podem gerar discriminação, como os relacionados à situação socioeconômica, bem como por desconsiderar que, a partir de dados pessoais não sensíveis, pode-se fazer inferências sensíveis, máxime na sociedade da informação, na qual os algoritmos e a inteligência artificial ampliam sobremaneira a capacidade de análise de dados.

A esse respeito, Mendes afirma que dados aparentemente insignificantes podem se tornar sensíveis, a depender do tratamento a que são submetidos. "Trata-se, na realidade, de um tratamento sensível dos dados, que é capaz de transformar dados inofensivos em informações potencialmente discriminatórias".[32] Aduz, ainda, que não existem dados insignificantes no contexto do processamento eletrônico.

Desse modo, conforme Ribeiro:

> Entende-se que a apreciação da natureza do dado sensível depende do tratamento automático que lhe é dado, por exemplo: um enfermeiro que presta apoio domiciliário a um idoso com a doença de Alzheimer incluindo a compra do medicamento com o seu cartão de débito e que o banco utiliza para construir o seu perfil de compras está a tratar dados sensíveis. A conexão entre o comprador e o produto não parece evidente, dado que há uma aquisição por conta de outrem. O dado que originalmente não é sensível, que depois de recolhido e tratado tem um determinado valor econômico, pode transformar-se em dado sensível dependendo da natureza da comunicação, isto é, o enfermeiro que mais tarde se dirige ao banco para celebrar um contrato de

32 MENDES, *op. cit.*, p. 76.

> mútuo para aquisição de habitação poderá ser confrontado com a recusa da celebração de um contrato de seguro associado ao mútuo devido à doença que foi incluída no seu perfil.[33]

Tendo em vista os efeitos nefastos que o tratamento e a utilização inadequada de informações sensíveis podem trazer aos titulares dos dados, faz-se necessário que a classificação de um dado como sensível ou não seja dinâmica e contextual, e que se considere o uso que se fará dos dados e quais as inferências que se pode obter a partir deles, razão por que é preciso investigar com mais profundidade os métodos de tratamento de dados.

Métodos de tratamento e a abrangência das legislações sobre proteção de dados

O desenvolvimento tecnológico e o aumento dos mecanismos utilizados para coleta de dados fazem surgir, de igual modo, a necessidade de ampliação de meios capazes de garantir a efetivação da privacidade das pessoas quando no processo de tratamento desses mesmos dados.

Quando o que está em jogo é a privacidade no âmbito da sociedade da informação e a ampla conectividade, o tratamento de dados ganha especial importância pois, a depender do tratamento conferido aos dados pessoais, pode-se atrair a tutela das legislações referentes à proteção de dados ou descaracterizá-los como dado pessoal e, consequentemente, afastar o alcance de normas de proteção de dados pessoais como a LGPD e o RGPD.

A LGPD, em seu artigo 5º, X, define o tratamento de dados como toda operação realizada com dados pessoais. Oferece como exemplo as operações que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição,

33 RIBEIRO, *op. cit.*, p. 62.

processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Por sua vez, o artigo 3º da LGPD dispõe que a lei deverá ser aplicada a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, ou seja, dentro ou fora da internet, por meios digitais ou não.

Os métodos de tratamento utilizados podem ser automatizados ou manuais. Além disso, podem ser operações necessárias às finalidades para a qual os dados foram coletados ou operações que visam à proteção da privacidade dos titulares dos dados, como, por exemplo, a manipulação das informações para a eliminação ou modificação dos atributos que podem identificar o indivíduo, como a codificação, a pseudonimização e a anonimização, que serão discutidas adiante.

Ademais, podem ser operações que atraem a aplicação da LGPD, como a coleta de dados pessoais, como também manipulações que afastam a aplicabilidade da norma. Isso porque o artigo 12 da Lei nº 13.709/2018 estabelece que os dados anonimizados não serão considerados dados pessoais para os fins da lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.[34]

Dessa forma, os dados pessoais podem ser tratados de modo a desvincular-se de seu titular, impossibilitando qualquer associação com um indivíduo específico ou, ainda, por meio de utilização de ferramentas, a exemplo da criptografia e da pseudonimização, as quais têm como objetivo prover maior segurança para os usuários de internet, dificultando a associação entre os dados e seu titular, mas possibilitando a reversão desse procedimento.

34 Também o RGPD, em seu artigo 2°, 1, dispõe que seu âmbito de aplicação é o tratamento de dados pessoais, trazendo a ressalva de sua não aplicação a informações anônimas ou dados pessoais tornados anônimos, conforme explicita o Considerando 26.

Ressalte-se que, a depender do tratamento conferido ao dado pessoal, ele pode perder essa característica e, portanto, sair do âmbito de proteção da legislação específica. Alguns procedimentos podem ser aptos a fazer com que o dado perca a identificabilidade, ao passo que outros, embora sejam importantes práticas para a proteção da privacidade, não são hábeis a impedir essa identificação.

Torna-se imperioso analisar até que ponto um dado pode ser considerado pessoal e se realmente há a possibilidade de se desvincular um dado pessoal de seu titular de forma irreversível, excluindo-o do alcance da tutela legal conferida aos dados pessoais. Para tanto, faz-se necessário diferenciar três desses métodos: a criptografia, a pseudonimização e a anonimização, verificando-se quais dessas técnicas afastam a aplicação da LGPD.

Criptografia, pseudonimização e anonimização: uma diferenciação necessária

A criptografia pode ser definida como uma técnica por meio da qual os dados são codificados e apenas aquele que tiver acesso à chave criptográfica pode decifrar aquela informação. No caso da criptografia ponta a ponta, somente emissor e destinatário têm acesso a essa chave e, como consequência, apenas eles podem ter acesso às informações enviadas e recebidas.[35]

A criptografia tem como objetivo assegurar um maior grau de segurança às comunicações ou transmissões de dados, minimizando ameaças advindas de pontos intermediários ou internos que se utilizem do mesmo serviço. Enfim, a criptografia visa a possibilitar maior grau de confidencialidade na troca de informações entre emissor e destinatário, dificultando o acesso a esses dados

35 MACHADO; DONEDA, *op. cit.*, p. 114

por pessoas que tentem o acesso de fora ou, ainda, por parte do próprio servidor da internet.[36]

Importa frisar, no entanto, que mesmo se o dado criptografado for interceptado por outrem, este terá dificuldade no acesso às informações criptografadas. Trata-se apenas de uma dificuldade e não de uma impossibilidade, pois, uma vez que existe uma chave, ela pode ser acessada e o processo de criptografia poderá ser revertido, verificando-se, aqui, a possibilidade de reidentificação do dado pessoal.

Já no que diz respeito à pseudonimização e à anonimização, ambos são métodos de tratamento que operam nos atributos de identificação, influindo na possibilidade de identificação de uma pessoa a partir de seus dados pessoais. Desse modo, somente a partir da análise do caso concreto, a depender do nível de dificuldade, tempo expendido, custos e atividades necessárias para identificar uma pessoa, é que poderá ser observado se estamos diante de pseudonimização ou da anonimização e, também, se as informações tratadas ou em tratamento são ou não dados pessoais.[37] Explica-se.

A pseudonimização é um instrumento utilizado para dificultar a identificação das pessoas no tratamento de dados pessoais.[38] Essa técnica se efetiva pela criação de pseudônimos, isto é, pela substituição de um atributo de um registro por outro.[39] Para essa substituição, pode-se recorrer à encriptação, ou seja, a dados encriptados, por meio de uma cifra, denominada chave criptográfica, conhecida apenas por quem está realizando o tratamento dos dados.[40]

Para que ocorra a pseudonimização, as informações do indivíduo não podem estar conectadas ao titular específico, a não ser que se

36 MACHADO; DONEDA, *op. cit.*, p. 114-115.

37 RIBEIRO, *op. cit.*, p. 55-56.

38 RIBEIRO, *op. cit.*, p. 59-60.

39 GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29°. *Parecer 05/2014 sobre as técnicas de anonimização*. [*S. l.*: *s. n.*], 2014. p. 22.

40 RIBEIRO, *op. cit.*, p. 59-60

recorra à utilização de informações suplementares, as quais devem ser mantidas separadas dos dados principais.[41] Desse modo, quando criados os pseudônimos, sua identidade não está associada a um indivíduo específico, a não ser que sejam reunidos condições e procedimentos que interliguem indivíduo e pseudônimo.[42] Verifica-se que aqui também há a possibilidade de a identificação do titular do dado vir a ocorrer.

Já a anonimização consiste na remoção ou na ofuscação de toda a informação pessoal de uma base de dados, com o objetivo de impedir a identificação dos indivíduos. Aplicam-se técnicas que pretendem tornar impraticável, ou razoavelmente impossível, a reidentificação, inclusive pelo próprio técnico que realizou a operação inicial.[43]

Para parte da doutrina, a pseudonimização se situaria num espaço entre o dado pessoal e o dado anônimo, submetendo-se ao regime de proteção conferido aos dados pessoais.[44] Tanto a LGPD quanto o RGPD tratam sobre a pseudonimização. Na LGPD, a pseudonimização é entendida como uma forma de tratamento de dados pessoais por meio do qual o dado não pode ser associado a um indivíduo, direta ou indiretamente, salvo pela utilização de informação suplementar mantida separadamente pelo responsável pelo tratamento, conforme disposto no artigo 13, § 4º, do referido diploma legal.

Por sua vez, o RGPD, em seu artigo 4º, 5, define a pseudonimização; já o Considerando 26 enfatiza que dados pessoais que tenham sido pseudonimizados, mas que possam ser atribuídos a um indivíduo específico por meio da utilização de informações suplementares, devem ser considerados "informações sobre uma pessoa singular identificável",

41 MACHADO; DONEDA, *op. cit.*, p. 112-113.

42 RIBEIRO, *op. cit.*, p. 60-61.

43 PINHO, Frederico A. S. O. *Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados*. 2017. Dissertação (Mestrado em Segurança Informática) – Departamento de Ciência de Computadores, Faculdade de Ciências, Universidade do Porto, Porto, 2017. p. 29.

44 MACHADO; DONEDA, *op. cit.*, p. 60-61.

ou seja, deverão ser considerados dados pessoais, sendo, portanto, abarcados pela tutela desse regulamento.

Como se vê, a pseudonimização deve ser entendida não como anonimização, senão como uma técnica que auxilia na proteção à privacidade, pois ela não serve para excluir dados de outras medidas de segurança, sendo até mesmo incentivadas medidas de cuidados com medidas técnicas e organizativas adequadas.[45]

O fato de não estarmos diante de dados irreversivelmente anonimizados não significa, no entanto, que criptografia e pseunimização devam ser rechaçadas, visto que se trata de meios de assegurar maior segurança e, consequentemente, auxiliam na proteção aos dados pessoais e ao direito à privacidade.

Em relação à anonimização, o RGPD traz sua definição em seu Considerando 26, por meio do qual aduz que os princípios nele previstos, bem como todas as suas disposições, não dizem respeito a dados anônimos, sendo entendidos como dados que não podem ser relacionados a um indivíduo identificado ou identificável. No mesmo sentido, a LGPD define dados anônimos em seu artigo 5º, III, dispondo que dados anonimizados devem ser entendidos como aqueles cujo titular não possa ser identificado. Ambos os conceitos levam em consideração a utilização de meios razoáveis e disponíveis quando do tratamento para anonimização desses dados.

Dessa forma, dados anônimos são aqueles que não podem ser relacionados a um indivíduo específico, seja exclusivamente por meio dos dados ou combinando-os com outros dados, podendo ser utilizados diversos instrumentos para tornar o dado anônimo, a exemplo da encriptação.[46] O objetivo da utilização da anonimização é justamente desvincular os dados de seu titular de forma

45 RIBEIRO, *op. cit.*, p. 60-61.

46 RIBEIRO, *op. cit.*, p. 59.

definitiva; seu fundamento é a proteção da privacidade do titular daqueles dados.[47]

A esse respeito, ainda, o Grupo de Trabalho do Artigo 29 da Diretiva 95/46/CE do Parlamento Europeu e do Conselho[48] emitiu parecer apresentando quatro características sobre anonimização: 1. impossibilidade de identificação do titular dos dados de forma irreversível; 2. a utilização de qualquer meio para alcançar a anonimização; 3. a razoabilidade dos meios para reidentificação deve ser avaliada no contexto em que se situam; e 4. anonimização e fator de risco caminham juntos.[49]

A importância de definir o que são dados anonimizados situa-se em dizer o que são dados pessoais ou não, visto que tanto a RGPD quanto a LGPD tutelam apenas dados pessoais, não alcançando dados que não se relacionem a um indivíduo identificado ou identificável. Dizer o que são dados anônimos significa dizer o que não são dados pessoais.

Quando tratamos de dados anonimizados, a reidentificação deve ser considerada impossível de ocorrer ou, no mínimo, só poderá ocorrer por meio de utilização de instrumentos que superem a razoabilidade de instrumentos considerados no contexto da época da anonimização. Deve ser afastada a identificabilidade ou o risco de identificabilidade do titular dos dados.[50]

47 MACHADO, Diego. Tutela jurídica da privacidade, anonimização de dados e anonimato na internet. *In*: POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves (org.). *Tecnologias e conectividade*: direito e política na governança das redes. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018. p. 276-277.

48 O Grupo de Trabalho do Artigo 29 da Diretiva 95/46/CE era um órgão consultivo europeu independente em matéria de proteção de dados e privacidade, cuja criação estava prevista no artigo 29 da mencionada Diretiva. O Grupo do Artigo 29 deixou de existir em 25 de maio de 2018 e foi substituído pelo Conselho Europeu de Proteção de Dados (EDPB), estabelecido pelo RGPD. Os documentos do Grupo de Trabalho do Artigo 29 podem ser encontrados em: https://ec.europa.eu/newsroom/article29/news-overview.cfm.

49 MACHADO, *op. cit.*, p. 282.

50 MACHADO, *op. cit.*, p. 282.

Não estando mais conectados a uma pessoa identificada e não sendo mais possível que ocorra a identificação dessa pessoa, o dado pessoal submetido à anonimização perde sua característica de dado pessoal e, por consequência, afasta-se da tutela pelos dispositivos legais, a exemplo da RGPD e da LGPD. No entanto, isso não significa que ficarão nessa condição para sempre.

Anonimização: entre riscos e benefícios

Estima-se que, até 2020, sejam criadas para cada pessoa em torno de 1,7 megabyte de novas informações por minuto e que se ultrapasse o volume de 40 zettabytes (o que equivale a 40 trilhões de gigabytes) de dados armazenados[51] em todo o mundo. Esses dados adquirem bastante relevância, pois seu tratamento adequado pode trazer muitos benefícios para o desenvolvimento da sociedade.

A enorme quantidade de dados produzida diariamente pelos estabelecimentos de saúde, por exemplo, pode ser tratada, analisada e utilizada para que os médicos tenham mais informações sobre os avanços das doenças e os melhores tratamentos, salvem vidas e melhorem a qualidade de vida de diversos pacientes.

Por sua vez, os milhares de gigabytes gerados diariamente pelas movimentações financeiras são analisados tanto para a identificação de atividades comerciais problemáticas, prevenindo fraudes, como para ajudar empresas a crescer e a fortalecer a economia.[52] Os dados também são de grande importância nas análises estatísticas utilizadas pelos governos para a elaboração dos seus planos de desenvolvimento, permitindo estimar, com um bom grau de precisão, relevantes variáveis

51 MARR, Bernard. 20 fatos sobre a internet que você (provavelmente) não sabe. *Forbes*, New York, 1 out. 2015.

52 BUSINESS SOFTWARE ALLIANCE. *Qual é o "x" da questão em relação a dados?* London: BSA, 2015. p. 8.

como tamanho da população, taxa de emprego e desemprego e índices de inflação.[53]

Esses são somente alguns dos exemplos da relevância dos dados para a sociedade da informação. Impedir o tratamento desses dados significa obstaculizar o desenvolvimento da sociedade.

Obviamente, nem todos os dados produzidos são dados pessoais. Existem dados, por exemplo, que são produzidos pelo monitoramento climático por satélite ou pelo desempenho de turbinas de aviões e que não se relacionam com nenhuma pessoa natural identificável. No entanto, parcela bastante considerável dos dados produzidos são dados pessoais. A esse respeito, importa ressaltar que a maior parte das legislações sobre proteção de dados exige o consentimento do titular para que os dados sejam objeto de tratamento.[54]

Assim, aquele que pretende armazenar, tratar os dados pessoais e compartilhá-los deverá obter consentimento expresso dos titulares dessas informações. Na atualidade, em que a produção e o fluxo de dados são imensos, atender a essa obrigação nem sempre será tarefa fácil. Acontece que, como visto, o tratamento e o compartilhamento de dados não é algo que seja, por si mesmo, ruim. Os dados são hoje indispensáveis ao desenvolvimento da sociedade e o seu tratamento pode propiciar diversos benefícios às pessoas.

É claro que na era do *big data* crescem os riscos à privacidade, no entanto, faz-se necessário ter em mente que, nesse contexto, não existem somente perigos ou apenas benefícios. É possível que o uso das informações e a privacidade dos titulares de dados não estejam em lados opostos, mas convirjam para que as pessoas possam se beneficiar do uso de suas informações sem ter seus direitos violados.

53 IGNÁCIO, Sérgio Aparecido. Importância da estatística para o processo de conhecimento e tomada de decisão. *Revista Paranaense de Desenvolvimento*, Curitiba, n. 118, p. 1-17, 2010.

54 Nesse sentido, artigo 7°, I, da Lei Geral de Proteção de Dados Pessoais.

Nesse ponto reside a importância das legislações sobre a proteção dos dados pessoais: permitir o uso responsável das informações de modo a compatibilizar direitos fundamentais dos titulares dos dados com a utilização destes pelos agentes de tratamento. Entender a correta aplicação da LGPD bem como sua abrangência material é fundamental para impedir que se pense que a lei é um entrave a tudo, solicitando-se novos pedidos de consentimento que não sejam necessários, máxime porque seria impraticável exigir o consentimento para todas as situações de tratamento de dados.

A anonimização desponta como uma importante alternativa àqueles que precisarem coletar e tratar dados pessoais, além de ser um relevante mecanismo de proteção da privacidade dos indivíduos. Ademais, as pessoas podem se mostrar mais dispostas a revelar mais dados se elas acreditarem que seus dados serão anonimizados.[55]

Como visto, por meio do processo de anonimização busca-se desvincular as informações identificativas contidas numa base de dados das pessoas a quem estas informações se referem. Essa prática fundamenta-se na proteção à privacidade da pessoa ou grupos de pessoas cujos dados serão anonimizados.[56]

Por décadas, acreditou-se que a privacidade poderia ser protegida a partir do emprego de técnicas simples de anonimização, ao tempo que a utilidade dos dados seria preservada, de modo que hoje a anonimização é onipresente.[57] Nesse contexto, "a crença na idoneidade da anonimização [...] se espraia por diversos ordenamentos jurídicos, de

55 HARGITAI, Viktor; SHKLOVSKI, Irina; WASOWSKI, Andrzej. *Going Beyond Obscurity*: organizational approaches to Data Anonymization. *Proceedings of the ACM on Human-Computer Interaction*, New York, v. 2, nov. 2018.

56 MACHADO, *op. cit.*, p. 276

57 OHM, Paul. Broken Promises of Privacy: *res*ponding to the surprising failure of anonymization. *UCLA Law Review*, Los Angeles, n. 1.701, p. 1701-1777 2010. p. 1706.

sorte a tornar-se parte integrante de leis de proteção da privacidade e de dados pessoais mundo afora".[58]

Apesar disso, a anonimização não é livre de riscos. Assim, alguns pesquisadores veem a anonimização como a chave para permitir o uso justo de dados pessoais, ao passo que outros atentam às suas falhas.

Os riscos da reidentificação

Os críticos da anonimização afirmam que uma base de dados anonimizados sempre poderá ser combinada com outras bases de dados e essa agregação poderá levar à reidentificação dos dados. É o que se chama de entropia da informação.[59]

A esse respeito, Bruno Bioni comenta que, com o crescimento da cultura do *open data*, nossas vidas têm sido cada vez mais datificadas e nossas informações, dispersas e publicamente acessíveis na rede. A crescente interação das pessoas com o mundo *on-line* cria uma biografia digital de suas vidas que é compartilhada com inúmeros indivíduos que fazem parte desses "relacionamentos *on-line*".[60]

Nessa senda, Paul Ohm alerta, ainda, para o problema que ele denomina de "*accretion problem*": uma vez que um adversário[61] tenha vinculado dois bancos de dados anonimizados, ele pode utilizar essas novas informações para abrir outros bancos de dados anônimos. Por conseguinte, eventos de reidentificação que exponham apenas informações não sensíveis também devem ser objeto de preocupação, haja vista que tais informações aumentam a capacidade de vinculação dos dados, o que expõe as pessoas a um potencial dano futuro.[62]

58 MACHADO, *op. cit.*, p. 276.

59 OHM, *op. cit.*, p. 1.749.

60 BIONI, *op. cit.*, p. 29.

61 Essa é a expressão correntemente utilizada na literatura científica para designar aquele que busca a reidentificação.

62 OHM, *op. cit.*, p. 1746.

Arvind Narayanan e Vitaly Shmatikov afirmam que há um amplo espectro de características humanas que permitem reidentificação, como preferências de consumo, transações comerciais, navegação na *web* e históricos de pesquisa.[63] Por essa razão, para os autores:

> A versatilidade e o poder dos algoritmos de reidentificação implicam que termos como 'pessoalmente identificável' e 'quase-identificadores' simplesmente não têm significado técnico. Enquanto alguns atributos podem identificar unicamente por si próprios, qualquer atributo pode ser um identificador em combinação com os outros. Considere, por exemplo, os livros que uma pessoa leu ou até mesmo as roupas em seu guarda-roupa: embora nenhum elemento seja um (quase)-identificador, qualquer subconjunto suficientemente grande identifica exclusivamente o indivíduo.[64]

Para *ilustrar* como os dados anonimização são suscetíveis de reidentificação, apresentam-se alguns casos a seguir.

Netflix Prize

No ano de 2006, a Netflix lançou o *Netflix Prize*, por meio do qual oferecia um prêmio de $ 1.000.000,00 (um milhão de dólares), desafiando os concorrentes a aprimorarem seu algoritmo de recomendação de filmes (*Cinematch*). Para a realização da competição foram disponibilizadas avaliações de usuários dos serviços da empresa, coletados entre 1999 e 2005, os quais haviam sido submetidos à anonimização, segundo sua política de privacidade em vigor à época do tratamento

63 NARAYANAN, Arvind; SHMATIKOV, Vitaly. Privacy and Security: myths and fallacies of "Personally Identifiable Information". *Communications of the ACM*, New York, v. 53, n. 6, 2010.

64 NARAYANAN; SHMATIKOV, *op. cit.*, p. 26, tradução nossa.

dos dados. Foram disponibilizados, ao todo, mais de 100 milhões de avaliações feitas por mais de 480 mil assinantes da Netflix.[65]

Por meio do acesso aos dados disponibilizados pela Netflix, pesquisadores da Universidade do Texas realizaram um estudo que teve como objetivo verificar a técnica utilizada pela Netflix para a anonimização dos dados publicados de seus usuários. Como resultado, o estudo chegou às seguintes conclusões:

> Resultado do estudo: com oito avaliações de filmes – das quais se permitiu que duas fossem completamente erradas – e datas – com erro de até três dias, 96% dos consumidores da Netflix cujos registros foram lançados no conjunto dos dados puderam ser identificados de forma exclusiva; para 64% dos clientes, o conhecimento de apenas duas das avaliações e data foi suficiente para a desanonimização total. Além disso, se os filmes em questão não estiverem entre os cem mais bem classificados, então mesmo com um erro de 14 dias nas datas, o conhecimento aproximado de oito classificações (duas das quais estão erradas) reidentifica inteiramente 80% dos consumidores na base de dados.[66]

A reidentificação dos consumidores dos serviços da Netflix foi possível por meio do cruzamento de informações com uma plataforma de avaliações de filmes semelhante à Netflix, na qual os titulares dos dados também postavam suas avaliações. Com o auxílio de dados complementares, o anonimato, anunciado com segurança, foi violado.[67]

Compras no cartão de crédito

Trata-se de um estudo realizado pelo Instituto Tecnológico de Massachusetts (MIT) com o objetivo de analisar o poder dos metadados

65 NARAYANAN; SHMATIKOV, *op. cit.*, p. 1.

66 MACHADO, *op. cit.*, p. 277.

67 MACHADO, *op. cit.*, p. 277.

e do *big data*, visando a verificar a efetividade da anonimização das informações contidas em metadados. No estudo foram analisados dados de cartões de créditos de mais de um milhão de pessoas, demonstrando que quatro compras são suficientes para reidentificar os indivíduos em 90% dos casos.[68]

O estudo foi realizado utilizando-se dados cedidos por um responsável pelo tratamento dos dados dos titulares dos cartões de crédito, com garantia de sigilo por parte dos pesquisadores. Não se referem a dados pessoais, a princípio, ou dados que tratem da intimidade de seus titulares. Embora tivessem acesso aos dados dos cartões (titulares, números etc.), os pesquisadores optaram por realizar o estudo sem acessar esses dados, utilizando-os, posteriormente, apenas para conferir os resultados alcançados pelo estudo. Dessa forma, com metadados, informações genéricas, foi possível fazer o caminho inverso da anonimização e alcançar os titulares dos dados, evidenciando a fragilidade do processo de anonimização.[69]

Identificação dos estadunidenses

Trata-se de estudo realizado por Latanya Sweeney, durante a década de 1990, nos Estados Unidos da América. Sweeney é cientista da computação na Universidade de Harvard. O objetivo da pesquisa foi testar a segurança dos processos de anonimização de dados pessoais.

A pesquisa foi realizada por meio do cruzamento de informações anonimizadas de saúde da população estadunidense com uma lista de dados referentes a eleitores cadastrados para votar. O cruzamento de poucas características, a exemplo de código postal, data de nascimento e sexo, permitiu reidentificar os indivíduos, titulares dos dados

68 MONTJOYE, Yves-Alexandre; RADAELLI, Laura; SINGH, Vivek; PENTLAND, Alex. Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, London, v. 347, n. 6221, p. 536-539, 2015.

69 MONTJOYE; RADAELLI; SINGH; PENTLAND, *op. cit.*

pessoais de saúde, de forma simples e muito precisa, resultando na possibilidade de identificação dos titulares de dados pessoais anonimizados em 87% dos casos, utilizando-se indicadores simples (código postal, data de nascimento e sexo). A reidentificação foi possível em 50% dos casos apenas pela utilização de lugar, sexo e data de nascimento (sem código postal) e em 18% dos casos, restringindo-se o condado do indivíduo, a reidentificação torna-se possível.[70]

No caso do estudo em comento, a autora utilizou informações que estavam sendo comercializadas pela indústria de saúde, dados estes que não continham nomes, endereços ou número de Seguro Saúde dos indivíduos, mas continham informações sobre diagnósticos, doenças sexualmente transmissíveis (DST), uso de drogas, além de data de nascimento, sexo e código postal. As informações, em si, podem ser consideradas dados pessoais sensíveis, mas foram submetidas a tratamento para anonimização, de modo a não ser possível conectá-las aos seus titulares.[71]

Os dados pessoais sensíveis do sistema de saúde foram cruzados com dados adquiridos pela pesquisadora por apenas 20 dólares, uma lista de eleitores de determinada localidade, a qual continha dados como data de nascimento, sexo e código postal.[72] Dessa forma, com dados genéricos de duas listas distintas, foi possível reidentificar os titulares dos dados da primeira lista, a qual continha dados sensíveis, e associar a eles esses dados, violando sua privacidade.

Jane Yakowitz, embora não negue que realmente exista o risco da reidentificação, afirma que a utilidade social dos dados é muito desvalorizada pelos estudiosos da privacidade, bem como que estes riscos são insignificantes, não havendo ocorrências conhecidas de reidentificação indevida de um conjunto de dados de pesquisa. Para a

70 SWEENEY, Latanya. Simple demographics often identify people uniquely. *Carnegie Mellon University*, Pittsburgh, 2000.

71 ADVICE to my younger self: Latanya Sweeney. *Ford Foundation*, [*s. l.*], 12 mar. 2019.

72 ADVICE to my younger self: Latanya Sweeney. *Ford Foundation*, [*s. l.*], 12 mar. 2019.

autora, os riscos relacionados aos dados anonimizados são menores que outros riscos relacionados à informação, como o vazamento de dados e a pirataria, riscos estes que, por conveniência, são tolerados.[73]

Yakowitz aduz, ainda, que, caso se presuma que a anonimização dos dados é impossível, o futuro dos dados abertos e toda a sua utilidade social serão postos em questão, o que fará com que os indivíduos não queiram fornecer seus dados. Contudo, quase todos os debates recentes sobre políticas públicas se beneficiaram da disseminação em massa de dados anônimos.[74]

Nesse sentido, o Parecer 5/2014, do Grupo de Trabalho de Proteção de Dados do Artigo 29º, afirma que nenhuma técnica analisada no documento satisfaz completamente os critérios de anonimização eficaz, entretanto, os resultados das técnicas podem ser robustecidos por meio de um planejamento meticuloso na definição de qual técnica será utilizada, tendo em vista as peculiaridades da situação específica, bem como por meio da combinação de técnicas.[75] Assim, conclui que "as técnicas de anonimização podem fornecer garantias de privacidade e podem ser utilizadas para gerar processos eficazes de anonimização, mas apenas se a sua aplicação for adequadamente construída".[76]

O fato é que as legislações e os debates jurídicos sobre proteção de dados não têm ficado alheios aos riscos da reidentificação dos dados anonimizados, assim como também não são desprezados todos os benefícios que os dados anônimos proporcionam à sociedade. Nesse sentido, tanto a LGPD quanto o RGPD buscaram equilibrar essa questão a partir do critério da razoabilidade dos meios que podem ser utilizados para a reversão do processo de anonimização.

73 BAMBAUER, Jane R. Tragedy of the data commons. *Harvard Journal of Law and Technology*, Cambridge, v. 25, 19 mar. 2011. p. 4.

74 BAMBAUER, *op. cit.*, p. 9.

75 GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29°, *op. cit.*, p. 26.

76 GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29°, *op. cit.*, p. 34.

Dessa feita, "a função da anonimização deixa de ser determinada pela lógica do tudo ou nada",[77] de forma que não é a aplicação de uma técnica de anonimização que, por si só, dispensará a aplicação das normas de proteção de dados. Havendo uma potencial identificabilidade do titular dos dados diante dos meios existentes de serem razoavelmente utilizados para tanto ou existindo um inaceitável risco da identificabilidade do dado, o ente responsável deverá cumprir os princípios e regras do direito de proteção dos dados pessoais.[78]

O critério da razoabilidade e a necessidade de uma definição contextual de dados anonimizados

A LGPD reconhece que as técnicas de anonimização são, em algum grau, falíveis, de modo que sempre existirá a possibilidade de que um dado seja atrelado a um indivíduo específico. No entanto, uma vez que esse fato poderia expandir imensuravelmente o espectro de incidência do conceito amplo de dados pessoais, há a necessidade de se estabelecer um filtro a fim de que nem toda e qualquer possibilidade seja suficiente para que se considere o dado identificável e, portanto, pessoal.[79]

Uma lei cujo conceito de dado pessoal se expandisse de tal forma tornar-se-ia "a lei de tudo", mas na prática seria muito difícil o seu cumprimento. Se não houvesse esse filtro, isso significaria que não existiriam dados anônimos, o que implicaria grandes obstáculos aos avanços tecnológicos e às vantagens que estes avanços podem proporcionar ao desenvolvimento da sociedade. Assim,

77 MACHADO, *op. cit.*, p. 282.

78 MACHADO, *op. cit.*, p. 282.

79 BIONI, *op. cit.*, p. 32.

> o critério da razoabilidade nada mais é do que uma diretriz acerca do que venha a ser um risco aceitável em torno da reversibilidade do processo de anonimização, a fim de que os dados anonimizados estejam fora do conceito de dados pessoais".[80]

A esse respeito, a Lei nº 13.709/2018, em seu artigo 12, dispõe que os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Além disso, estabelece que a determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. Essa definição do que seja razoável está de acordo com o Considerando 26 do RGPD.[81]

O contexto e as circunstâncias de um caso concreto influenciam diretamente a identificabilidade. A investigação, as ferramentas e as capacidades da tecnologia evoluem, razão por que não seria viável nem útil especificar, num rol taxativo, todas as hipóteses em que a identificação deixa de ser possível.[82] Não há uma unidade de medida para avaliar previamente o tempo ou o esforço necessários para a reidentificação após o tratamento dos dados.[83]

80 BIONI, *op. cit.*, p. 32.

81 Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de serem razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica.

82 GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29°, *op. cit.*, p. 9.

83 GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29°, *op. cit.*, p. 30.

Posto isso, o critério para conceituar determinado dado como anonimizado é a segurança da preservação da sua dissociação em relação aos titulares, o que envolve um exame das tecnologias e alternativas disponíveis.[84]

A LGPD, em seu artigo 12, §3º, estabeleceu que a autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais. Assim, na LGPD, quem dirá o que é ou não razoável será a Autoridade Nacional.

O Grupo de Trabalho de Proteção de Dados do Artigo 29º da Diretiva 95/46/CE, em seu Parecer 5/2014, sugere que, além dos meios, deve-se avaliar a probabilidade e a gravidade da identificação. Ademais, este Parecer apresenta importante reflexão acerca da obrigação do terceiro que fará o tratamento de dados anonimizados: os terceiros devem considerar os fatores contextuais e circunstanciais, incluindo as características específicas das técnicas de anonimização de dados pessoais aplicadas pelo responsável pelo tratamento de dados inicial, ao decidir como utilizar e, em especial, combinar tais dados anonimizados para fins próprios, de modo que sempre que tais fatores e características implicarem um risco inaceitável de identificação dos titulares dos dados, o tratamento deverá se sujeitar à legislação de proteção de dados.[85]

Considerações finais

Os dados pessoais são uma extensão da nossa personalidade e, por isso, merecem ser tutelados, sendo a proteção desses dados um direito fundamental. Como visto, existe um conceito amplo e um restrito de dado pessoal. A LGPD adotou a acepção ampla, de modo que os

84 FRAZÃO, Ana. *A nova Lei Geral de Proteção de Dados*. [*S. l.: s. n.*], 2018. p. 4.

85 GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29°, *op. cit.*, p. 11.

dados pessoais são aqueles relacionados a uma pessoa identificada ou identificável.

Os dados pessoais que podem ser utilizados com finalidades discriminatórias são classificados como sensíveis e recebem tratamento específico da legislação. Entretanto, para que a tutela desses dados pessoais seja adequada, faz-se necessário que a classificação de um dado como sensível ou não sensível seja dinâmica e contextual, considerando o uso que se fará dos dados e quais as inferências que se pode obter a partir deles.

A utilização dos dados pessoais traz inúmeros benefícios à sociedade, por outro lado, na sociedade da informação crescem os riscos de danos à privacidade dos indivíduos. Privacidade e avanços tecnológicos devem coexistir, uma vez que impedir o tratamento dos dados pessoais significa obstaculizar o desenvolvimento da sociedade. Nesse ponto reside a importância das legislações sobre a proteção dos dados pessoais: permitir o uso responsável das informações sem, contudo, tornar-se um entrave a tudo.

Existem métodos de tratamentos que visam à proteção da privacidade dos titulares dos dados, como a codificação, a pseudonimização e a anonimização. Desses métodos, apenas a anonimização faz, de maneira eficaz, com que um dado perca a possibilidade de associação, direta ou indireta, a um indivíduo, tendo em conta a razoabilidade dos meios possíveis de serem utilizados para reidentificar esses dados.

Dito isso, a anonimização desponta como uma importante alternativa àqueles que precisarem coletar e tratar dados pessoais, uma vez que afasta a aplicabilidade da LGPD e permite a utilização dos dados sem lesionar a privacidade dos indivíduos. Entretanto, a anonimização é falível, existindo o risco da reidentificação. Atentas a isso, mas também tendo em vista todos os benefícios que os dados anonimizados proporcionam à sociedade, as legislações, a exemplo da LGPD, buscam equilibrar essa questão a partir do critério da

razoabilidade dos meios que podem ser utilizados para a reversão do processo de anonimização.

No entanto, cabe aqui uma crítica. Tendo em vista os riscos inerentes à anonimização, excluir os dados anonimizados de qualquer proteção conferida pela LGPD não se mostrou a técnica legislativa mais adequada.

É claro que se exigir sempre o consentimento para a utilização dos dados anonimizados seria um entrave muito grande às inovações tecnológicas. Contudo, exigir dos responsáveis pelo tratamento de dados anônimos certas práticas conferiria mais proteção aos direitos fundamentais tutelados pela LGPD, de forma a garantir mais efetividade da legislação sem obstaculizar os avanços tecnológicos.

Nesse sentido, a LGPD poderia ter previsto, no setor privado, a publicidade do compartilhamento e uso que se faz dos dados anônimos, para que as pessoas e a Autoridade Nacional pudessem ter ciência e controle do que acontece com os dados depois de anonimizados.

Além disso, uma vez que as evoluções tecnológicas podem tornar uma técnica de anonimização falha, permitindo que a identificabilidade aconteça sem maiores esforços, um dado anonimizado pode voltar a ser um dado pessoal. Por essa razão, a Autoridade Nacional, ao dispor sobre os padrões e técnicas utilizados em processos de anonimização, bem como ao realizar verificações acerca de sua segurança, deverá levar em conta que a caracterização de um dado como anonimizado deve ser contextual.

Assim, caberá à Autoridade Nacional estabelecer procedimentos que sejam capazes de identificar novos riscos de reidentificação, bem como reavaliar, regularmente, a razoabilidade de utilização dos meios para os riscos já identificados. A Autoridade Nacional deverá avaliar, regularmente, se as medidas de segurança adotadas pelas organizações para os riscos identificados são suficientes. Essas medidas são necessárias para que, ao se verificar que o risco de reidentificação não é mais tolerável, os dados sejam imediatamente considerados pessoais

e a LGPD lhes seja aplicável, permitindo que a privacidade das pessoas continue segura mesmo com a evolução das tecnologias.

A Lei nº 13.709/2018 tutelaria de uma melhor forma a privacidade das pessoas se não houvesse excluído completamente os dados anonimizados de seu escopo e, pelo contrário, tivesse exigido das organizações que manipulam dados anonimizados uma série de medidas para prevenir a reidentificação ou minimizar seus efeitos, responsabilizando os terceiros que lidassem com esses dados em caso de identificabilidade.

Entretanto, como a LGPD preferiu excluir os dados anonimizados de sua abrangência material, caberá à Autoridade Nacional, dentro de suas competências, adotar medidas que protejam os brasileiros dos riscos da reidentificação.

Em que pesem as críticas, as técnicas de anonimização, quando bem aplicadas, podem fornecer garantias de privacidade eficazes, não havendo ocorrências conhecidas de reidentificação indevida de um conjunto de dados de pesquisa. Dessa forma, o risco da reidentificação pode ser tolerado, haja vista que são muito menores que todos os benefícios que os dados anonimizados proporcionam à sociedade.

Assim, a anonimização dos dados pessoais pode ser vista como o caminho para que a privacidade e a utilização dos dados coexistam, de modo a se permitir que os direitos fundamentais dos indivíduos sejam assegurados sem, contudo, obstaculizarem os avanços tecnológicos e a nova economia.

Referências

ADVICE to my younger self: Latanya Sweeney. *Ford Foundation*, New York, 12 mar. 2019. Disponível em: https://www.fordfoundation.org/ideas/equals-change-blog/posts/advice-to-my-younger-self-latanya-sweeney/. Acesso em: 12 jun. 2019.

ARAÚJO, Alexandra Maria Rodrigues. As transferências transatlânticas de dados pessoais: o nível de proteção adequado depois de *Schrems*. *Revista Direitos Humanos e Democracia*, Unijuí, RS, v. 5, n. 9, p. 201-236, 2017. Disponível em: https://www.revistas.unijui.edu.br/index.php/direitoshumanosedemocracia/article/view/6058. Acesso em: 12 jun. 2019.

BAMBAUER, Jane R. Tragedy of the data commons. *Harvard Journal of Law and Technology*, Cambridge, v. 25, p. 1-67, 2011. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749. Acesso em: 9 jun. 2019.

BIONI, Bruno R. Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. *Privacidade e Vigilância*, São Paulo, 2015. Disponível em: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 12 jun. 2019.

BRASIL. http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2013.709-2018?OpenDocument Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 12 jun. 2019.

BRASIL. *Proposta de Emenda à Constituição nº 17, de 2017*. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, DF: Senado Federal, 2017. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1567535523044&disposition=inline. Acesso em: 25 set. 2019.

BUSINESS SOFTWARE ALLIANCE. *Qual é o "x" da questão em relação a dados?* London: BSA, 2015. Disponível em: https://data.bsa.org/wp-content/uploads/2015/10/BSADataStudy_br.pdf. Acesso em: 11 jun. 2019.

CONSELHO DA EUROPA PARA A PROTEÇÃO DAS PESSOAS SINGULARES. *Convenção nº 108, de 1981*. Tratamento Automatizado de Dados Pessoais. [União Europeia],1981. Disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 25 set. 2019.

DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, 2011. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 12 jun. 2019.

ENTENDA o escândalo de uso político de dados que derrubou valor do *Facebook* e o colocou na mira de autoridades. *BBC News*, London, 20 mar. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 11 jun. 2019.

FRAZÃO, Ana. *A nova Lei Geral de Proteção de Dados*. [*S. l.: s. n.*], 2018. Disponível em: http://anafrazao.com.br/files/publicacoes/2018-09-05-A_nova_Lei_Geral_de_Protecao_de_Dados_Repercussoes_para_a_atividade_empresarial_o_alcance_da_LGPD_Parte_II.pdf. Acesso em: 12 jun. 2019.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29º. *Parecer 5/2014 sobre as técnicas de anonimização*. [*S. l.: s. n.*], 2014. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf. Acesso em: 10 jun. 2019.

HARGITAI, Viktor; SHKLOVSKI, Irina; WASOWSKI, Andrzej. Going Beyond Obscurity: organizational approaches to Data Anonymization. *Proceedings of the ACM on Human-Computer Interaction*, New York, v. 2, 2018. Disponível em: https://dl.acm.org/citation.cfm?id=3274335.
Acesso em: 12 jun. 2019.

IGNÁCIO, Sérgio Aparecido. Importância da estatística para o processo de conhecimento e tomada de decisão. *Revista Paranaense de Desenvolvimento*, Curitiba, n. 118, 2010. Disponível em: http://www.ipardes.gov.br/biblioteca/docs/NT_06_importancia_estatistica_tomada_decisao.pdf. Acesso em: 11 jun. 2019.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. *PNAS*, [*s. l.*], v. 110, n. 15, p. 5802–5805, 2013. Disponível em: https://www.pnas.org/content/pnas/110/15/5802.full.pdf. Acesso em: 12 jun. 2019.

MACHADO, Diego. Tutela jurídica da privacidade, anonimização de dados e anonimato na internet. *In*: POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves (org.). *Tecnologias e conectividade: direito e política na governança das redes*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018. p. 272-285. Disponível em: https://www.researchgate.net/publication/328784970_Tutela_juridica_da_privacidade_anonimizacao_de_dados_e_anonimato_na_internet. Acesso em: 12 jun. 2019.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*, São Paulo, v. 998, p. 99-128, 2018, Caderno Especial. Disponível em: https://www.researchgate.net/publication/330401277_Protecao_de_dados_pessoais_e_criptografia_tecnologias_criptograficas_entre_anonimizacao_e_pseudonimizacao_de_dados. Acesso em: 12 jun. 2019.

MARR, Bernard. 20 fatos sobre a internet que você (provavelmente) não sabe. *Forbes*, New York, 1 out. 2015. Disponível em: https://forbes.uol.com.br/fotos/2015/10/20-fatos-sobre-a-internet-que-voce-provavelmente-nao-sabe/. Acesso em: 12 jun. 2019.

MAYER, Jonathan; MUTCHLER, Patrick. MetaPhone: The Sensitivity of Telephone Metadata. *Web Policy*, [*s. l.*], 12 mar. 2014. Disponível em: http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/. Acesso em: 12 jun. 2019.

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

MENEZES NETO, Elias J.; MORAIS, José Luis B.; BEZERRA, Tiago José S. L. O projeto de Lei de Proteção de Dados Pessoais (PL 5.276/2016) no mundo do Big Data: o fenômeno da Dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. *Revista Brasileira de Políticas Públicas*, Brasília, DF, v. 7, n. 3, p. 185-200, 2017. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4840. Acesso em: 12 jun. 2019.

MONTJOYE, Yves-Alexandre; RADAELLI, Laura; SINGH, Vivek; PENTLAND, Alex. Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, London, v. 347, n. 6221, p. 536-539, 2015. Disponível em: https://www.researchgate.net/publication/271591449_Unique_in_the_shopping_mall_On_the_reidentifiability_of_credit_card_metadata. Acesso em: 12 jun. 2019.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, p. 159-180, 2018. Disponível em: http://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 12 jun. 2019.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Privacy and Security: myths and fallacies of "Personally Identifiable Information". *Communications of the ACM*, New York, v. 53, n. 6, jun. 2010. Disponível em: https://pdfs.semanticscholar.org/44f3/2957fd4cdd2633b6d0cb744b3461f1b73124.pdf. Acesso em: 12 jun. 2019.

OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, Los Angeles, n. 1.701, p. 1701-1777, 2010. Disponível em: https://www.uclalawreview.org/pdf/57-6-3.pdf. Acesso em: 12 jun. 2019.

PASSOS, Bruno Ricardo dos Santos. *O Direito à Privacidade e a Proteção aos Dados Pessoais na Sociedade da Informação*: uma abordagem acerca de um novo direito fundamental. 2017. Dissertação (Mestrado em Direito Público) – Programa de Pós-Graduação em Direito da Universidade Federal da Bahia, Salvador, 2017. Disponível em: https://repositorio.ufba.br/ri/handle/ri/22478. Acesso em: 12 jun. 2019.

PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. *Revista Brasileira de Direito Civil*, Belo Horizonte, v. 16, p. 35-56, 2018. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/230. Acesso em: 12 jun. 2019.

PEZZELLA, Maria Cristina Cereser; GHISI, Silvano. A manipulação de dados pessoais nas relações de consumo e o sistema "*crediscore*". *Civilista.com*, Rio de Janeiro, v. 4, n. 1, p. 1-31, 2015. Disponível em: http://civilistica.com/a-manipulacao-de-dados-pessoais/. Acesso em: 12 jun. 2019.

PINHO, Frederico A. S. O. *Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados*. 2017. Dissertação (Mestrado em Segurança Informática) – Departamento de Ciência de Computadores, Faculdade de Ciências, Universidade do Porto, Porto, 2017. Disponível em: https://cracs.fc.up.pt/sites/default/files/MSI_Dissertacao_FINAL.pdf. Acesso em: 12 jun. 2019.

PSICÓLOGO que criou aplicativo da Cambridge Analytica acreditava que sistema era legal. *O Globo*, São Paulo, 21 mar. 2018. Disponível em: https://oglobo.globo.com/mundo/psicologo-que-criou-aplicativo-da-cambridge-analytica-acreditava-que-sistema-era-legal-22510640. Acesso em: 11 jun. 2019.

RIBEIRO, Florbela da Graça Jorge da Silva. *O tratamento de dados pessoais de clientes para marketing*. 2017. Dissertação (Mestrado em Direito, Especialidade em Ciências Jurídico-Políticas) – Departamento de Direito, Universidade Autónoma de Lisboa, Lisboa, 2017. Disponível em: https://www.academia.edu/33292289/O_TRATAMENTO_DE_DADOS_PESSOAIS_DE_CLIENTES_PARA_MARKETING. Acesso em: 12 jun. 2019.

ROCHA, Luiz A. C. B. L. M. da; FILPO, Klever P. L. Proteção do direito a vida privada na sociedade da hiperexposição: paradoxos e limitações empíricas. *Civilista.com*, Rio de Janeiro, ano 7, n. 1, p. 1-31, 2018. Disponível em: http://civilistica.com/protecao-do-direito-a-vida-privada/. Acesso em: 12 jun. 2019.

RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SWEENEY, Latanya. Simple demographics often identify people uniquely. *Carnegie Mellon University*, Pittsburgh, *Data Privacy Working Paper 3*, 2000. Disponível em: https://dataprivacylab.org/projects/identifiability/paper1.pdf. Acesso em: 12 jun. 2019.

UNIÃO EUROPEIA. *Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados). Europa: União Europeia, 2016. Disponível em: https://protecao-dados.pt/wp-content/uploads/2017/07/Regulamento-Geral-Prote%C3%A7%C3%A3o-Dados.pdf. Acesso em: 12 jun. 2019.

WAKABAYASHI, Daisuke. Google and the University of Chicago are sued over data sharing. *The New York Times*, New York, 26 jun. 2019. Disponível em: https://www.nytimes.com/2019/06/26/technology/google-university-chicago-data-sharing-lawsuit.html. Acesso em: 27 jun. 2019.

A DISCRIMINAÇÃO ALGORÍTMICA E AS NOVAS PERSPECTIVAS SOBRE O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Diego Carneiro Costa

Introdução

A sociedade atual atravessa uma mudança radical em seus princípios de organização, fruto da difusão das tecnologias da informação e comunicação (TIC), do uso das modernas técnicas de inteligência artificial (IA), como o *machine learning* e o *deep learning*, e do advento do fenômeno do *big data*.

Atualmente, boa parte da vida cotidiana passou a ser regida por dados e controlada por algoritmos, que estão, paulatinamente, substituindo o ser humano na tomada de decisões importantes. Cada vez mais, tanto as empresas, visando vantagens competitivas através da otimização de seus processos decisórios internos, como a administração pública, visando implementar uma gestão mais eficiente, passaram a delegar a sistema inteligentes a tomada de decisões que influenciam a vida das pessoas.

Nesse contexto, é necessário destacar que se por um lado a delegação de capacidade decisória às máquinas oferece melhorias significativas no que tange à eficiência e acurácia dos processos internos, por outro, pode implicar riscos significativos à garantia dos direitos

humanos e fundamentais dos indivíduos. Conforme será demonstrado ao longo deste trabalho, evidências empíricas apontam que os algoritmos de IA, sobretudo os de *machine learning* e *deep learning*, podem conter vieses capazes de reproduzir e até amplificar os preconceitos sociais já existentes, sobretudo contra minorias e grupos vulneráveis.

Ademais, tendo-se em conta que a maioria das decisões automatizadas envolvem não só a utilização das modernas técnicas de IA, mas também o processamento de uma imensa quantidade de dados, inclusive dados pessoais sensíveis, as questões jurídicas nos processos algorítmicos perpassam necessariamente pela análise das normas de proteção de dados pessoais.

A partir dessas premissas, o presente capítulo pretende analisar o arcabouço normativo de proteção aos dados pessoais no contexto das decisões algorítmicas, bem como demonstrar as novas perspectivas sobre a forma de tratamento dos dados pessoais a partir de um reexame da categoria especial dos dados sensíveis, na tentativa de mitigar a ocorrência de discriminações.

Para tanto, utilizar-se-á do método científico-dedutivo de pesquisa bibliográfica.

O viés do algoritmo e a discriminação

O uso de programas de aprendizado de máquina (*machine learning*) e a sua técnica de abordagem mais profunda (*deep learning*) deram às máquinas a incrível capacidade de se desenvolverem através da experiência e de decidirem de forma autônoma, ou seja, dispensando a intervenção humana nas etapas subsequentes ao desenvolvimento do algoritmo.

Assim, se inicialmente apenas um ser humano era capaz de programar um algoritmo, hoje já é possível e até mesmo mais comum que a própria máquina atue como programadora ou que os próprios

algoritmos possam se interligar reciprocamente para chegar a melhores resultados. Nesse sentido, são chamadas de decisões automatizadas ou decisões algorítmicas aquelas que são alcançadas apenas através do processamento automático, sem a necessidade de intervenção humana.[1]

Decisões algorítmicas não são mais ficção; pelo contrário, são uma realidade cada vez mais frequente. São os algoritmos, por exemplo, que decidem quais trabalhadores serão selecionados para trabalhar numa empresa; a quem serão concedidos ou negados empréstimos pessoais; e os valores das apólices dos seguros. Eles até mesmo já auxiliam em decisões judiciais.

Esse desenvolvimento tecnológico, entretanto, não foi acompanhado de um correspondente desenvolvimento jurídico de ferramentas para governança e regulação de algoritmos utilizados para esses fins.[2] Por conseguinte, na prática, as decisões tomadas por algoritmos têm se mostrado tendenciosas, impactando de forma negativa sobretudo os indivíduos e grupos sociais menos favorecidos.

Um exemplo ilustra bem a questão: recentemente, foi implantada em alguns sistemas de justiça criminal estadunidenses, como nos estados de New Jersey e Wisconsin, uma ferramenta de IA denominada Compas (*Correctional Offender Management Profiling for Alternative Sanctions*), que objetiva avaliar o risco de reincidência dos réus. Através do *software*, dados obtidos no *big data* são utilizados para arbitrar a pena do sujeito condenado, podendo esta ser majorada em caso de o sistema acusar um índice de reincidência.

Com base na análise preditiva feita pelo algoritmo, Eric Loomis, réu, negro, teve negada sua liberdade provisória e ainda aumentada sua

1 COSTA, Diego Carneiro. *O viés do algoritmo e a discriminação por motivos relacionados à sexualidade*. 2020. Dissertação (Mestrado) – Universidade Federal da Bahia, Faculdade de Direito, Salvador, 2020.

2 FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro. *Arbitrium ex machina*: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. *Revista dos Tribunais*, São Paulo, v. 995, p. 635-655, 2018.

pena sob a justificativa de que ele apresentaria alto risco de violência, reincidência e evasão. Acontece que através de pesquisa realizada pela ONG ProPublica, constatou-se que o programa tendia a classificar em dobro os acusados negros como prováveis reincidentes em comparação com os brancos,[3] relatando uma discriminação causada por um viés racial do algoritmo, que afetou a igualdade de tratamento entre os presos brancos e negros.

O exemplo acima descrito se insere no que se convencionou chamar de discriminação algorítmica, que é uma consequência do enviesamento do algoritmo que ocasiona distinções, preferências ou exclusões capazes de afetar a igualdade de tratamento ou de direitos entre seres humanos. No caso relatado, o viés do programa criou um verdadeiro *feedback loop*, concretizando a estigmatização de um grupo vulnerável por razão de critérios raciais (racismo algorítmico).

As pesquisas mais recentes sobre o tema demonstram que a discriminação algorítmica ocorre por dois motivos principais: 1. porque a técnica de aprendizado de máquina pode confirmar os vieses existentes desde a programação, reproduzindo o preconceito (consciente ou inconsciente) do programador; 2. porque os dados aos quais os algoritmos são expostos podem refletir o preconceito presente na sociedade, fazendo com que as decisões daí derivadas carreguem o mesmo viés e ocasionem toda sorte de discriminações.

Nessa linha, faz-se necessário trazer a doutrina de Solon Barocas e Andrew Selbst:

> Enquanto a discriminação certamente persiste em parte devido aos preconceitos dos tomadores de decisão, um grande componente da desigualdade moderna pode ser atribuído ao que os sociólogos chamam de discriminação 'institucional'.

3 LOPES, André. Preconceito Automático: Softwares guiados por algoritmos que buscam simular o comportamento humano acabaram por reproduzir também o que há de pior entre nós: a discriminação contra o outro. *Veja*, São Paulo, 19 jul. 2019.

> Em vez de escolhas intencionais, os preconceitos inconscientes e implícitos, bem como a inércia das instituições da sociedade respondem por grande parte dos efeitos desproporcionais observados. Realizada sem cuidados, a mineração de dados pode reproduzir padrões de discriminação existentes, herdar prejuízos de antigos tomadores de decisão, ou simplesmente refletir os vieses que persistem na sociedade. Pode até gerar o resultado perverso de exacerbar desigualdades existentes ao sugerir que determinados grupos que sofrem desvantagens históricas na verdade merecem um tratamento menos favorável.[4]

Além disso, tecnologias que se utilizam do *big data* podem amplificar a discriminação no caso dos vieses implícitos nos dados. Por exemplo, ao terem contato com bases de dados enviesadas de gênero ou raça presentes nas redes sociais, os algoritmos podem aprender a reforçar o preconceito e a discriminação contra as minorias sexuais, raciais, étnicas etc.[5]

Foi o que aconteceu com a robô virtual Tay, desenvolvida pela Microsoft para simular uma adolescente de 17 anos no *Twitter*, que em menos de 24 horas de interação nas redes sociais passou a reproduzir mensagens xenofóbicas, racistas e antissemitas, quando teve que ser desativada.[6] Verificou-se nesse caso que, ao aprender com a categorização de um banco de dados como o *Twitter*, que muitas vezes é utilizado por usuários para disseminar *hate speech*,[7] os algoritmos rapidamente passaram a reproduzir tais comportamentos.

4 BAROCAS, Solon; SELBST; Andrew D. Big Data's Disparate Impact. *California Law Review*, Washington, D.C., v. 104, p. 2-6, 2016.

5 COSTA, *op. cit.*, p. 94.

6 CANO, Rosa Jiménez. O robô racista, sexista e xenófobo da Microsoft acaba silenciado: projetado para o mercado dos 'millennials' nos Estados Unidos, Tay não foi capaz de lidar com piadas e perguntas controvertidas. *El País*, São Francisco, 25 maio 2016.

7 Nesse contexto, a expressão *hate speech* pode ser entendida na língua portuguesa como "discurso de ódio" ou "manifestação de ódio" nas redes sociais.

Percebe-se, portanto, que para o correto funcionamento do algoritmo, inicialmente, faz-se necessário um grande volume de dados, já que são eles que "alimentam" o sistema. Porém, ainda mais importante do que a quantidade é a qualidade desses dados que serão utilizados pela máquina, pois a existência de dados enviesados ensinará o algoritmo a desempenhar suas funções também de forma enviesada, perpetuando, de forma automatizada, as desigualdades sociais verificadas na sociedade.

Sendo assim, tendo como objetivo a proteção das vítimas e o combate à discriminação algorítmica, faz-se imprescindível avançar na investigação de como será feito o tratamento dos dados utilizados como matéria-prima para a intervenção algorítmica. Por tais razões, deve-se invocar todo o arcabouço normativo de proteção aos dados pessoais, como veremos a seguir.

Discriminação algorítmica e as normas de proteção de dados pessoais

Considerando que grande parte das decisões algorítmicas discriminatórias envolvem a coleta, o tratamento e o compartilhamento de dados pessoais dos indivíduos, os dilemas éticos e jurídicos advindos do uso desta tecnologia necessariamente passarão pela análise dos princípios e regras que regem a proteção de dados pessoais.

Casos como o da Cambridge Analytica redobraram a atenção da comunidade internacional para a necessidade de um desenvolvimento progressivo da defesa dos direitos e das liberdades dos indivíduos contra os arbítrios de empresas e governos no que tange ao controle e tratamento de dados pessoais, solidificando-se a ideia de uma sociedade orientada por dados mais conscientes[8] e chamando atenção para a necessidade de se adotar estratégias de regulação e

8 FERRARI; BECKER; WOLKART, *op. cit.*, p. 6.

utilização de IA, sobretudo para mitigar os potenciais danos aos usuários e à sociedade.

Nessa linha, pode-se dizer que atualmente vivencia-se uma virada paradigmática quanto ao tratamento de dados pessoais, passando-se da perspectiva da autodeterminação informacional para a do gerenciamento de riscos das atividades de tratamento de dados.[9] A principal característica a ser observada nessa nova fase é a mudança de um arquétipo de normas de cunho liberal, fundadas no consentimento do usuário como fator preponderante para a licitude da utilização dos dados para um modelo social, que parte de uma ideia de assimetria da informação.[10]

Isso ocorre, principalmente, por conta da percepção de que o tratamento de dados pessoais necessita de uma proteção no seu mais alto grau, que não pode ser conferida exclusivamente por uma decisão individual de consentimento, haja vista a posição de hipossuficiência que o titular dos dados ocupa, em contraposição às grandes empresas que controlam o tráfego de dados mundialmente.

Sob esse prisma, a principal referência normativa desse novo paradigma é o Regulamento Geral de Proteção de Dados da União Europeia 2016/679 (General Data Protection Regulation – GDPR).[11] Para a normativa europeia, que influenciou muito o direito brasileiro acerca do tema, o consentimento continua sendo importante, mas há regras mais específicas para se proteger a parte hipossuficiente da relação, como o fato de o pedido de consentimento 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" (art. 7º, item 2)[12] e

9 BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 215.

10 BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação da Inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada?. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). *Inteligência artificial e o direito*: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019. p. 216.

11 UNIÃO EUROPEIA. *Regulamento (UE)* 2016/679. Europa: União Europeia, 2016.

12 *Ibidem*.

o direito do titular dos dados de retirar o seu consentimento a qualquer momento (art. 7º, item 3).[13]

No que concerne às decisões algorítmicas, a GDPR traça limites à tomada de decisão exclusivamente automatizadas quando estas produzirem efeitos jurídicos similares significativos nos indivíduos. No artigo 12 do regulamento, há previsão de que os responsáveis pelo tratamento de dados têm o dever de informar os titulares dos dados acerca da existência de decisões automatizadas, da lógica envolvida e das consequências previstas para os titulares de dados.[14]

Outrossim, o artigo 22, item 1, do GDPR permite que o titular dos dados se recuse a ser submetido a uma decisão exclusivamente automatizada, desde que ela possa produzir efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. Há, todavia, algumas exceções, tais como o consentimento do titular dos dados; a necessidade de celebração de contrato entre o titular dos dados e o responsável pelo tratamento dos dados; e o caso de autorização estatal, sempre resguardados os direitos e liberdades fundamentais do titular.

Já no item 3 do artigo 22, da GDPR, também há a previsão da intervenção humana nas decisões automatizadas, além do direito de manifestar o seu ponto de vista e contestar a decisão. Em outras palavras, o dispositivo autoriza a intervenção de um agente humano no processo decisório para referendar ou ajustar eventuais erros de decisão por parte do algoritmo, o que, como veremos, não foi previsto no Brasil.

Nesse contexto, é possível inferir, das previsões contidas nos diversos itens do artigo 22 da GDPR, o chamado direito à explicação das decisões automatizadas, que é a possibilidade de o titular de dados ter acesso e conhecimento dos métodos utilizados pela IA para alcançar o resultado da decisão algorítmica.

13 *Ibidem*.

14 FERRARI; BECKER; WOLKART, *op. cit.*, p. 4.

Outra normativa fundamental no que se refere à proteção de dados pessoais é a Resolução do Parlamento Europeu, de 14 de março de 2017, que trata de forma mais específica das implicações dos grandes volumes de dados nos direitos fundamentais, como privacidade, proteção de dados, não discriminação e segurança. Esta norma versa mais diretamente sobre decisões automatizadas de IA, utilização de redes neurais e os novos modelos de análises preditivas que se utilizam do *big data*. Dentre outros preceitos, a Resolução especificamente prevê a proteção contra a discriminação algorítmica, como se infere:

> os dados e/ou os procedimentos de baixa qualidade em que se baseiam os processos de tomada de decisão e os instrumentos analíticos podem traduzir-se em algoritmos parciais, correlações ilegítimas, erros, numa subestimação das implicações jurídicas, sociais e éticas, no risco de utilização de dados para fins discriminatórios ou fraudulentos e na marginalização do papel dos seres humanos nestes processos, podendo resultar em processos imperfeitos de tomada de decisão, com um impacto nocivo nas vidas e nas oportunidades dos cidadãos, mormente nos grupos marginalizados, bem como em consequências negativas para as sociedades e as empresas.[15]

A resolução também estende à atividade de tratamento de dados toda atividade de tratamento de dados capaz de gerar impactos discriminatórios, a aplicação da legislação da UE relativa à proteção da vida privada e dos dados pessoais, o direito à igualdade e à não discriminação, bem como o direito das pessoas de receberem informações relativas à lógica subjacente aos processos de tomada de decisões e criação de perfis automatizados (item 5).

15 UNIÃO EUROPEIA. Regulamento (UE) 2016/679. *op. cit.*

Já no âmbito do direito pátrio, recentemente foi sancionada a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD),[16] que constitui um novo marco regulatório da proteção de dados no país, de forte inspiração nas normas europeias de proteção de dados supramencionadas.

Destarte, com a entrada em vigor da LGPD tem-se, finalmente, uma fonte normativa mais específica para resolver as eventuais questões relativas às decisões automatizadas, inclusive no que tange à prevenção e correção de vieses algorítmicos e seus impactos negativos na vida das pessoas.

Nesse sentido, faz-se importante destacar que dentre os princípios trazidos pela LGPD e que regem as atividades de tratamento de dados pessoais estão alguns muito caros às questões relativas às decisões automatizadas, tais como: o princípio do livre acesso aos dados (art. 6º, inciso IV), que é a garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; o princípio da qualidade dos dados (art. 6º, inciso V), que garante aos titulares a exatidão, clareza, relevância e atualização dos dados pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; o princípio da transparência (art. 6º, inciso VI), que traz a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; o princípio da não discriminação, que trata da impossibilidade de realização do tratamento de dados para fins discriminatórios ilícitos ou abusivos; o princípio da responsabilização e prestação de contas (art. 6º X), que traz a obrigatoriedade de demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.[17]

16 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

17 *Ibidem*.

Além disso, a LGPD também traz, em seu artigo 20, a possibilidade de revisão das decisões tomadas com base em tratamento automatizado de dados "que afetem seus interesses, inclusive de decisões destinadas a garantir o seu perfil pessoal, profissional, de consumo e de crédito ou aspectos da sua personalidade".[18] É de se lamentar, contudo, o fato de ter sido retirado do texto original a obrigatoriedade da intervenção humana na revisão da decisão algorítmica, o que, sem dúvida, enfraquece a tutela antidiscriminatória.

Por fim, é importante destacar a previsão de auditoria ou supervisão algorítmica para os casos de não recebimento da informação, realizada pela autoridade nacional para verificar os possíveis aspectos discriminatórios em tratamento automatizado de dados pessoais. Trata-se de um clamor antigo da doutrina mais recente pela necessidade de uma supervisão constante dos processos algorítmicos, como aqueles capazes de causar impactos discriminatórios, como nos casos em que há tratamento ou inferência a dados pessoais sensíveis, como veremos a seguir.

Discriminação algorítmica e o "tratamento sensível de dados pessoais"

Pode-se conceituar os dados pessoais sensíveis como aqueles dotados de um grau maior de fundamentalidade e que, justamente por isso, apresentam um elevado potencial discriminatório. Em grande medida, esses dados estão intimamente relacionados aos direitos da personalidade do seu titular, razão pela qual mereceram um tratamento mais restritivo nas normas de proteção de dados.[19]

Sob esse prisma, destaca-se a correlação intrínseca entre o princípio da não-discriminação (art. 6º, IX, da LGPD)[20] e os dados pessoais

18 *Ibidem*, p. 59.

19 COSTA, *op. cit.*, p. 154.

20 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

sensíveis, que abrange, na dicção legal da LGPD, qualquer dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, II, da LGPD).[21]

Por outro lado, numa lógica de exclusão, poder-se-ia entender que se incluem no conceito de dados pessoais "comuns" – e não de dados pessoais sensíveis – os chamados identificadores básicos, como nome, número de identificação, dados de localização, dentre outros.[22] Acontece que a somatória de alguns desses dados pessoais não qualificados como sensíveis também pode, na prática, colocar o seu titular numa situação semelhante de vulnerabilidade.[23]

Isso porque, tratando-se de decisões automatizadas tomadas por algoritmos de *machine learning* e, principalmente, *deep learning*, ainda que não se utilizem diretamente dados sensíveis, é possível que os dados utilizados como *proxies* gerem também, junto a outros dados, perfis relacionados a gênero, raça, religião, orientação sexual etc., violando o princípio da não-discriminação.[24]

É esclarecedor o exemplo trazido por Thiago Junqueira, no qual o nome da pessoa, talvez o dado pessoal de mais fácil acesso ao agente de tratamento, gerou uma discriminação algorítmica:

> Amplamente divulgada pela mídia britânica, a reportagem denunciou o fato de algumas seguradoras atuantes no ramo de automóvel estarem fixando prêmios de forma consideravelmente distinta para proponentes com perfis idênticos – à exceção do nome do condutor. Entre as várias cotações feitas

21 *Ibidem*.

22 FRAZÃO, Ana. Nova LGPD: o tratamento de dados pessoais sensíveis. *Jota*, [*s. l.*], 2018. p. 3.

23 JUNQUEIRA, Thiago. *Tratamento de dados pessoais e discriminação algorítmica nos seguros*. São Paulo: Thomson Reuters Brasil, 2020. p. 242.

24 BAROCAS; SELBST, *op. cit.*, p. 2-6.

> on-line, em sites de comparação de preços e diretamente com seguradoras, chama a atenção o relato de um seguro de automóvel, modelo Ford Focus 2007, na cidade de Leicester, ter sido precificado por 1.333 libras esterlinas para 'John Smith' e 2.252 libras esterlinas para 'Muhammed Ali'.[25]

Este exemplo serve para demonstrar que o traço distintivo entre dados pessoais sensíveis e não sensíveis não é tão claro, razão pela qual a doutrina mais atual sobre o tema tem clamado por um reexame dessa categoria. Como destaca Ana Frazão, há boas razões para sustentar que devam ser considerados sensíveis todos os dados que permitem que se chegue, como resultado final, a informações sensíveis a respeito das pessoas.[26]

O tema não passou despercebido pela Resolução do Parlamento Europeu, de 14 de março de 2017, que ressaltou no seu texto a dificuldade atual de se distinguir entre dados sensíveis e não sensíveis, uma vez que, tendo em vista o grande volume de tráfego de dados e a ausência de controle do tratamento deles, é perfeitamente possível inferir informações sensíveis sobre pessoas a partir de dados não sensíveis (item 3).

A LGPD também encampou essa ideia quando, no seu artigo 11, §1º, trouxe a ressalva de que, nada obstante o elenco trazido no artigo 5º, inciso II, qualquer tratamento de dados pessoais que "revele dados pessoais sensíveis e que possa causar dano ao titular"[27] deve ser igualmente considerado abrangido pelo regime dos dados sensíveis. Conclui-se, portanto, que o rol de dados sensíveis trazidos pela LGPD é um catálogo aberto e dinâmico, ou seja, é meramente exemplificativo.

Entretanto, é de se questionar se a especificação de uma categoria justificadora de proteção mais ampla, por constarem em seu selo "dados sensíveis", não deveria ser revista, de modo a prestigiar uma

25 JUNQUEIRA, *op. cit.*, p. 216-217.

26 FRAZÃO, *op. cit.*, p. 4.

27 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

noção mais moderna de "tratamentos sensíveis de dados pessoais". Nesse sentido, cumpre destacar a visão de Danilo Doneda:

> Hoje, no entanto, o próprio conceito de dados pessoais sensíveis como fator que fundamenta uma proteção de nível mais elevado tende a ceder à noção de tratamento sensível de dados pessoais. Esta tendência provém do reconhecimento de que não é possível, hoje, predizer os efeitos que um tratamento de dados pessoais possa causar ao seu titular apenas a partir da consideração da natureza dos dados que são tratados. Com as modernas técnicas estatísticas e de análise de dados, até mesmo informações pessoais que, em si, não são sensíveis podem causar tanto (i) um tratamento discriminatório em si, quanto (ii) a dedução ou inferência de dados sensíveis obtidos a partir de dados pessoais não sensíveis. Em ambos os casos ocorre, efetivamente, justamente aquilo que se procura inibir com a criação de um regime especial para os dados sensíveis, que é a discriminação a partir do tratamento de dados pessoais.[28]

Portanto, clama-se por uma mudança de paradigma no que concerne a uma necessidade de conceito especial para os dados sensíveis, devendo-se considerar cada vez mais a importância de um "tratamento sensível de dados pessoais", de modo a proteger de forma mais ampla o titular dos dados quanto a possíveis discriminações diante da sua condição de vulnerabilidade perante aqueles que possuem a tecnologia para realizar o tratamento de dados.

Conclusão

O contexto atual da tecnologia favorece que as decisões que antes eram tomadas por seres humanos sejam totalmente transferidas para os

28 ESCOLA NACIONAL DE DEFESA DO CONSUMIDOR. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Brasília, DF: SDE:DPC, 2010. p. 27.

algoritmos inteligentes, visando obter maior eficiência e acurácia aos processos decisórios. A contratação de um empregado, a concessão de um crédito pessoal, seguros pessoais e até mesmo as decisões judiciais atualmente estão sendo delegadas a algoritmos preditivos, o que traz uma série de questões éticas e jurídicas.

Tais questões devem ser analisadas a partir do arcabouço jurídico de proteção de dados pessoais. No Brasil, as disposições da LGPD, inspiradas pelo GDPR, da União Europeia, e pela Resolução do Parlamento Europeu, de 14 de março de 2017, trazem o princípio da não discriminação, o direito à explicação e a revisão das decisões automatizadas como os principais instrumentos à disposição do titular dos dados em termos de prevenção e mitigação das discriminações algorítmicas.

Nesse contexto, também houve uma preocupação especial do legislador pátrio com os dados sensíveis (artigo 5º, item II da LGPD), quais sejam, aqueles dotados de um grau maior de fundamentalidade e que apresentam um elevado risco discriminatório, a exemplo dos dados pessoais relativos ao sexo (gênero),[29] orientação sexual e identidade de gênero dos indivíduos.

Demonstramos, todavia, que tal conceito deve ser reexaminado, cedendo espaço para uma concepção de "tratamento sensível de dados pessoais", a partir da constatação de que os dados pessoais não sensíveis (como o simples nome de uma pessoa ou o seu endereço), quando inseridos em um contexto de decisões automatizadas movidas a algoritmos de *machine learning* e *deep learning*, também podem revelar, a partir dos *proxies*, dados passíveis de serem utilizados para fins discriminatórios.

29 Enquanto sexo se refere às categorias inatas do ponto de vista biológico (sexo feminino e masculino), o gênero diz respeito aos papeis sociais relacionados com a mulher e o homem.

Referências

BAROCAS, Solon; SELBST; Andrew D. Big Data's Disparate Impact. *California Law Review*, Berkeley, v. 104, p. 2-6, 2016. Disponível em: http://ssrn.com/abstract=2477899. Acesso em: 1 mar. 2020.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação da Inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada?. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). *Inteligência artificial e o direito*: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019. p. 207-228.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

CANO, Rosa Jiménez. O robô racista, sexista e xenófobo da Microsoft acaba silenciado: projetado para o mercado dos 'millennials' nos Estados Unidos, Tay não foi capaz de lidar com piadas e perguntas controvertidas. *El País*, São Francisco, 25 maio 2016. Disponível em: https://brasil.elpais.com/brasil/2016/03/24/tecnologia/1458855274_096966.html. Acesso em: 10 nov. 2020.

COSTA, Diego Carneiro. *O viés do algoritmo e a discriminação por motivos relacionados à sexualidade*. 2020. Dissertação (Mestrado) – Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2020.

ESCOLA NACIONAL DE DEFESA DO CONSUMIDOR. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Brasília, DF: SDE:DPC, 2010.

FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro. *Arbitrium ex machina*: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. *Revista dos Tribunais*, São Paulo, v. 995, p. 635-655, 2018.

FRAZÃO, Ana. Nova LGPD: o tratamento de dados pessoais sensíveis. *Jota*, [*s. l.*], 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpdo-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em: 14 nov. 2020.

JUNQUEIRA, Thiago. *Tratamento de dados pessoais e discriminação algorítmica nos seguros*. São Paulo: Thomson Reuters Brasil, 2020.

LOPES, André. Preconceito Automático: Softwares guiados por algoritmos que buscam simular o comportamento humano acabaram por reproduzir também o que há de pior entre nós: a discriminação contra o outro. *Veja*, São Paulo, 19 jul. 2019. Disponível em: https://veja.abril.com.br/tecnologia/inteligencia-artificial-pode-reproduzir-racismo-homofobia-e-misoginia/. Acesso em: 10 fev. 2020.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679*. Europa: União Europeia, 2016. Disponível em: https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679___protecao_de_dados.pdf. Acesso em: 12 nov. 2020.

INTELIGÊNCIA ARTIFICIAL, SAÚDE MENTAL E OS DADOS: A DIMENSÃO DIGITAL NA REFORMA PSIQUIÁTRICA BRASILEIRA

Laércio Martins

Introdução

Embora não haja predominância, entre as dimensões da Reforma Psiquiátrica brasileira,[1] da dimensão jurídica, entendo que a abordagem dos estudos jurídicos no campo da legislação em saúde mental, ao longo dos últimos 30 anos, teve um caráter subsidiário. Tanto é assim que há raras pesquisas acadêmicas por juristas no campo da saúde mental, em comparação com a quantidade e qualidade de pesquisas nas dimensões política, teórico-conceitual, técnico-assistencial e sociocultural.

Sobre esse aspecto, é importante também salientar a dimensão sociocultural e os desdobramentos das discussões sobre a noção de "loucura" no imaginário social, a fim de eliminar a discriminação no convívio político. Em outras palavras, tão importante quanto o fim dos manicômios físicos é o fim dos manicômios mentais.[2]

1 AMARANTE, Paulo. A(clínica) e a Reforma Psiquiátrica. *In*: AMARANTE, Paulo (org.). *Arquivos de saúde mental e atenção psicossocial*. Rio de Janeiro: Nau, 2003. p. 45-65.

2 PELBART, Peter Pál. *Manicômio mental*: a outra face da clausura. *In*: LANCETTI, Antonio (org.). *Saúde loucura*. São Paulo: Hucitec, 1990. v. 2, p. 130-138.

Portanto, a atividade de convívio comunitário e do exercício da dimensão política não prescinde do âmbito sociocultural. Pelo contrário, é condição de possibilidade do exercício da cidadania para as pessoas em sofrimento psíquico.

Acrescento a isso a dimensão digital que, com o advento da pandemia da covid-19 e o processo de aceleração digital por meio da utilização das plataformas e mídias sociais, decorrente do desejo[3] social de manutenção das relações interpessoais e dos vínculos afetivos, aprofundou o debate sobre o cuidado por meio de tecnologias em saúde.

Com efeito, a entrada no século XXI caracterizada pela imersão da digitalização das experiências subjetivas de estar no mundo atravessa a humanidade engendrando novos modos de viver, ao digitalizar a vida, conforme afirma Paula Sibilia:

> Acompanhando as transformações das últimas décadas, certos discursos dos meios de comunicação, das ciências e das artes estão engendrando um novo personagem: o homem pós-orgânico. Essa criatura é fruto do ideário fáustico da tecnociência mais atual, que tem se expandido pelo tecido social para atingir as áreas mais diversas, turvando muitas definições que outrora pareciam claras e inquestionáveis. Uma delas é, precisamente, a de ser humano, cujas turbulências também são fruto de outras sacudidas conceituais.[4]

Essa nova dinâmica da tendência digital reformulou as discussões no âmbito do sistema de justiça, com a presença do uso da inteligência artificial, ao nos convidar a refletir inclusive sobre a natureza do corpo pós-orgânico no campo do direito à saúde mental e da proteção de dados e privacidade das pessoas com sofrimento mental,

3 ESPINOSA, Baruch de. *Ética*. Tradução: Grupo de Estudos Espinosanos e Coordenação Marilena Chauí. São Paulo: EdUSP, 2015.

4 SIBILIA, Paula. *O homem pós-orgânico*: a alquimia dos corpos e das almas à luz das tecnologias digitais. 2. ed. Rio de Janeiro: Contraponto, 2015. p. 69.

ao considerar um novo fenômeno: a dimensão digital na Reforma Psiquiátrica brasileira.

Inteligência artificial e sua aplicação no sistema de justiça brasileiro

Em que pese toda a controvérsia sobre a utilização da inteligência artificial no Poder Judiciário brasileiro, é preciso destacar que já se trata de uma realidade jurídica atual, a fim de dar maior celeridade processual, conforme recomendação do Conselho Nacional de Justiça (CNJ).[5]

O sistema de justiça brasileiro já adota o emprego da inteligência artificial, a exemplo da *Dra. Luzia* da Procuradoria-Geral do Distrito Federal; das *Alice*, *Sofia* e *Mônica*, utilizadas pelo Tribunal de Contas da União; do *Radar* no Tribunal do Estado de Minas Gerais; da *Elis* no Tribunal do Estado de Pernambuco; do *Berna* no Tribunal de Justiça do Estado de Goiás; e do *Victor* no Supremo Tribunal Federal (STF).

Diante desse cenário, não restam dúvidas sobre os impactos das tecnologias de inteligência artificial no âmbito das instituições de saúde e em decisões judiciais com possíveis implicações no campo da saúde mental. Um fenômeno inédito para as discussões da Reforma Psiquiátrica brasileira.

Lamentavelmente, os estudos do campo da saúde mental no ensino jurídico brasileiro são raros, quando não incipientes, o que reflete na formação do profissional do Direito, que, na maioria das vezes, não tem conhecimento da dimensão jurídica da Reforma Psiquiátrica brasileira.

Isso é extremamente preocupante, uma vez que a ausência de alimentação de dados dessa interface entre Direito e Saúde Mental nos sistemas de inteligência artificial torna ainda mais problemáticos os

5 CONSELHO NACIONAL DE JUSTIÇA. *Inteligência artificial no poder judiciário brasileiro*. Brasília, DF: CNJ, 2019.

resultados decorrentes do uso dos algoritmos nas propostas de decisões administrativa e judicial em sede dos direitos e garantias das pessoas com deficiência mental, intelectual e sensorial.

Em outras palavras, faz-se importante o ingresso de ações judiciais no sentido de promover a efetividade e defesa do cuidado em liberdade da pessoa em sofrimento psíquico. Além disso, para evitar mais retrocessos na Política Nacional de Saúde Mental (PNSM) duramente construída ao longo da trajetória de reabertura democrática no Brasil dos anos 1980,[6] são urgentes discussões sobre a regulação jurídica do sofrimento psíquico no STF, a fim de defender ações e serviços assistenciais antimanicomiais.

Dentro desse contexto institucional e jurídico, entendo que, em razão da ausência da implementação ou da implantação parcial da Rede de Atenção Psicossocial no sentido de permitir o cuidado em liberdade da pessoa em sofrimento mental, mais do que justifica-se a demanda judicial, como também potencializa a luta antimanicomial enquanto movimento social a participar nos espaços do Poder Judiciário.[7]

Nesse sentido, o acesso ao sistema de justiça se faz necessário sempre que houver ineficiência das ações do Poder Executivo (União, Estados, Municípios e Distrito Federal) em propor políticas públicas antimanicomiais, que agora, diante do mandamento jurídico das boas práticas administrativas e da governança institucional, deve zelar pela proteção dos dados e da privacidade das pessoas com sofrimento mental, seja na esfera pública, seja na fiscalização do âmbito privado de cuidado em liberdade.

6 MEZZA, Martín; TORRENTÉ, Mônica de Oliveira Nunes de. A Reforma Psiquiátrica Brasileira como luta pelo reconhecimento e progresso moral. *Revista do Centro Brasileiro de Estudos de Saúde*, Rio de Janeiro, v. 44, n. 3, p. 235-249, 2020.

7 FALCÃO, Monique. *Poder Judiciário como espaço público*: análise de uma possível integração entre movimentos sociais e Estado. [*S. l.*]: Novas Edições Acadêmicas, 2015.

Proteção de dados e saúde mental

Dessa forma, é oportuno também considerar que a vigência da Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018[8] – tem repercussão no âmbito da saúde mental e, portanto, é imprescindível na defesa dos direitos das pessoas em sofrimento psíquico. Nesse sentido, deve ser observada a relevância da proteção do *livre desenvolvimento da personalidade da pessoa natural* (art. 1º da Lei nº 13.709/2018), inclusive das pessoas com deficiência mental, sensorial e intelectual.

Somado a isso, cumpre considerar, dentre os fundamentos da proteção de dados pessoais, a *autodeterminação informativa* (art. 2º, II da Lei n°. 13.709/2018) e *os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e exercício da cidadania pelas pessoas naturais* (art. 2º, VII da Lei n°. 13.709/2018). Observe que também em defesa da autonomia da pessoa, o STF, por meio do julgamento da ADI 6390 MC/DF,[9] reconheceu como *direito fundamental a autodeterminação informativa*, bem como *o direito fundamental à proteção de dados*.

Pode-se notar a importância de zelar e proteger as pessoas com sofrimento psíquico, em condições de vulnerabilidade socioeconômica, ao mesmo tempo em que é preciso romper com os manicômios mentais ainda presentes na sociedade brasileira.

Dentre outras conceituações, a LGPD faz a distinção entre dado pessoal (art. 5º, I da Lei nº 13.709/2018) e dado pessoal sensível (art. 5º, II da Lei nº 13.709/2018). Sobre esse aspecto, *os dados referentes à saúde são considerados sensíveis*. Veja que a interpretação sobre o sentido e o alcance desse texto jurídico tem repercussão direta nas ações e serviços da PNSM, que devem ser adequados à política de governança e boas

8 BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n° 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

9 BRASIL. Supremo Tribunal Federal. *ADI 6390 MC/DF*. Relatora Ministra Rosa Weber. 19 de abril de 2020.

práticas sobre as informações sensíveis das pessoas que utilizam os serviços de saúde mental no Brasil.

Em interpretação sistemática com a Lei da Reforma Psiquiátrica (Lei nº 10.216/2001),[10] nota-se que o dispositivo relativo ao *dado pessoal sensível* (art. 5º, II da Lei nº 13.709/2018) encontra correspondência no art. 1º da Lei nº 10.216/2001. Dentre a previsão dos direitos da "pessoa portadora de transtorno mental", está *a garantia do sigilo nas informações prestadas* (art. 2º, parágrafo único, IV da Lei nº 10.216/2001).

Tal norma jurídica reforça politicamente os mandamentos constitucionais (art. 5º, *caput*, CRFB/88 c/c art. 5º da Convenção Internacional sobre o Direito das Pessoas com Deficiência), ao assegurar a *vedação de qualquer forma de discriminação* às pessoas "acometidas de transtorno mental" quanto à raça, cor, sexo, orientação sexual, religião, opção política, nacionalidade, idade, família, recursos econômicos e ao grau de gravidade ou tempo de evolução de seu transtorno, ou qualquer outra situação.

Ainda nesse escopo constitucional, deve ser observada a *inviolabilidade do sigilo de dados* (art. 5, XII, CRFB/88) e a *inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas* (art. 5º, X, CRFB/88).

Além disso, deve-se dizer que o Estatuto da Pessoa com Deficiência (Lei nº 13.146/2015) assegura a igualdade de oportunidades com as demais pessoas (art. 4º da Lei nº 13.146/2015), sendo protegida de toda forma de discriminação, negligência, exploração, violência, tortura, crueldade, opressão e tratamento desumano e degradante (art. 5º da Lei nº 13.146/2015).

Além disso, o tratamento de dados pessoais, dentre outras hipóteses, só poderá ser realizado mediante o fornecimento de consentimento

10 BRASIL. Lei no 10.216, de 6 de abril de 2001. Dispõe sobre a proteção e os direitos das pessoas portadoras de transtornos mentais e redireciona o modelo assistencial em saúde mental. *Diário Oficial da União*: seção 1, Brasília, DF, ano 139, n. 69-E, p. 2, 9 abr. 2001.

pelo titular (art. 7º, I da Lei nº 13.709/2018), para a proteção da vida ou da incolumidade física do titular ou de terceiro (art. 7º, VII da Lei nº 13.709/2018) e para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou de autoridade sanitária (art. 7º, VIII da Lei nº 13.709/2018).

Ao considerar o tratamento de dados das pessoas com sofrimento psíquico, a permissão da utilização deve vir acompanhada de "o maior número de informação a respeito de sua doença e de seu tratamento" (art. 2º, VII da Lei nº 10.216/2001).

A fim de efetivar o direito fundamental à vida das pessoas com deficiência, é indispensável para a realização de tratamento, procedimento, hospitalização e pesquisa científica, o consentimento prévio, livre e esclarecido (art.12 da Lei nº 13.146/2015 c/c art. 25, letra "d" da Convenção Internacional dos Direitos das Pessoas com Deficiência)

Na hipótese de curatela, a pessoa com deficiência deve ter assegurada sua participação, no maior grau possível, para a obtenção de consentimento (art. 12, §1º da Lei nº 13.146/2015). Assim, a pessoa com deficiência somente será atendida sem seu consentimento prévio, livre e esclarecido em casos de risco de morte e de emergência em saúde, resguardado seu superior interesse e adotadas as salvaguardas legais cabíveis (art. 13 da Lei nº 13.146/2015).

Dessa forma, toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade (art. 17 da Lei nº 13.709/2018). Em análise conjunta com o Estatuto da Pessoa com Deficiência, deve-se observar que, além da titularidade dos dados, em regra, a deficiência não afeta a plena capacidade civil da pessoa (art. 6º da Lei nº 13.146/2015), inclusive ao ser facultado o exercício de sua autonomia através da tomada de decisão apoiada (art. 1.783-A da Lei nº 13.146/2015).

De acordo com o art. 4, inciso III do Código Civil de 2002, as pessoas que, por causa transitória ou permanente, não puderem exprimir sua vontade, são incapazes relativamente a certos atos ou à maneira de os

exercer. Portanto, via de regra, não existe a incapacidade absoluta para as pessoas com deficiência mental, sensorial ou intelectual, por exemplo. Logo, é preciso muita cautela quanto à interpretação a favor do tratamento de dados pessoais das pessoas com deficiência psíquica, sem o consentimento e até mesmo com autorização do representante legal.

Além disso, o consentimento para o tratamento dos dados deve ser feito por escrito ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º da Lei nº 13.709/2018). Fica vedado o tratamento de dados pessoais mediante vício de consentimento (art. 8º, §3º da Lei nº 13.709/2018), o consentimento deverá referir-se a finalidades determinadas e as autorizações genéricas para o tratamento de dados pessoais serão nulas (art. 8º, §5º da Lei nº 13.709/2018).

Já no que diz respeito ao tratamento de dados pessoais sensíveis, somente poderá ocorrer, dentre outras hipóteses: quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas (art. 11, I, da Lei nº 13.709/2018) e sem o fornecimento de consentimento do titular em que for indispensável para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 11. II, letra "f", da Lei nº 13.709/2018).

A regra é a vedação da comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, como objetivo de obter vantagem econômica (art. 11, §4º da Lei nº 13.709/2018); todavia, a LGPD apresenta as seguintes exceções: 1. prestação de serviços de saúde; 2. de assistência farmacêutica, 3. de assistência à saúde e 4. serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, desde que seja respeitado o mandamento jurídico de vedação às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários (art. 11, §5º da Lei nº 13.709/2018).

A fim de reforçar a garantia do direito de proteção de dados, o legislador reconheceu que, para fins da LGPD, podem ser considerados como dados pessoais aqueles utilizados para a formação do perfil comportamental de determinada pessoa natural, se identificada (art. 12, §2º da Lei nº 13.709/2018).

Ainda no âmbito sanitário, na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a base de dados pessoais, que serão tratados exclusivamente dentro do órgão, estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anomização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas (art. 13 da Lei nº 13.709/2018).

De modo singular, ao considerar a pesquisa científica envolvendo pessoa com deficiência, deve ser observado que para fins diagnósticos ou terapêuticos não poderá ser realizada sem o consentimento expresso do paciente, ou de seu representante legal, e sem a devida comunicação aos conselhos profissionais competentes e ao Conselho Nacional de Saúde (art. 11 da Lei nº 10.216/2001).

Em situação de tutela ou de curatela deve ser realizada, em caráter excepcional, apenas quando houver indícios de benefício direto para sua saúde ou para a saúde de outras pessoas com deficiência e desde que não haja outra opção de pesquisa de eficácia comparável com participantes não tutelados ou curatelados (art. 12, §2º da Lei nº 13.146/2015).

Cumpre destacar que o Poder Público e, portanto, as ações e serviços públicos de saúde mental no Brasil devem se adequar à proteção da privacidade e dos dados das pessoas que acessam os equipamentos de cuidado mental e que o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e de atribuição legal pelos órgãos e pelas entidades

públicas, respeitados os princípios de proteção de dados pessoais previstos no art. 6 da LGPD – art. 26 da Lei nº 13.709/2018.

A regra é a utilização das boas práticas e da governança no âmbito do Estado brasileiro, de modo a implementar programa de governança em privacidade (art. 50, I da Lei nº 13.709/2018). Em caso de descumprimento da LGPD, há previsão de sanções administrativas (art. 52 a 54 da Lei nº 13.709/2018). Por fim, o esforço hermenêutico aqui apresentado nos convida também a refletir sobre a dimensão digital na experiência da Reforma Psiquiátrica brasileira. Vejamos.

A dimensão digital na Reforma Psiquiátrica brasileira

Uma vez apresentado o panorama geral da aplicação da LGPD no campo da saúde mental, a partir de uma interpretação sistemática e integrada com a Constituição Federal de 1988,[11] em favor da defesa dos direitos e garantias das pessoas com sofrimento mental, devemos nos atentar para a presença da dimensão digital *na* Reforma Psiquiátrica brasileira.

Ora, por dimensão digital deve ser entendida a extensão nas redes de internet, por meio de plataformas digitais, aplicativos e mídias sociais. Os impactos da experiência digital na Reforma Psiquiátrica brasileira são notórios, sobretudo através de eventos virtuais, nos quais são debatidos assuntos relacionados às dimensões jurídico-política, teórico-conceitual, técnico-assistencial e sociocultural.

A realidade do mundo virtual no âmbito dos debates da Reforma Psiquiátrica brasileira tornou-se cada vez mais comum em nossa sociedade hiperconectada. A exemplo disso, pode-se apontar atos e passeatas "virtuais", *lives* em plataformas digitais, congressos e

11 BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

eventos acadêmicos *on-line*. Isso confirma o que Paula Sibilia comenta sobre as novas formas de resistência:

> Nesse cenário que ainda está em mutação, não surpreende que tenham perdido efetividade as práticas de resistência características das sociedades disciplinares: das greves e passeatas mais tradicionais a todas as outras ações sindicais nelas inspiradas.[12]

Trata-se de uma tendência sociocultural que ao também perpassar a experiência da Reforma Psiquiátrica brasileira, envolve a dimensão jurídica com os debates sobre o Direito Digital.[13] Atualmente, a subjetividade humana encontra-se profundamente afetada pela exposição ao excesso de informação.

Nesse sentido, a regra, para a manutenção da saúde mental, é selecionar (filtrar) as informações, já que a atenção, considerada um ativo financeiro (moeda), no século XXI, é motivo de disputa mercadológica e captura no capitalismo de vigilância.[14]

Considerações finais

A presente Era Digital gera também uma ruptura da percepção de localização geográfica das pessoas e fortalece a formação de uma cultura cosmopolita. Assim, o uso das tecnologias digitais e dos aplicativos em *smartphones* permite a comunicação instantânea entre diversas pessoas, em localidades distintas, no compartilhamento de dados e informação, por exemplo.

Nesse contexto, uma marca da nossa época é estar *entre*. A sensação do modo de vida em suspenso e atravessado pelos mundos orgânico e

12 SIBILIA, *op. cit.*, p. 38.

13 HOFFMANN-RIEM, Wolfgang. *Teoria Geral do Direito Digital*: transformação digital, desafios para o Direito. São Paulo: Forense, 2020.

14 ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. New York: Public Affairs, 2019.

virtual afeta e reconstrói a subjetividade humana com desdobramentos no sistema de justiça e das tecnologias de inteligência artificial, com desdobramentos também no escopo de proteção de dados das pessoas com sofrimento mental. É importante observar a advertência de César Rendueles ao defender a importância da dependência mútua para um convívio igualitário:

> Deveríamos desconfiar daqueles projetos de libertação que não só não dizem nada sobre dependência mútua, como a maioria parte dos programas políticos modernos, mas literalmente não podem dizer nada sobre ela, como é o caso das propostas identitária pós-modernas e do ciberutopismo. A emancipação e a igualdade, a livre realização em comum de nossas capacidades não podem ser dissociadas do mútuo cuidado de nossas debilidades: de certo modo, seria conceder demais ao capitalismo. A codependência não tutelada é a matéria-prima com que podemos desenhar um entorno institucional amigável e igualitarista.[15]

Saímos do entorno amigável e igualitário da comunidade política e partimos para uma distopia de um lugar existencial, processo iniciado na experiência social concreta e geográfica – sem transcendentalismo – e transmutada para uma dimensão digital em permanência num local virtual, no qual os corpos digitais (imagens) interagem entre si, o que nos coloca uma questão: 1. estaremos nessa (im)permanência de estar *entre* mundos (orgânico e digital)? 2. ou ficaremos fadados à busca pelo *entrar*, mas sem acessar, paradoxalmente, os mundos (orgânico e digital) e habitar o não-lugar?

Não restam dúvidas de que a realidade do mundo virtual atravessa a sociabilidade e engendra novos modos de viver, modificando inclusive a dimensão do tempo, nessa transição do relógio analógico para o digital, conforme salienta Paula Sibilia:

15 RENDUELES, César. *Sociofobia*: mudança política na era da utopia digital. Tradução: Sérgio Molina. São Paulo: Edições Sesc São Paulo, 2016. p. 160.

> Nos novos modelos, o tempo perdeu os interstícios. O próprio aparelho específico tende a desaparecer, para se incrustar em toso os outros e se diluir por toda parte. Como ocorre com as instituições de confinamento, parece que também aqui os muros estão desabando: o tempo não é mais compartimentado geometricamente, passando a ser um contínuo fluido e ondulante, sempre escoando e nunca suficiente. Mais uma vez, o relógio serve como emblema e como sintoma, expressando em seu corpo maquínico a intensificação e a sofisticação da lógica disciplinar na sociedade de controle.[16]

Nesse contexto de espaço-tempo, ao se admitir a simbiose entre os mundos orgânico e virtual e a formação do homem pós-orgânico, não há que se falar em dicotomia da experiência geográfica e virtual. Ora, então, que corpo é este do século XXI que sofre mentalmente?

> Na pessoa saudável, o irracional não é suprimido em favor do racional. A pessoa saudável aceita seus sentimentos, mesmo quando eles vão contra a lógica aparente da situação. O esquizoide nega seus sentimentos, ao passo que o neurótico desconfia deles. O corpo é abandonado quando o irracional é negado e o sentimento, reprimido. Para recuperar o corpo, o indivíduo deve aceitar o irracional dentro de si. A genialidade do irracional é que ele tem o poder de nos mover. É a fonte de criatividade e de alegria.[17]

Assim, do acesso à sensibilidade corporal ao movimento criativo e saudável como potência do caminhar geográfico-virtual, outra indagação já se faz oportuna: existe uma dimensão digital *da* Reforma Psiquiátrica? Tal indagação é a busca pela tradução e entendimento da nova dimensão (digital) na Reforma Psiquiátrica brasileira:

16 SIBILIA, *op. cit.*, p. 29.

17 LOWEN, Alexander. *O corpo traído*. 8. ed. São Paulo: Summus, 2019. p. 202.

> Tradução e tradição, palavras que sagazmente dizem *caminho* e *entrega*, o percurso e a guarda exercida no cuidado do que há de ser conduzido e transportado em bom estado a um destinatário. Caminho e cuidado também comparecem à atividade quotidiana do pastor. Mas traduzir não é apascentar mansas ovelhas, é antes conduzir uma caravana. Com camelos exaustos e sob a inclemência das tempestades de areia, os tradutores seguem mascateando produtos que não fabricaram e que tampouco consideram como seus. Durante o percurso, o tradutor se faz íntimo dos tesouros que transporta. Mas sem querê-los para si, empenha-se antes em fazê-los circular. E só mesmo quem alimenta uma genuína fé na chegada pode fazer do caminho mais incerto a aventura da própria vida, alcançando com máxima realização a abertura de novas rotas.[18]

Assim, na certeza da construção de uma democracia antimanicomial, sigamos traduzindo as novas dinâmicas de vida em afetos potentes com genuína fé na chegada: uma sociedade sem manicômios, livre, libertária e antirracista. Do caminho mais incerto à aventura da própria vida: avante tradutores e tradutoras do novo porvir!

Referências

AMARANTE, Paulo. A (clínica) e a Reforma Psiquiátrica. *In*: AMARANTE, Paulo (org.). *Arquivos de saúde mental e atenção psicossocial*. Rio de Janeiro: Nau, 2003.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

18 GONÇALVES, Marcus Fabiano. *Bruno Palma, escolhedor de palavras*: ensaio sobre a arte e o ofício de um tradutor. São Paulo: Com-Arte, 2019. p. 91.

BRASIL. Lei no 10.216, de 6 de abril de 2001. Dispõe sobre a proteção e os direitos das pessoas portadoras de transtornos mentais e redireciona o modelo assistencial em saúde mental. *Diário Oficial da União*: seção 1, Brasília, DF, ano 139, n. 69-E, p. 2, 9 abr. 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10216.htm. Acesso em: 17 dez. 2020.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: seção 1, Brasília, DF, ano 130, n. 8, p. 1-74, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 17 dez. 2020.

BRASIL. Lei nº 13.146, de 6 de julho de 2015. Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência). *Diário Oficial da União*: seção 1, Brasília, DF, ano 152, n. 127, p. 2-11, 7 jul. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13146.htm. Acesso em: 17 dez. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 dez. 2020.

BRASIL. Supremo Tribunal Federal. *ADI 6390 MC/DF*. Relatora Ministra Rosa Weber. 19 de abril de 2020. Disponível em: http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5895176. Acesso em: 17 dez. 2020.

CONSELHO NACIONAL DE JUSTIÇA. *Inteligência artificial no poder judiciário brasileiro*. Brasília, DF: CNJ, 2019.

ESPINOSA, Baruch de. *Ética*. Tradução: Grupo de Estudos Espinosanos; Coordenação Marilena Chauí. São Paulo: EdUSP, 2015.

FALCÃO, Monique. *Poder Judiciário como espaço público*: análise de uma possível integração entre movimentos sociais e Estado. [*S. l.*]: Novas Edições Acadêmicas, 2015.

GONÇALVES, Marcus Fabiano. *Bruno Palma, escolhedor de palavras*: ensaio sobre a arte e o ofício de um tradutor. São Paulo: Com-Arte, 2019.

HOFFMANN-RIEM, Wolfgang. *Teoria Geral do Direito Digital*: transformação digital, desafios para o Direito. São Paulo: Forense, 2020.

LOWEN, Alexander. *O corpo traído*. 8. ed. São Paulo: Summus, 2019.

MEZZA, Martín; TORRENTÉ, Mônica de Oliveira Nunes de. A Reforma Psiquiátrica Brasileira como luta pelo reconhecimento e progresso moral. *Revista do Centro Brasileiro de Estudos de Saúde*, Rio de Janeiro, v. 44, n. 3, 2020.

PELBART, Peter Pál. Manicômio mental: a outra face da clausura. *In*: LANCETTI, Antonio (org.). *Saúde Loucura*. São Paulo: Hucitec, 1990. p.131-138. v. 2.

RENDUELES, César. *Sociofobia*: mudança política na era da utopia digital. Tradução Sérgio Molina. São Paulo: Edições Sesc São Paulo, 2016.

SIBILIA, Paula. *O homem pós-orgânico*: a alquimia dos corpos e das almas à luz das tecnologias digitais. 2. ed. Rio de Janeiro: Contraponto, 2015.

ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. New York: Public Affairs, 2019.

A PSEUDONIMIZAÇÃO COMO MEDIDA PROTETIVA PARA OS DADOS PESSOAIS SENSÍVEIS REFERENTES À SAÚDE

Rodrigo Castro Nascimento

Introdução

A entrada em vigor da Lei Geral de Proteção de Dados (Lei nº 13.709/2018)[1] no ano de 2020 trouxe a consolidação de preocupações que desde a sua construção já existiam: afinal, a LGPD vai trazer instrumentos que forneçam uma proteção no plano concreto, ou servirá apenas como uma lei bonita de ler, haja vista os seus diversos princípios positivados, mas difícil de efetivar no plano concreto?

A preocupação da Lei Geral de Proteção de Dados (LGPD) é de extrema importância para a tutela de dados pessoais, principalmente se estes dados forem considerados como sensíveis, pois estão ligados diretamente aos direitos da personalidade. Sendo assim, além de tutelar os diversos dados pessoais que se apresentam, a LGPD deve conferir um regime protetivo especial aos dados sensíveis.

Dentre os dados sensíveis, há os dados pessoais referentes à saúde, cujo conteúdo tem potenciais elementos discriminatórios, com alto

1 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

risco de causar estigmatizações aos seus titulares. Por conta disso, estes dados merecem uma tutela especial por parte da LGPD.

Apesar de haver outros instrumentos normativos que buscam proteger os dados sensíveis relativos à saúde, constantemente se observa casos de vazamentos e exposição deles, seja por empresas privadas, seja por parte da Administração Pública.

Tendo isso em vista, questiona-se: Qual a importância de se tutelar os dados sensíveis? A LGPD conta com dispositivos protetores dos dados pessoais referentes à saúde? A pseudonimização pode ser traduzida como uma medida protetiva concreta para os dados sensíveis à saúde?

A presente pesquisa se debruça acerca dessas questões, tendo como objetivo abordar uma medida protetiva que aqui se acredita que poderia coibir vazamentos e exposições de dados sensíveis à saúde.

Para que isso ocorra, o presente trabalho, se valendo de uma pesquisa bibliográfica e legislativa, é separado em três principais seções, cujo objetivos específicos são: demonstrar a importância dos dados sensíveis, dando um maior enfoque aos dados sensíveis à saúde; apresentar o tratamento conferido por algumas leis esparsas e pela LGPD acerca dos dados sensíveis de saúde, a fim de demonstrar se há ou não um regime protetivo especial para eles e se esse regime vem se mostrando como efetivo no plano concreto; e, por fim, busca-se trabalhar sobre a pseudonimização como medida protetiva possível para os dados pessoais sensíveis à saúde.

As garantias buscadas pelos dados pessoais sensíveis

A proteção dos dados pessoais sensíveis surge com o fundamento de se garantir direitos essenciais para o ser humano, dentre os quais estão: a igualdade, a privacidade, a não discriminação e a dignidade.

A igualdade material, no âmbito dos dados sensíveis, é uma forma de se evitar estigmas sociais e atos discriminatórios à pessoa; busca-se, então, a manutenção e fomentação da integração social.

> A própria seleção de quais seriam estes dados considerados sensíveis provém da constatação de que a circulação de determinadas espécies de informação apresentariam um elevado potencial lesivo aos seus titulares, em uma determinada configuração social.[2]

A tentativa de implantar a igualdade na sociedade teve várias faces. Nos séculos XVIII e XIX, com a ascensão do liberalismo e individualismo exacerbado, se entendia que para o alcance efetivo da igualdade, bastava conferir tratamento igual para as pessoas, tendo a igualdade um viés meramente formal.

Na contemporaneidade, desenvolveu-se o entendimento para a aplicação da igualdade na sociedade, o que ensejou o que se chama hoje de igualdade material ou substancial. O art. 3º da Constituição Federal brasileira demonstra que a concepção referente à igualdade sofreu transformações, sendo que ela

> passou de igualização estática, meramente negativa, no que se proibia a discriminação, para uma igualização eficaz, dinâmica, já que os verbos 'construir', 'garantir', 'erradicar' e 'promover' implicam, em si, mudança de óptica, ao denotar 'ação'. Não basta não discriminar. É preciso viabilizar – e encontramos, na Carta da República, base para fazê-lo – as mesmas oportunidades. Há de ter-se como página virada o sistema simplesmente principiológico. A postura deve ser, acima de tudo, afirmativa. E é necessário que essa seja a posição adotada pelos nossos legisladores.[3]

2 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Thomson Reuters: Revista dos Tribunais, 2019. p. 143.

3 MELLO, Marco Aurélio. A igualdade e as ações afirmativas. *Revista Cidadania e Justiça*, Rio de Janeiro, 2002. p. 98.

A partir da ideia de igualdade material e de prestação positiva por parte do Estado, passou-se a conceber que este não apenas deve se abster de práticas discriminatórias, mas também deve garantir proteção contra qualquer uma delas, sendo que as pessoas iguais devem ser tratadas de forma igual e as desiguais, de maneira desigual, na medida de suas desigualdades. Esse fato tomou uma importância muito grande nas relações privadas, pois nem toda manifestação de vontade expressa, de fato, um desejo da pessoa.

Existem até hoje contratos que são celebrados, não por conta da vontade, mas sim por questões de necessidade. Assim como contratos, muitas pessoas disponibilizam seus dados em operações bancárias ao longo dos dias, ou são internadas em hospitais ou atendidas em clínicas e disponibilizam seus dados pessoais porque necessitam.[4]

Em relações como essas, não seria correto a aplicação da igualdade em seu aspecto formal, pois em diversas relações privadas, principalmente as que implicam um negócio jurídico celebrado por necessidade, há um forte desequilíbrio entre as partes. No âmbito contratual, o que se mostra lesivo "é quando permanentemente uma das partes se encontra com sua liberdade de contratar e de definir o conteúdo do instrumento comprometida. É hora de intervir para garantir a liberdade de contratar".[5]

Dessa maneira, cabe ao Estado fornecer instrumentos protetivos para as pessoas que estão em situações de desequilíbrio nas relações privadas, a fim de conferir prerrogativas a estes indivíduos para que

4 Em 2015, por exemplo, a Secretaria da Fazenda da Bahia instituiu uma medida que obriga os consumidores baianos a fornecerem o seu número de CPF no caso de realizarem compras em redes de supermercados com sistema de venda para atacado e varejo, em valor acima de R$ 400,00 (quatrocentos reais). Ver SEFAZ institui exigência de CPF em compras acima de R$ 400. *Sefaz Net*, Bahia, 2015.

5 RAPOSO, Paulo Marcelo Wanderley. Autonomia privada e autonomia da vontade em face das normas constitucionais. *In*: LOTUFO, Renan (coord.). *Direito Civil Constitucional*. São Paulo: Malheiros, 2002. p. 83. Caderno 3

se obtenha um reequilíbrio nas relações, ou seja, para que haja uma igualdade substancial à situação.

Os dados sensíveis também têm por objetivo garantir o direito à privacidade. Enquanto a privacidade, na época do individualismo exacerbado, se mantinha atrelada à ideia tradicional do "*right to be let alone*", a Revolução Tecnológica permitiu que a privacidade aumentasse o seu sentido e o seu alcance.[6] A privacidade passou a ser concebida também como "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular".[7] Esta nova concepção marca a privacidade como um importante agente na proteção da sociedade em face dos avanços tecnológicos.

> Emerge um profundo vínculo entre liberdade, dignidade e privacidade, que nos obriga a observar esta última para além de sua definição histórica como direito a ser deixado só.
> Sem uma forte tutela para as informações que lhe dizem respeito, a pessoa é cada vez mais ameaçada de ser discriminada pelas suas opiniões, crenças religiosas, condições de saúde: a privacidade se apresenta assim como um elemento fundamental da *sociedade da igualdade*. Sem uma forte tutela dos dados referentes às convicções políticas ou à inscrição em partidos, sindicatos, associações, os cidadãos sofrem a ameaça de exclusão dos processos democráticos: desta forma a privacidade torna-se uma condição essencial para a inclusão na *sociedade da participação*. Sem uma forte tutela do 'corpo eletrônico', do conjunto das informações recolhidas a nosso respeito, a própria liberdade pessoal está em perigo e resulta muito evidente que a privacidade é um instrumento necessário para defender

6 MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva Jur, 2019. p. 29.

7 RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 15.

> a *sociedade da liberdade* e para se opor às forças que levam à construção de uma sociedade da vigilância, da classificação, da seleção social.[8]

Além da igualdade material e da privacidade, a proteção conferida aos dados sensíveis busca evitar o tratamento dos dados pessoais de forma discriminatória. A LGPD (Lei nº 13.709/2018),[9] que entrou em vigor no ano de 2020, fornece instrumentos com o objetivo de garantir a não discriminação, prevendo em seu art. 6º, inciso IX que a não discriminação se traduz na impossibilidade de realização do tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos.

Os dados sensíveis também se voltam para a dignidade da pessoa humana, o princípio basilar do ordenamento jurídico brasileiro e que possui a árdua tarefa de fazer com que o Estado e a sociedade tratem a pessoa como um valor e não como um patrimônio.

As finalidades e garantias dos dados sensíveis têm, portanto, o objetivo de assegurar a dignidade da pessoa humana no mundo tecnológico, pois dentro da dignidade "desenrolam-se manifestações infinitas, insuscetíveis de serem exauridas em modelos típicos, já que ela se transforma e se renova com as transformações da sociedade em que a pessoa se insere".[10]

A dignidade da pessoa humana é um princípio que consegue alcançar a todos, a todo momento. Conforme o crescimento e desenvolvimento da personalidade de cada indivíduo, suas noções e particularidades caminham juntamente com as suas noções do que considera

8 *Ibidem*, p. 233.

9 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

10 KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revistas dos Tribunais, 2019. p. 447.

ser uma vida digna. Essa concepção de dignidade, por mais que seja mutável, deve ser respeitada e garantida.

A dignidade da pessoa humana faz gerar inúmeras manifestações que não terminam em "modelos típicos, já que ela se transforma e se renova, para, por meio de novas manifestações, proteger, diante desse contexto, a liberdade de pessoa humana para ser quem ela é, para livremente construir sua própria personalidade".[11]

O avanço da tecnologia diminuiu distâncias, possibilitou tratamentos à saúde e confortos aos seus consumidores; mapas de papel foram trocados por assistentes virtuais que dizem e mostram qual o melhor caminho; mundos são criados em redes sociais onde as pessoas podem compartilhar seus pensamentos, fotografias, desejos, agradecimentos ou reclamações. O acesso à informação melhorou, tornou-se mais célere e maior, versando sobre tudo e sobre todos.

Porém, juntamente com os benefícios da tecnologia, também surgiram os seus malefícios. Empresas captam dados dos indivíduos que consomem a tecnologia, para interferirem no que as pessoas vão ou não ter facilidade de assistir na internet. Estas empresas captam dados pessoais sem o consentimento e ciência dos seus titulares, a fim de os comercializar.

Dessa forma, percebe-se que "a violação da privacidade e dos dados pessoais torna-se, portanto, um lucrativo negócio que, baseado na extração e na monetização de dados, possibilita a acumulação de um grande poder que se retroalimenta indefinidamente".[12]

Perfis são traçados com base nas publicações das pessoas nas redes sociais e são vendidos e compartilhados para que grandes empresas sejam contratadas e possam interferir na autonomia de escolha dos

11 *Ibidem*, p. 447.

12 FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revistas dos Tribunais, 2019. p. 29.

indivíduos, como ocorreu, por exemplo, com a empresa Cambridge Analítica quando da eleição de Donald Trump em 2016.[13] Os dados pessoais são o petróleo do século XXI.

Democracias estão sendo abaladas, dados utilizados como moeda para finalidades econômicas diversas e a autonomia está sendo atacada. A Revolução Tecnológica acabou se mostrando no século XXI como uma ameaça para a sociedade que a abraçou.

Sob esse viés de igualdade material, liberdade, dignidade da pessoa humana, direito à privacidade e a não discriminação, resultou a parte final do art. 1º da LGPD, a qual trata do direito ao desenvolvimento da personalidade, pois a pessoa, estando dentro da legalidade, deve ter garantido o seu direito de expressão e deve ter a segurança de que seus dados não serão utilizados para finalidades discriminatórias ou que cerceiem de alguma forma a sua liberdade.

Tendo em vista que a sociedade está cada vez mais estruturada no que tange à informação, a tutela dos dados pessoais sensíveis se torna indispensável, "como forma de impedir as finalidades discriminatórias e atentatórias à dignidade da pessoa, que ameaçam a construção das identidades individuais de forma plural".[14]

E essa é a importância de se regular a proteção dos dados sensíveis, os quais são dados pessoais que têm uma grande suscetibilidade para a utilização com finalidade discriminatória – como estigmatização, segregação, exclusão –, atacando diretamente os principais valores que a LGPD busca resguardar. Exatamente por implicarem no valor

13 Acerca do caso da empresa Cambridge Analytica, indica-se o documentário: PRIVACIDADE Hackeada. Direção: Karim Amer e Jehane Noujaim. Estados Unidos: Netflix, 2019. (114 min).

14 BARBOZA, Heloísa Helena; PEREIRA, Paula Moura Francesconi de Lemos Pereira; ALMEIDA, Vitor. Proteção dos dados pessoais da pessoa com deficiência. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters: Revistas dos Tribunais, 2019. p. 545.

intrínseco da dignidade, os dados sensíveis são aqueles referentes apenas à pessoa humana.[15]

A razão da proteção reforçada que se confere aos dados sensíveis centra-se "no potencial discriminatório de tais informações, que estigmatiza e exclui determinadas pessoas em razão de suas escolhas existenciais mais íntimas ou de traços biológicos".[16]

Por conta disso, tais dados merecem uma proteção especial, caso contrário, se encontraria um campo mais propício ao avanço das desigualdades e cerceamentos de liberdades existenciais, sendo que uma frágil tutela de tais dados impediria "a livre construção da identidade e a projeção de sua personalidade da forma que lhe aprouver, livre das âncoras do preconceito e discriminação".[17]

O art. 5º, inciso II da LGPD conceitua os dados sensíveis como todo

> dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Contudo, o rol de dados sensíveis apresentado pela LGPD não se trata de um rol taxativo, "já que eles são definidos pelos efeitos potencialmente lesivos do seu tratamento".[18] Dessa forma, além do rol apresentado pelo art. 5º, inciso II da LGPD, deve ser considerado como sensível todo dado pessoal que seja utilizado com a finalidade de discriminar, estigmatizar, fomentar preconceitos e atentar contra a segurança dos seus titulares.

15 KONDER, *op. cit.*, p. 455.

16 BARBOZA; PEREIRA; ALMEIDA, *op. cit.*, p. 546.

17 *Ibidem*.

18 KONDER, *op. cit.*, p. 455.

Um exemplo hipotético seria o do receio que se tem acerca de vendas ou até disponibilização de prontuários médicos para planos de saúde a fim de que eles utilizarem tais dados clínicos, que são sigilosos, para realizarem o exame de risco dos pretensos segurados.

Ainda em relação à saúde, existe o perigo de ocorrerem vazamentos de prontuários médicos e assim dados pessoais de saúde serem expostos, o que pode contribuir com estigmatizações, julgamentos e discriminações a depender do seu conteúdo.

Os dados relacionados à saúde são sensíveis e têm enorme potencial para gerar discriminações. O sigilo de prontuários médicos e de qualquer dado pessoal de um paciente – seja em clínicas, hospitais e até mesmo em farmácias – é essencial porque refere-se a dados extremamente perigosos e que necessitam de cuidado extremo no que tange ao seu tratamento.

Importante salientar que a pessoa que necessita de tratamento médico, ao buscar ajuda médica coloca-se em uma situação de vulnerabilidade, uma vez que procura se curar ou amenizar o sofrimento que possa estar lhe acometendo e, em troca, esse indivíduo acaba disponibilizando diversas informações íntimas não apenas de si mas também de sua família.[19]

Há grandes chances de os dados pessoais de saúde serem suficientes para violar a privacidade e intimidade de toda uma família. Um exemplo seria uma doença genética, pois se um dos familiares apresentar a enfermidade e seus dados clínicos forem expostos, isso impactará na intimidade de toda sua família, podendo causar discriminações a todos.

A tecnologia vem ameaçando os direitos das personalidades e há uma importância significativa na proteção dos dados sensíveis relacionados à saúde, uma vez que essa tutela abrange toda a

19 SCHAEFER, Fernanda. *Proteção de dados de saúde na sociedade de informação*: a busca pelo equilíbrio entre privacidade e interesse social. Curitiba: Juruá, 2010. p. 52.

sociedade, que "cada dia mais patrimonializa aspectos da personalidade, o direito da pessoa de controlar suas informações médicas e de mantê-las reservadas".[20]

Tendo isso em vista, questiona-se: de que maneira a LGPD busca tutelar os dados sensíveis à saúde e de quais instrumentos ela dispõe para tanto? As próximas seções buscam se debruçar sobre esses questionamentos.

Tratamento da LGPD acerca dos dados sensíveis à saúde

Como em toda análise que se faz acerca dos avanços tecnológicos, percebe-se que a evolução no tratamento de dados pessoais de saúde[21] não possui apenas pontos negativos, mas também pontos positivos, como a utilização de tais dados pessoais pelo Estado para realizar controles de epidemias,[22] a utilização de dados pessoais para estudos médicos com a finalidade de se difundir novos tratamentos acerca de determinadas doenças ou até para se chegar a novas curas a partir de estudos e pesquisas.

20 *Ibidem*, p. 61.

21 Importante salientar que quando se utiliza a expressão "tratamento de dados", entenda-se o conceito atribuído pela LGPD acerca do termo "tratamento de dados pessoais", qual seja: "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

22 Em 2009 houve a determinação no Brasil de cadastramento de passageiros de embarcações, voos, ônibus de linhas internacionais. Estes passageiros, ao entrarem no Brasil, deveriam preencher um extenso formulário, disponibilizando diversos dados pessoais (nome, endereço onde poderiam ser localizados, poltrona onde estavam sentados), tudo isso como forma de trazer uma maior facilidade no acompanhamento médico, em casos da gripe A(H1N1) no nos meios de transporte que foram utilizados. Ver: SCHAEFER, *op. cit.*, p. 63; BRASIL. Ministério da Saúde. *Plano brasileiro de preparação para enfrentamento de uma pandemia de influenza*. Brasília, DF: Ministério da Saúde, 2010.

Contudo, a utilização de dados pessoais relacionados à saúde torna necessário uma regulamentação a fim de traçar limites e assegurar direitos acerca do tratamento de tais dados, sempre tendo em mente a proteção de seus titulares, principalmente no que tange à sua imagem, honra, intimidade, privacidade e dignidade.

Dessa forma, a LGPD contempla dispositivos que visam tratar acerca dos dados sensíveis referentes à saúde, de forma a lhes conferir um regime especial. O art. 6º trata acerca de princípios que visam a sua proteção (e a de todos os dados pessoais), dentre eles os quais destacam-se no presente trabalho os princípios da: finalidade, necessidade, transparência, prevenção e segurança.

Os referidos princípios são de extrema importância para a tutela dos dados pessoais referentes à saúde, uma vez que estes dados devem ser utilizados por terceiros com uma finalidade específica e necessária, sendo que quando esta finalidade cessar, o tratamento de dados deverá se encerrar. Além disso, medidas preventivas devem ser tomadas desde o início do tratamento de dados pessoais, para que haja uma maior garantia de transparência e segurança no seu uso.

Além dos princípios estabelecidos pelo art. 6º da LGPD, o seu art. 7º, inciso VIII, dispõe que os tratamentos de dados pessoais de saúde, só serão realizados "para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária".[23]

O art. 11, inciso II, alíneas "d" e "e",[24] aborda a possibilidade de dispensa do consentimento do titular dos dados pessoais, quando a situação se mostrar indispensável para a proteção à vida, incolumidade

23 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

24 "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária".

física ou saúde do titular, ou seja, são casos em que outros princípios falam mais alto do que o próprio direito ao consentimento.

A título de exemplo, imagine-se um médico que está atendendo um paciente em caráter de emergência e necessita conhecer onde ele reside, para saber se aquela localidade é zona endêmica de determinada doença (malária ou dengue, por exemplo).

As causas de dispensa do consentimento dos dados sensíveis referentes à saúde não afastam as garantias trazidas pela LGPD, sendo que os médicos, hospitais e clínicas só deverão utilizar tais dados com o objetivo de atingir a finalidade pela qual foram captados, de forma lícita. Cessada a finalidade, o tratamento dos dados pessoais deve terminar, assegurando a autodeterminação informativa ao paciente, além de garantir instrumentos que evitem os vazamentos de dados. Portanto, na finalidade para o tratamento de dados, exige-se o respeito à "correlação entre o tratamento dos dados e a finalidade informada".[25]

Acerca das situações que se configuram como indispensáveis e justificam a dispensa do consentimento em dados pessoais de saúde, o legislador previu em seu art. 11, §4º da LGPD a vedação à utilização de tais dados com intuito de obter vantagem econômica, salvo nos casos de prestações de serviços ou assistências de saúde ou farmacêutica. Além disso, cabe a utilização de tais dados para permitir: portabilidade de dados solicitada pelo titular ou no caso de transações financeiras e administrativas que decorram do uso e da prestação de serviços voltados à saúde.

Porém, o §5º do art. 11 da LGPD veda expressamente que dados pessoais médicos sejam comercializados ou transferidos para as operadoras de planos privados, evitando assim a discriminação por

25 OLIVEIRA, Marco Aurélio Belizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters: Revistas dos Tribunais, 2019. p. 73.

parte delas quando realizarem a seleção de riscos na contratação dos seus serviços, bem como evitando o uso de dados pessoais com fins discriminatórios.

Apesar de se tratar de um dispositivo em que consta uma importante vedação, o §5º do art. 11 da LGPD torna difícil imaginar que "possa impedir a organização das estratégias empresariais de empresas de seguro saúde, as quais, como é cediço, desenvolvem suas atividades a partir de análises de risco e de probabilidade de sinistros".[26]

No que se refere aos casos de estudos em saúde pública, o art. 13 da LGPD traz uma importante proteção: os órgãos de pesquisa poderão ter acesso aos bancos de dados pessoais de saúde apenas dentro do órgão, devendo tal utilização seguir fielmente a finalidade de estudos e pesquisas. O ambiente em que os dados pessoais estão localizados deve ser controlado e seguro, seguindo-se as devidas "práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas".

De acordo com o artigo mencionado, caso haja qualquer divulgação acerca dos estudos, os dados pessoais não poderão ser revelados e o órgão de pesquisa, responsável pela segurança da informação, não poderá transferir os dados a terceiro.

Com isso, observa-se que a LGPD prevê dispositivos gerais, como o seu art. 6º, mas também normas voltadas para os dados pessoais sensíveis referentes à saúde, com o intuito de conferir uma tutela mais ampla e específica para estes dados.

Os dispositivos aqui abordados não exaurem com regime protetivo da LGPD, contudo, após esta breve análise, resta o seguinte

26 LUCCA, Newton de; MACIEL, Renata Mota. A proteção de dados pessoais no Brasil a partir da Lei 13.709/2018: efetividade?. *In*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (coord.). *Direito Digital*: direito privado e internet. Indaiatuba: Foco, 2020. p. 223.

questionamento: de que maneira os dispositivos que tutelam os dados pessoais relacionados à saúde podem combater as constantes violações das quais os titulares destes dados são vítimas?

Muito embora a Lei nº 13.709/2018 conte com diversos dispositivos protetivos para os dados sensíveis relacionados à saúde, antes do seu nascimento já existiam dispositivos que visavam a proteger tais dados.

No ano de 2001, por exemplo, a Lei nº 10.216/2001,[27] conhecida como Lei da Reforma Psiquiátrica, já previa em seu artigo 2º, IV a garantia de que nos atendimentos em saúde mental, a pessoa portadora de transtorno mental teria a garantia de sigilo das informações prestadas.

O Código de Ética Médica (Resolução nº 1.931/2009) do Conselho Federal de Medicina (CFM), em seu art. 85, dispõe ser vedado ao médico "Permitir o manuseio e o conhecimento dos prontuários por pessoas não obrigadas ao sigilo profissional quando sob sua responsabilidade".[28] Além disso, em seus artigos 75 a 77 a mencionada Resolução dispõe ser vedado ao médico:

> Art. 75. Fazer referência a casos clínicos identificáveis, exibir pacientes ou seus retratos em anúncios profissionais ou na divulgação de assuntos médicos, em meios de comunicação em geral, mesmo com autorização do paciente.
> Art. 76. Revelar informações confidenciais obtidas quando do exame médico de trabalhadores, inclusive por exigência dos dirigentes de empresas ou de instituições, salvo se o silêncio puser em risco a saúde dos empregados ou da comunidade.

27 BRASIL. Lei no 10.216, de 6 de abril de 2001. Dispõe sobre a proteção e os direitos das pessoas portadoras de transtornos mentais e redireciona o modelo assistencial em saúde mental. *Diário Oficial da União*: seção 1, Brasília, DF, ano 139, n. 69-E, p. 2, 7 abr. 2011.

28 BRASIL. Resolução nº 1.931/2009. Aprova o Código de Ética Médica. *Diário Oficial da União*: seção 1, Brasília, DF, p. 90, 24 set. 2009.

> Art. 77. Prestar informações a empresas seguradoras sobre as circunstâncias da morte do paciente sob seus cuidados, além das contidas na declaração de óbito, salvo por expresso consentimento do seu representante legal.

Na Resolução nº 1.974/2011 do CFM, a qual versa sobre a propaganda em Medicina, discorre em seu art. 3º que é vedada a exposição da "figura de seu paciente como forma de divulgar técnica, método ou resultado de tratamento, ainda que com autorização expressa do mesmo",[29] trazendo uma ressalva no art. 10, o qual dispõe que se a exposição do paciente for imprescindível para os trabalhos e eventos científicos, "o médico deverá obter prévia autorização expressa do mesmo ou de seu representante legal".

A Lei nº 12.965/2014 (o Marco Civil da Internet)[30] já previa em seu art. 3º a proteção da proteção da privacidade, a proteção dos dados pessoais, na forma da lei; e a responsabilização dos agentes de acordo com suas atividades, nos termos da lei.

Em seu art. 7º, a Lei nº 12.965/2014[31] já considerava como invioláveis a intimidade e a vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação, bem como a inviolabilidade do sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei.

Em 2018 surge a Lei nº 13.787/2018,[32] que dispõe acerca da digitalização e utilização de sistemas informatizados para a guarda, o

29 BRASIL. Resolução nº 1.974/2011. Estabelece os critérios norteadores da propaganda em Medicina, conceituando os anúncios, a divulgação de assuntos médicos, o sensacionalismo, a autopromoção e as proibições referentes à matéria. *Diário Oficial da União*: seção 1, Brasília, DF, n. 160, 19 ago. 2011.

30 BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: seção 1, Brasília, DF, ano 151, n. 77, p. 1-3, 24 abr. 2014.

31 BRASIL. Lei nº 12.965, *op. cit.*

32 BRASIL. Lei nº 13.787, de 27 de dezembro de 2018. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio

armazenamento e o manuseio de prontuário de paciente. Esta Lei dos Prontuários Eletrônicos aduz em seu art. 2º que "o processo de digitalização de prontuário de paciente será realizado de forma a assegurar a integridade, a autenticidade e a confidencialidade do documento digital".[33]

Em seu art. 4º, a Lei nº 13.787/2018 é clara ao afirmar que os meios de armazenamento de documentos digitais devem conferir-lhes proteção de "acesso, do uso, da alteração, da reprodução e da destruição não autorizados",[34] sendo que tais documentações devem ser controladas mediante "sistema especializado de gerenciamento eletrônico de documentos, cujas características e requisitos serão especificados em regulamento".[35]

E o Código Penal prevê os tipos penais de: violação do segredo profissional (art. 153, CP) e violação de sigilo funcional (art. 325, CP). Além disso, há um projeto de lei em vigor, o PL nº 7237/2017, chamado de Lei Marisa Letícia, que busca criminalizar divulgação de prontuário médico.[36]

de prontuário de paciente. *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 249, p. 3, 28 dez. 2018.

33 Cumpre registrar que "mesmo que o prontuário esteja na forma de papel ou em meio eletrônico, são assegurados o sigilo profissional e a privacidade do paciente, que configuram direito personalíssimo do paciente e dever do médico, calcados na confiança que surge na relação médico-paciente. [...]."
Ao lado desse direito ao sigilo, têm o médico e sociedades prestadoras de serviços médico-hospitalares o dever de guardar segredo acerca dos fatos dos quais teve ciência em razão de sua atividade profissional dos dados pessoais do paciente, dos resultados de exames realizados com finalidade terapêutica, diagnóstica ou prognóstica, informações contidas no prontuário, arquivo ou boletim médico. Além do dever de se abster de abusos, já que a relação médico-paciente está fundada na confiança, no respeito mútuo, na discrição e na reserva". PEREIRA, Paula Moura Francesconi de Lemos. O uso da internet na prestação de serviços médicos. *In*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (coord.). *Direito Digital*: direito privado e internet. Indaiatuba: Foco, 2020. p. 451.

34 BRASIL. Lei n° 13.787, *op. cit.*

35 BRASIL. Lei n° 13.787, *op. cit.*

36 LEI Marisa Letícia, que criminaliza divulgação de prontuário médico, é aprovada em Comissão da Câmara. *PT na Câmara*, [s. *l.*], 2018.

Contudo, mesmo havendo a existência de diversos dispositivos que servem tanto para médicos como para hospitais, clínicas e empresas que prestam de algum modo serviços e assistência à saúde, observa-se no Brasil diversos casos de vazamentos de dados pessoais relacionados à saúde.

Em 2016, por exemplo, foi descoberta uma falha de segurança nos sistemas da Prefeitura de São Paulo, o que gerou a exposição de dados pessoais de pelo menos 650 mil pessoas. Tais dados variavam "desde informações pessoais sobre os cidadãos cadastrados e servidores da Secretaria Municipal de Saúde até detalhes de prontuários médicos".[37]

No ano de 2018 foi noticiada uma falha no aplicativo e-Saúde do Ministério da Saúde, que armazena dados pessoais sensíveis como histórico de medicamentos, consultas agendadas, dentre outros; a falha ensejou o vazamento de milhões de brasileiros usuários do SUS desde o lançamento do aplicativo em 2017. Na ocasião, o médico e gestor público Giliate Coelho Neto afirmou que tudo indicava que o ministro Ricardo Barros havia pressionado os técnicos do Datasus para lançar o aplicativo e-Saúde sem os devidos mecanismos de segurança.[38]

Em 2019 a operadora de planos de saúde Unimed Brasil alegou falha em seu sistema que causou a exposição de dados pessoais dos seus clientes, como, por exemplo: fichas cadastrais, históricos médicos, exames, raio-X, ultrassonografias e certidões de óbito, dentre outros documentos particulares. Mesmo não havendo uma divulgação de quantos dados foram expostos, sabe-se que a Unimed, à época do ocorrido, contava com cerca de 18 milhões de beneficiários por todo o Brasil. [39]

37 FALHA de segurança expõe dados de milhares de pacientes do SUS em São Paulo. *Canaltech*, [*s. l.*], 2016.

38 VAZAMENTO de dados do E-Saúde expõe informações de milhões de brasileiros. *Fenafar*, [*s. l.*], 2018.

39 DUARTE, Marcella. Falha em sistema da Unimed expõe dados pessoais e até exames de pacientes. *UOL*, São Paulo, 2019.

No ano de 2020, houve um vazamento de senhas do Ministério da Saúde que davam acesso a dados pessoais de pelo menos 16 milhões de pacientes com diagnósticos suspeitos ou confirmados da covid-19. Tais dados ficaram disponíveis na internet por quase um mês, supostamente por causa de uma conduta indevida de um funcionário do Hospital Albert Einstein. O Hospital justificou que possuía "acesso aos dados porque está trabalhando em um projeto com o Ministério da Saúde".[40]

Também no ano de 2020, na cidade de Arapongas, localizada no Norte do Paraná, ocorreu o vazamento de uma lista com dados pessoais de sujeitos que testaram positivo para a doença covid-19. A lista continha nomes, endereços, telefones e a data em que os titulares dos dados receberam o resultado, constando inclusive o posto de saúde onde foram atendidos.[41]

Ainda em 2020, o Instituto Brasileiro de Defesa do Consumidor (Idec) oficiou a Agência Nacional de Vigilância Sanitária (Anvisa) por causa de um "vazamento de dados pessoais sensíveis de usuários cadastrados na agência para uso de medicamentos a base de canabidiol".[42]

Diante dos casos acima expostos, questiona-se: se as leis anteriores à LGPD não tiveram efetividade na proteção de dados pessoais referentes à saúde, apesar de conterem dispositivos principiológicos e instrumentais que versavam acerca da sua proteção, a LGPD conseguirá cumprir tal papel protetivo?

O vazamento de dados sensíveis à saúde é uma realidade, na medida em que órgãos públicos, pessoas físicas e jurídicas demonstram total ausência de segurança e falta de interesse diante do tratamento destes dados pessoais, o que enseja os constantes casos de vazamento.

40 VAZAMENTO de senhas do Ministério da Saúde expõe informações de pacientes de covid-19, diz jornal. *G1*, São Paulo, 2011.

41 LISTA com nomes de pacientes com covid-19 vaza no norte do PR. *CNN Curitiba*, Curitiba, 2020.

42 IDEC cobra Anvisa por vazamento de dados de pacientes que usam canabidiol. *IDEC*, São Paulo, 2002.

Esses vazamentos acabam implicando na própria vida das pessoas que têm os seus dados pessoais sensíveis expostos, sendo algo que pode impactar tanto nos aspectos negociais quanto existenciais do indivíduo. Observe-se que a proteção de dados é um direito fundamental autônomo, sendo uma "expressão de liberdade e dignidade pessoais e como tal, não se deve tolerar que um dado seja usado de modo a transformar um indivíduo em objeto sob vigilância constante".[43]

Para que o direito evolua para um sistema mais protetivo e valorativo acerca da pessoa, é necessário que o Estado e a sociedade façam cumprir as suas normas, principalmente suas essências principiológicas. Nesse sentido, leis como o Estatuto da Pessoa com Deficiência, o Código de Defesa do Consumidor e a própria LGPD, serão apenas exemplos de textos sem valor, se a sociedade não cumprir com os seus fundamentos.

Não faz sentido se conceber uma Lei de Proteção de Dados Pessoais, se a sociedade e o Estado não estão dispostos a respeitar a privacidade, a igualdade, a autodeterminação informativa, a não discriminação, o desenvolvimento pessoal, a finalidade e a dignidade da pessoa humana.

Tendo isso em vista, o presente trabalho busca apresentar uma proposta para que haja uma prevenção nos vazamentos de dados sensíveis relacionados à saúde. A presente pesquisa acredita que além de expor o problema, se faz necessário pensar e trabalhar com soluções, a fim de efetivar uma proteção de dados pessoais, a qual se mostra tão difícil no plano fático.

Pseudonimização: benefícios e vulnerabilidades da medida protetiva

A proteção dos dados pessoais deve ser enxergada não apenas no *post factum*, mas também com um enfoque preventivo. Sistemas que

43 RODOTÀ, *op. cit.*, p. 19.

captem e armazenem dados pessoais devem ser construídos com vistas à prevenção. A segurança e o sigilo de dados pessoais são pilares na construção de qualquer sistema protetivo e devem ser pensados, desde o nascimento de determinado produto ou serviço, sob a metodologia do *privacy by design*.[44, 45]

A metodologia do *privacy by design* tem "a ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviços, devendo eles ser embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais".[46]

Sendo assim, a *privacy by design* se apresenta quando determinado agente decide realizar qualquer tipo de tratamento de dados pessoais, devendo ter em mente o direito à privacidade "em cada passo, o que inclui projeto, desenvolvimento de produtos e *softwares*, sistemas de informática, dentre outros, a fim de assegurar que a privacidade será garantida durante todo o ciclo de tratamento".[47]

O *privacy by design* é uma metodologia que abarca os chamados PET's (*Privacy Enhancing Technologies*),[48] que concebem a ideia de que

44 SOUZA, Carlos Affonso Pereira de. Segurança e sigilo dos dados pessoais. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revistas dos Tribunais, 2019. p. 428.

45 Além do *privacy by design* existem outras máximas que as medidas de segurança devem observar na sua criação, desenvolvimento e atuação, como o *privacy by default*, a noção de privacidade incorporada ao *design*, a chamada funcionalidade total, a segurança de ponta a ponta e a garantia de que os *stakeholders* tratem os dados pessoais conforme as finalidades e promessas que se comprometeram. Para maior aprofundamento do tema, indica-se: SOUZA, *op. cit.*, 2019.

46 BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020, p. 167.

47 FRAZÃO, Ana. Objetivos e alcance da lei geral de proteção de dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters: Revistas dos Tribunais, 2019. p. 120.

48 As PET "são exemplos de como a tecnologia pode ser utilizada em prol da privacidade, o que se projeta desde a configuração de equipamentos eletrônicos, como *tablets* e *smartphones*, até mesmo à estruturação de produtos e serviços". *Ibidem*, p. 121.

apesar de a tecnologia poder ser utilizada como instrumento violador de direitos, ela também pode se traduzir como uma ferramenta protetiva dos dados pessoais e dos demais direitos.[49]

O art. 46, §2º da LGPD, inclusive, se coaduna com essa noção de prevenção, ao estabelecer que as medidas de segurança adotadas pelos agentes de tratamentos de dados pessoais, devem ser observadas "desde a fase de concepção do produto ou do serviço até a sua execução".[50]

Utilizando-se do *privacy by design* como base, passa-se a abordar um processo que tem grande potencial para ser uma efetiva medida de segurança preventiva: a pseudonimização.

A pseudononimização trata-se de um processo no qual há um disfarce na identificação dos dados pessoais de determinada pessoa, para que assim haja uma maior garantia da segurança de tais dados através de uma alteração em algum atributo exclusivo do titular de tais dados, por outro tipo de registro.[51]

Os dados pessoais que sofrerem o processo de pseudonimização se tornam disfarçados, pois algumas informações lhes são retiradas, com o objetivo de não se conseguir identificar o titular daqueles dados.

Contudo, as informações que são retiradas nesse processo ficam em posse de um controlador, para que quando necessário ele disponibilize tais informações, com a finalidade de conseguir "refazer toda a cadeia de identificação até se chegar novamente no titular de dados",[52] ou seja, "o titular do dado pseudonimizado só não é

49 Acerca de um maior aprofundamento acerca do estudo dos PET, recomenda-se a leitura de: BIONI, *op. cit.*

50 BRASIL. Lei nº 13.709, *op. cit.*

51 SOMBRA, Thiago Luís Santos. *Fundamentos da regulação da privacidade e proteção de dados pessoais*. São Paulo: Thomson Reuters Revistas dos Tribunais, 2019. p. 159.

52 *Ibidem*.

identificável por conta da separação entre ele e outra informação que levaria à identificação".[53]

A grande diferença entre a pseudonimização e a anonimização é que esta é um processo que objetiva tornar permanentemente anônimos determinados dados, enquanto na pseudonimização há a possibilidade de identificação do titular dos dados pseudonimizados, bastando, para tanto, que a pessoa responsável por guardar as informações adicionais as disponibilize, para que assim se consiga reidentificar o seu titular.[54]

Porém, tanto na anonimização quanto na pseudonimização, há uma supressão de informações dos dados pessoais a fim de impossibilitar a identificação destes dados com o seu titular. Tais supressões podem atingir, por exemplo: o CPF do titular dos dados ou o seu nome completo, localização geográfica, a idade, dentre outros dados que permitam a sua identificação.[55]

Em seu art. 13, §4º, a LGPD define a pseudononimização como um "tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro".[56]

O dispositivo mencionado acima se volta para a possibilidade de pseudonimização apenas para casos de estudos em saúde pública, quando na realidade esta medida de segurança deveria ser pensada para qualquer cenário em que há a utilização de dados sensíveis referentes à saúde.

53 KONDER, *op. cit.*, p. 453.

54 "A chamada 'anonimização' de dados pessoais – a retirada do vínculo da informação com a pessoa a qual se refere – é um recurso que algumas leis de proteção utilizam para diminuir os riscos presentes no seu tratamento. A mitigação de riscos é também obtida com técnicas como a da pseudonimização que, embora não torne o dado anônimo, pode dificultar a identificação do titular e é um recurso bastante utilizado". DONEDA, *op. cit.*, p. 140.

55 Nesse sentido, vide: BIONI, *op. cit.*, p. 62-63.

56 BRASIL. Lei nº 13.709, *op. cit.*

Em hospitais e clínicas médicas, por exemplo, a utilização da pseudonimização se mostra como um ótimo meio para evitar exposições desnecessárias de dados pessoais como prontuários médicos, pois os dados sensíveis gerados nos atendimentos não seriam identificáveis para grande parte dos funcionários, sendo que apenas o controlador ou determinados indivíduos teriam as informações adicionais necessárias para desfazer a pseudonimização e assim conseguir identificar o titular daqueles dados.

Isso traria um maior controle para que seja evitado o vazamento de dados sensíveis referentes à saúde, além de facilitar a identificação da origem dos vazamentos quando eles decorrerem da conduta de algum funcionário do hospital ou clínica.

A pseudonimização se vale de técnicas de segurança a fim de cumprir com seus objetivos; dentre elas está a criptografia, utilizada da seguinte maneira: uma chave privada tem a capacidade de revelar dados pessoais e assim proceder com a reidentificação dos seus titulares, contudo, apenas alguma(s) pessoa(s) detém esta chave.[57] Dessa forma, a criptografia trata-se de uma forma de linguagem com o objetivo assegurar o sigilo de comunicações.[58]

A criptografia se mostra como uma pretensa solução para o tratamento de dados pessoais constantes nos prontuários eletrônicos, sendo que se tais prontuários forem criptografados e apenas alguns funcionários (como, por exemplo, o diretor do hospital e os médicos) tiverem as chaves de acesso para cada caso, os dados sensíveis referentes à saúde teriam mais segurança em relação a vazamentos, pois haveria a possibilidade de identificar quem acessou tais dados com base na chave utilizada para tanto.[59]

57 Existem outras técnicas que também podem ser utilizadas pela pseudonimização, como: Função Hash e a Tokenização. Nesse sentido: SOMBRA, *op. cit.*, p. 160.

58 *Ibidem*, p. 161.

59 Ainda no que tange aos prontuários eletrônicos, cumpre salientar que a Lei nº 13.787/2018, em seu art. 5º, §2º, versando acerca dos documentos digitalizados

Além disso, transferências de dados pessoais entre clínicas e hospitais (envio de exames médicos para realização de procedimentos cirúrgicos, por exemplo) ficariam mais seguras com a criptografia, o que também coadunando-se coaduna com os princípios basilares da LGPD, como o da privacidade.

A criptografia combinada com a aplicação de tecnologias de inteligência artificial avançadas, pode se mostrar como uma boa solução para a prevenção dos vazamentos de dados.

Cientistas, hospitais e até a indústria farmacêutica, contam com bancos de dados que apresentam sintomas e testes de tratamentos de um grande número de pacientes, com a finalidade de se traçar padrões e dessa forma se obter cada vez mais êxito nas taxas de terapias. Os dados do coletivo, dizem muito mais, a nível de padronização, do que os dados individuais.

Contudo, de que forma se consegue obter a liberação dos dados relativos aos sintomas dos pacientes, sem que haja a lesão de dados confidenciais? Esse vem sendo um desafio no qual alguns institutos e empresas vem tentando solucionar.

O MIT (Instituto de Tecnologia de Massachusetts – EUA), por exemplo, desenvolveu um método de criptografia que protege os dados utilizados em redes neurais online. Esse método possui como finalidade possibilitar que as redes neurais baseadas em nuvem, analisem imagens médicas ou qualquer outro aplicativo que se valha de dados confidenciais.[60]

para a guarda, o armazenamento e o manuseio de prontuário de paciente, é clara ao afirmar que "Poderão ser implementados sistemas de certificação para a verificação da conformidade normativa dos processos referida no *caput* deste artigo", o que demonstra a total compatibilidade da criptografia no tratamento dos prontuários médicos eletrônicos.

60 MIT NEWS. More efficient security for cloud-based machine learning. Ver em https://news.mit.edu/2018/more-efficient-security-cloud-based-machine-learning-0817.

De outro lado, o Secure Al Labs (SAIL), fundado pela ex-aluna Anne Kim e pelo professor do MIT Manolis Kellis promete trazer uma tecnologia que permite que os algoritmos de inteligência artificial

> sejam executados em conjuntos de dados criptografados que nunca saem do sistema do proprietário dos dados. As organizações de saúde podem controlar como seus conjuntos de dados são usados, enquanto os pesquisadores podem proteger a confidencialidade de seus modelos e consultas de pesquisa. Nenhuma das partes precisa ver os dados ou o modelo para colaborar.[61]

Os avanços nas pesquisas referentes às proteções de dados médicos demonstram a possibilidade de uma maior segurança contra vazamentos de dados pessoais relacionados à saúde. A ideia é que os novos sistemas de proteção busquem detectar o que é informação desnecessária para a pesquisa, bem como dados que possibilitem a identificação dos pacientes, a fim de encriptá-los. O fato de a pseudonimização se configurar como importante processo para a proteção dos dados pessoais de saúde, não significa que essa medida protetiva não tenha fraquezas, sendo que a implantação deste processo, por si só, não irá erradicar os vazamentos de dados pessoais.

Em primeiro lugar, conforme visto acima, os processos de anonimização e de pseudonimização implicam na supressão de determinadas informações a fim de impedir a identificação do titular de determinados dados. Contudo, em alguns casos, mesmo que haja a supressão de informações – como nome completo, CPF, localização geográfica, dentre outros – se faz possível identificar o titular dos dados anonimizados, ou pseudonimizados, através da técnica chamada de *profiling*.

61 WINN, Zach. Secure AI Labs, Founded by Alumna Anne Kim and MIT Professor Manolis Kellis, Anonymizes data for AI Researchers. *MIT Schwarzman College of Computing*, Boston, 7 out. 2021. Disponível em: https://computing.mit.edu/news/enabling-ai-driven-health-advances-without-sacrificing-patient-privacy/. Acesso em: 15 mar. 2022.

O *profiling* é um método que busca a elaboração de perfis comportamentais das pessoas, a partir de informações que elas disponibilizam ou que são captadas.

> Os dados pessoais são tratados com o auxílio de métodos estatísticos e de técnicas de inteligência artificial, com o fim de se obter uma 'metainformação', que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destino de uma pessoa ou grupo [...]
> Um perfil assim obtido pode se transformar numa verdadeira representação virtual da pessoa, e pode ser o seu único aspecto visível a outros sujeitos que com ela terão algum tipo de interação.[62]

Dessa forma, muitas vezes o perfil das pessoas é construído a partir da interação das pessoas nas redes sociais a partir: das suas curtidas e comentários nas diversas publicações, ou das fotos que postam ou compartilham, ou seja, a partir de metadados, os quais estão previstos no art. 12, §2º da LGPD.[63]

Com isso, o *profiling* pode ser utilizado para que se obtenha informações capazes de identificar os titulares de dados pessoais anonimizados ou pseudonimizados.

Em 2006, por exemplo, a empresa AOL (America Online Labs), antigo *site* de buscas, divulgou um arquivo de 2 gigabytes com o histórico de busca de cerca de 650 mil usuários, suprimindo os nomes dos usuários mas mantendo outras informações como: números de seguro

62 DONEDA, *op. cit.*, p. 152.

63 "§2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada". BRASIL. Lei nº 13.709, *op. cit.*

social, nomes de família e telefones. Com base nestas informações e nos perfis traçados, foi possível identificar diversos titulares.[64]

O New York Times identificou diversas pessoas através das suas buscas na internet, sendo que eles chegaram a constatar o número de ID de uma mulher, a sua idade, onde ela vivia e até mesmo aspectos da sua personalidade, a partir das suas buscas realizadas através da AOL.[65]

Em outro caso, em 2007, a Netflix divulgou dados contendo 100 milhões de avaliações realizadas por 500 mil clientes. Foi realizado um processo de suposta anonimização substituindo os nomes dos clientes por IDs aleatórios, acrescidos de algumas variações nas avaliações.[66] Ocorre que

> Cruzando esta base de dados com a informação disponibilizada pela IMDB, investigadores da Universidade de Texas-Austin demonstraram que 99% dos registos poderiam ser potencialmente re-identificados, bastando para tal encontrar oito filmes em comum nas duas bases de dados. Com este exercício foi possível explicitar preferências políticas e outras informações sensíveis de clientes previamente identificados.[67]

Percebe-se que a questão do *profiling*, formado a partir de dados e metadados, possibilita desfazimento no processo de anonimização ou pseudonimização.

Outro ponto fraco da pseudonimizção se configura no seguinte fato: assim como as pessoas estão passíveis de serem vítimas de roubos ou

64 AOL expõe dados de seus usuários. *Folha de S. Paulo Informática*, São Paulo, 2016; AMERICA Online perde noção da realidade e divulga dados de 657.427 usuários. *MeioBit*, [*s. l.*], 2006.

65 GOMES, Marison. Privacidade diferencial e anonimização. *Privacy Tech*, [*s. l.*], 2019.

66 PINHO, Frederico António Sá Oliveira Pinho. Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados. 2017. Dissertação (Mestrado em Segurança Informática) – Universidade do Porto, Porto, 2017. p. 43.

67 *Ibidem*.

qualquer outro tipo de crime, os seus dados pessoais estão passíveis de sofrerem ataques de *hackers*. Em 2020, o Superior Tribunal de Justiça (STJ), o Ministério da Saúde e a Secretaria de Economia do Distrito Federal sofreram ataques de *hackers* em seus sistemas eletrônicos, o que demonstra que tanto as pessoas quanto o Estado estão passíveis de sofrer tais violações.[68]

Outro grande problema que pode até justificar diversos vazamentos de dados pessoais e até mesmo ataques de *hackers*, é a questão do investimento que é fornecido por parte das empresas e Administração Pública na instauração de sistemas protetivos, pois de nada adianta que a pseudonimização mostre-se como uma medida de segurança com forte potencial para ser um instrumento efetivo de proteção dos dados pessoais, se essa medida não tiver um bom investimento na sua aplicação.

Inclusive, acredita-se aqui que com o avanço da tecnologia, oportunizado por investimentos voltados à segurança dos dados pessoais, a pseudonimização possa se tornar um processo cada vez mais seguro e protegido de identificações mediante metadados ou de vazamentos diversos.

Porém, ainda que a pseudonimização seja um processo que não forneça total certeza acerca da proteção de dados pessoais, a sua utilidade deve ser enxergada sob o enfoque do *privacy by design*, ou seja, esse processo é necessário para que se alcance uma maior prevenção nos vazamentos de dados pessoais, sendo que a sua instauração nos sistemas de hospitais, clínicas, farmácias e demais prestadoras de saúde, torna-se imprescindível para a segurança dos pacientes/clientes.

O fato de a pseudonimização ter certas vulnerabilidades não faz com que haja a desconfiguração do seu caráter protetivo e preventivo,

68 TEMÓTEO, Antonio; MILITÃO, Eduardo. Após STJ, *hackers* atingem sistemas do Ministério da Saúde e governo do DF. *UOL*, Brasília, DF, 2020.

ou seja, não deixa de ser caracterizada como uma medida de segurança que visa a impedir e dificultar vazamentos de dados pessoais.

A busca pela evolução da pseudonimização está exatamente no reconhecimento das suas vulnerabilidades, a fim de serem sanadas. Aprende-se com suas fraquezas. Além disso, a pseudonimização não pode ser vista como a única medida protetiva dos dados pessoais, sendo que a sua efetividade depende de um trabalho conjunto com outros tipos de tutelas.

Assim, a instauração da pseudonimização mostra-se como uma das propostas que buscam consagrar os princípios da privacidade, igualdade, desenvolvimento da personalidade e dignidade, tendo por essência manter, prioritariamente, uma valorização dos aspectos existenciais do indivíduo, pois acima do que a pessoa tem, está o que ela é.

Conclusão

O advento da LGPD atribuiu aos dados sensíveis um regime jurídico especial voltado para a valorização da pessoa, priorizando em seus princípios aspectos existenciais importantes, com o objetivo de proteger direitos como a igualdade, a liberdade, a privacidade, a não discriminação e a dignidade da pessoa humana.

No que tange aos dados sensíveis referentes à saúde, observa-se que antes do advento da LGPD já existia uma forte regulamentação que visava a sua proteção, contudo, as legislações já existentes se mostraram inefetivas em relação à adesão por parte das pessoas, das empresas e da Administração Pública, uma vez que no plano fático constantemente os dados pessoais relacionados à saúde são expostos em vazamentos.

Com isso, há uma preocupação com a hipótese de a LGPD ser uma norma que irá se exaurir como um texto bonito inutilizado, ou se ela irá repercutir de forma significativa no plano fático, como uma lei de ampla adesão e forte aplicabilidade por parte da sociedade e do Estado.

É certo que a LGPD possui instrumentos protetivos dos dados pessoais, contudo, não se sabe se os seus dispositivos irão conseguir dar uma efetiva coibição aos vazamentos dos dados sensíveis à saúde, os quais possuem um forte potencial discriminatório.

Com isso, a pseudonimização, trazida pela LGPD, se mostra como uma promissora medida protetiva dos dados pessoais referentes à saúde. Utilizando-se da técnica referente à criptografia e à metodologia do *privacy by design*, a pseudonimização é uma medida de segurança que tem grandes chances de se tornar um grande processo coibidor de vazamentos de dados sensíveis de saúde.

Se faz importante demonstrar as fraquezas da pseudonimização para que o investimento na sua implantação seja feito tentando reduzir as vulnerabilidades que possam surgir, como defesas contra a reidentificação por causa de metadados ou proteção contra ataques de *hackers*.

A importância de pesquisar possíveis soluções aos vazamentos de dados, tem como fundamento trazer concretude a uma lei rica de instrumentos protetivos que, se utilizados, aderidos e investidos de forma correta, podem fazer com que a LGPD cumpra com os seus objetivos no plano fático, que são os de assegurar a privacidade, a igualdade, a liberdade, a não discriminação e a dignidade da pessoa humana, contribuindo assim com a valorização da pessoa e fomentando o desenvolvimento da sua personalidade.

Referências

AMERICA Online perde noção da realidade e divulga dados de 657.427 usuários. *MeioBit*, [*s. l.*], 2006. Disponível em: https://www1.tecnoblog.net/meiobit/2006/america-online-perde-nocao-da-realidade-e-divulga-dados-de-6/. Acesso em: 22 nov. 2020.

AOL expõe dados de seus usuários. *Folha de S. Paulo Informática*, São Paulo, 2016. Disponível em: https://www1.folha.uol.com.br/fsp/informat/fr1608200632.htm. Acesso em: 22 nov. 2020.

BARBOZA, Heloísa Helena; PEREIRA, Paula Moura Francesconi de Lemos Pereira; ALMEIDA, Vitor. Proteção dos dados pessoais da pessoa com deficiência. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revistas dos Tribunais, 2019. p. 531-560.

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

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. *Diário Oficial da União*: seção 1, Brasília, DF, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 24 nov. 2020.

BRASIL. Lei no 10.216, de 6 de abril de 2001. Dispõe sobre a proteção e os direitos das pessoas portadoras de transtornos mentais e redireciona o modelo assistencial em saúde mental. *Diário Oficial da União: seção 1, Brasília*, DF, ano 139, n. 69-E, p. 2, 7 abr. 20011. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10216.htm. Acesso em: 24 nov. 2020.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: seção 1, Brasília, DF, ano 151, n. 77, p. 1-3, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24 nov. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 nov. 2020.

BRASIL. Lei nº 13.787, de 27 de dezembro de 2018. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 249, p. 3, 28 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm. Acesso em: 24 nov. 2020.

BRASIL. Ministério da Saúde. *Plano brasileiro de preparação para enfrentamento de uma pandemia de influenza*. Brasília, DF: Ministério da Saúde, 2010. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/plano_brasileiro_pandemia_influenza_IV.pdf. Acesso: 20 nov. 2020.

BRASIL. Resolução nº 1.931/2009. Aprova o Código de Ética Médica. *Diário Oficial da União*: seção 1, Brasília, DF, p. 90, 24 set. 2009. Disponível em: https://portal.cfm.org.br/images/stories/biblioteca/codigo%20de%20etica%20medica.pdf. Acesso em: 25 nov. 2020.

BRASIL. Resolução nº 1.974/2011. Estabelece os critérios norteadores da propaganda em Medicina, conceituando os anúncios, a divulgação de assuntos médicos, o sensacionalismo, a autopromoção e as proibições referentes à matéria. *Diário Oficial da União*: seção 1, Brasília, DF, n. 160, 19 ago. 2011. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2011/1974. Acesso em: 25 nov. 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Thomson Reuters Revista dos Tribunais, 2019.

DUARTE, Marcella. Falha em sistema da Unimed expõe dados pessoais e até exames de pacientes. *UOL*, São Paulo, 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/11/17/falha-em-sistema-da-unimed-expoe-dados-pessoas-e-ate-exames-de-pacientes.htm. Acesso em: 20 nov. 2020.

FALHA de segurança expõe dados de milhares de pacientes do SUS em São Paulo. Disponível em: *Canaltech*, [*s. l.*], 2016. https://canaltech.com.br/seguranca/falha-de-seguranca-expoe-dados-de-milhares-de-pacientes-do-sus-em-sao-paulo-72271/. Acesso em: 22 nov. 2020.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters: Revistas dos Tribunais, 2019. p. 23-52.

FRAZÃO, Ana. Objetivos e alcance da lei geral de proteção de dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters: Revistas dos Tribunais, 2019. p. 99-129.

GOMES, Marison. Privacidade diferencial e anonimização. *Privacy Tech*, [*s. l.*], 2019. Disponível em: https://privacytech.com.br/artigos/privacidade-diferencial-e-anonimizacao,319897.jhtml. Acesso em: 22 nov. 2020.

IDEC cobra Anvisa por vazamento de dados de pacientes que usam canabidiol. *IDEC*, São Paulo, 2002. Disponível em: https://idec.org.br/noticia/idec-cobra-anvisa-por-vazamento-de-dados-de-pacientes-que-usam-canabidiol. Acesso em: 22 nov. 2020.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revistas dos Tribunais, 2019. p. 445-463.

LEI Marisa Letícia, que criminaliza divulgação de prontuário médico, é aprovada em Comissão da Câmara. *PT na Câmara*, [*s. l.*], 2018. Disponível em: https://ptnacamara.org.br/portal/2018/12/12/lei-marisa-leticia-que-criminaliza-divulgacao-de-prontuario-medico-e-aprovada-em-comissao-da-camara/. Acesso: 22 nov. 2020.

LISTA com nomes de pacientes com covid-19 vaza no norte do PR. *CNN Curitiba*, Curitiba, 2020. Disponível em: https://cbncuritiba.com/lista-com-nomes-pacientes-covid-19-vaza-norte-pr/. Acesso em: 20 nov. 2020.

LUCCA, Newton de; MACIEL, Renata Mota. A proteção de dados pessoais no Brasil a partir da Lei 13.709/2018: efetividade?. *In*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (coord.). *Direito Digital*: direito privado e internet. Indaiatuba: Foco, 2020. p. 211-228.

MATHESON, Rob. More Efficient Security for Cloud-Based Machine Learning. *MIT News*, Boston, 17 ago. 2018. Disponível em: https://news.mit.edu/2018/more-efficient-security-cloud-based-machine-learning-0817. Acesso em: 15 mar. 2022.

MELLO, Marco Aurélio. A igualdade e as ações afirmativas. *Revista Cidadania e Justiça*, Rio de Janeiro, 2002.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2019.

OLIVEIRA, Marco Aurélio Belizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revistas dos Tribunais, 2019. p. 53-83.

PEREIRA, Paula Moura Francesconi de Lemos. O uso da internet na prestação de serviços médicos. *In*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (coord.). *Direito Digital*: direito privado e internet. Indaiatuba: Ed. Foco, 2020. p. 429-466.

PINHO, Frederico António Sá Oliveira Pinho. Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados. 2017. Dissertação (Mestrado em Segurança Informática) – Universidade do Porto, Porto, 2017. Disponível em: http://oasisbr.ibict.br/vufind/Record/RCAP_1177c352299030ea983e79564487e407. Acesso em: 23 nov. 2020.

PRIVACIDADE Hackeada. Direção: Karim Amer e Jehane Noujaim. Estados Unidos: Netflix, 2019. (114 min).

RAPOSO, Paulo Marcelo Wanderley. Autonomia privada e autonomia da vontade em face das normas constitucionais. *In*: LOTUFO, Renan (coord.). *Direito Civil Constitucional*. São Paulo: Malheiros, 2002. p. 76-92. Caderno 3.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHAEFER, Fernanda. *Proteção de dados de saúde na sociedade de informação*: a busca pelo equilíbrio entre privacidade e interesse social. Curitiba: Juruá, 2010.

SEFAZ institui exigência de CPF em compras acima de R$ 400. *Sefaz Net*, Bahia, 2015. Disponível em: http://intranet.sefaz.ba.gov.br/scripts/fra_intra2.asp?corpo=http://intranet.sefaz.ba.gov.br/scripts/noticias/noticias.asp?LCOD_NOTICIA=6935. Acesso em: 24 nov. 2020.

SOMBRA, Thiago Luís Santos. *Fundamentos da regulação da privacidade e proteção de dados pessoais*. São Paulo: Thomson Reuters Revistas dos Tribunais, 2019.

SOUZA, Carlos Affonso Pereira de. Segurança e sigilo dos dados pessoais. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Revistas dos Tribunais, 2019. p. 417-441.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei Geral de Proteção de Dados Pessoais*: comentada artigo por artigo. Salvador: JusPodivm, 2020.

TEMÓTEO, Antonio; MILITÃO, Eduardo. Após STJ, *hackers* atingem sistemas do Ministério da Saúde e governo do DF. *UOL*, São Paulo, 2020. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2020/11/05/apos-stj-*hackers*-paralisam-sistemas-do-ministerio-da-saude-e-governo-do-df.htm. Acesso em: 22 nov. 2020.

VAZAMENTO de dados do E-Saúde expõe informações de milhões de brasileiros. *Fenafar*, [*s. l.*], 2018. Disponível em: https://www.fenafar.org.br/2016-01-26-09-32-20/saude/1992-vazamento-de-dados-do-e-saude-expoe-informacoes-de-milhoes-de-brasileiros. Acesso em: 2 0 nov. 2020.

VAZAMENTO de senhas do Ministério da Saúde expõe informações de pacientes de covid-19, diz jornal. *G1*, São Paulo, nov. 2011. Disponível em: https://g1.globo.com/bemestar/coronavirus/noticia/2020/11/26/vazamento-de-senhas-do-ministerio-da-saude-expoe-informacoes-de-pessoas-que-fizeram-testes-de-covid-19-diz-jornal.ghtml. Acesso em: 20 nov. 2020.

WINN, Zach. Secure AI Labs, Founded by Alumna Anne Kim and MIT Professor Manolis Kellis, Anonymizes data for AI Researchers. *MIT Schwarzman College of Computing*, Boston, 7 out. 2021. Disponível em: https://computing.mit.edu/news/enabling-ai-driven-health-advances-without-sacrificing-patient-privacy/. Acesso em: 15 mar. 2022.

PORNOGRAFIA *ON-LINE* E LGPD: INTERPRETANDO DADOS SENSÍVEIS

Fernando Araújo dos Santos

Introdução

A pornografia responde por 30% do tráfego total de dados na rede mundial de computadores.[1] Embora esse percentual tenha sido publicado há oito anos, tudo leva a crer que se ocorreu uma substancial modificação, certamente não foi em direção a uma diminuição.

Com o início da pandemia da covid-19 no mundo e o confinamento de milhões de pessoas em seus domicílios, os *sites* de conteúdo adulto registraram um considerável aumento de tráfego. O Pornhub, maior *site* pornográfico do mundo em quantidade de acessos, computou um aumento de 18% no número normal de visitas.[2] Uma pesquisa realizada no primeiro semestre de 2020 pela plataforma Netskope Security Cloud, revelou que o acesso a *sites* pornográficos aumentou cerca de 600%.[3]

A pornografia em si não é uma novidade na vida dos indivíduos. É inegável, no entanto, que com o advento da internet, um número crescente de pessoas passou a consumir material pornográfico motivadas

1 THORNHILL, Ted. Is the whole world looking at porn? Biggest site gets over four billion hits a month. *Dailymail*, [s. *l.*], 9 abr. 2012.

2 VIEIRA, Nathan. *Com a pandemia, aumenta a pornografia*: faz mal passar horas em sites pornô?. *Canaltech*, [s. *l.*], 19 maio 2020.

3 ALVES, Paulo. Acesso a sites pornôs cresce 600% em período de home office, diz pesquisa. *Techtudo*, [s. *l.*], 8 ago. 2020.

pela facilidade de acesso e pela sensação de anonimato que a rede aparentemente provoca em seus usuários.[4]

Essa sensação de anonimato, contudo, é apenas aparente. Pesquisas apontam que o consumo de pornografia *on-line* apresenta sérios riscos à privacidade do usuário, seja pela disponibilização indevida de seus dados pessoais a terceiros, seja pela vulnerabilidade tecnológica dos agentes de tratamento. As consequências dessas ações podem gerar danos variáveis e irreversíveis.

A título de ilustração, um dos mais emblemáticos vazamentos de dados relacionados à vida sexual foi o caso do *site* americano Ashley Madison. Com o slogan "A vida é curta, curta um caso", este *site* é conhecido por proporcionar encontros sexuais extraconjugais. Em agosto de 2015, *hackers* invadiram o banco de dados do *site* e tornaram públicos nomes, números de cartões de crédito, e-mails, endereços e preferências sexuais de cerca de 32 milhões de pessoas.[5] Como consequência, o estadunidense John Gibson, pastor e professor do Seminário Batista de Nova Orleans, após tomar conhecimento que seus dados estavam na lista publicada pelos *hackers*, cometeu suicídio.[6]

O exemplo, embora não tenha como objeto um *site* pornográfico, ajuda a compreender o grau de dano que a publicização de dados relacionados à vida sexual pode gerar. Isso coloca luz à necessidade de um rígido controle normativo sobre as empresas que operam *on-line* oferecendo serviços relacionados direta ou indiretamente à vida sexual das pessoas, o que inclui os sítios pornográficos.

4 MAÇARANDUBA, Pedro Ernesto Rodrigues. *Encenações do desejo*: contribuições para a iconologia do pornô. 2017. Dissertação (Mestrado em Psicologia em Saúde e Desenvolvimento) – Faculdade de Filosofia, Ciências e Letras de Ribeirão Preto, Universidade de São Paulo, Ribeirão Preto, 2017, p. 22.

5 ISIDORE, Chris; GOLDMAN, David. Ashley Madison hackers post millions of customer names. *CNN Business*, New York, 19 ago. 2015.

6 SEGALL, Laurie. Pastor outed on Ashley Madison commits suicide. *CNN Business*, New York, 8 set. 2015.

No Brasil, a promulgação da Lei Geral de Proteção de Dados (LGPD) conferiu expectativas de controle e proteção de dados mais adequadas às diversas relações jurídicas decorrentes do rápido avanço tecnológico no mundo contemporâneo. Há, contudo, um longo caminho a seguir. Estamos em um primeiro esforço de extrairmos da lei em questão normas compatíveis com as finalidades constitucionais, capazes de regular os mais variados casos concretos.

É neste contexto que esta pesquisa, em seus primeiros passos, finca os seus pilares. Ao analisar preliminarmente a política de privacidade de alguns *sites* pornográficos, duas questões chamaram atenção: a ideia de que parte dos dados pessoais dos usuários a serem tratados neste tipo de *site* não são dados sensíveis e, como consequência, a presença do legítimo interesse como uma das bases legais escolhidas para o tratamento. Destas questões, nosso estudo tem por objetivo buscar respostas aos seguintes problemas: Qual a natureza dos dados tratados por controladores de *sites* pornográficos? Mais precisamente, o que podemos entender como dados referentes à vida sexual, expressos no art. 5º, inciso II, da LGPD? Quais são as consequências dessa caracterização para o tratamento de dados? É possível a aplicação do legítimo interesse como base legal para o tratamento de alguns dados de usuários que consomem pornografia?

Interpretar um texto legal é buscar a norma visando a sua aplicação a casos concretos. A interpretação não pode ser entendida como uma ciência, mas sim, conforme leciona Eros Grau, como uma prudência, uma razão intuitiva que não diferencia o exato, mas sim o correto, não existindo apenas um correto para todos os casos possíveis.[7]

Partirmos da ideia de que a norma é uma moldura em que várias interpretações são possíveis.[8] Uma perspectiva restrita do que seriam

7 GRAU, Eros Roberto. *O direito posto e o direito pressuposto*. São Paulo: Malheiros, 2014. p. 24.

8 KELSEN, Hans. *Teoria Pura do Direito*. São Paulo: Martins Fontes, 2009. p. 390.

dados relacionados à vida sexual, entretanto, embora admissível a primeiro momento, talvez não seja capaz de atender às finalidades de proteção e controle de dados dispostas na própria LGPD e alicerçadas pela Constituição. É necessário, deste modo, uma interpretação contextualizada para melhor identificar quais seriam os dados relacionados à vida sexual, conforme analisaremos mais adiante. Isso determinará, por sua vez, as bases legais apropriadas para o tratamento de dados de um *site* pornográfico e, consequentemente, a validade do uso do legítimo interesse.

Devemos chamar atenção à importância deste estudo, embora a temática dos dados sensíveis esteja em voga nas inúmeras discussões acadêmicas sobre proteção e controle de dados pessoais. Em que pese já existir um expressivo debate no campo jurídico voltado ao tema da pornografia *on-line*,[9] o estudo centrado no controle e proteção de dados dos consumidores de pornografia na rede é um caminho praticamente inédito a se desbravar. Não encontramos nenhuma produção específica no Brasil e, até onde nossas investigações puderam alcançar, ainda existem poucas publicações sobre o tema no exterior.

Para fins didáticos, este capítulo foi dividido em duas partes. Na primeira parte, analisaremos algumas questões envolvendo a segurança de navegação em *sites* pornográficos. Demonstraremos que esta navegação, longe de ser um *tour* solitário, é permanentemente vigiada e muitas vezes abusivamente explorada pelos controladores, proporcionando grande insegurança à proteção e controle de dados dos usuários. Na segunda parte, discutiremos o conceito legal de dados sensíveis e a noção de dados referentes à vida sexual, dispostos na LGPD. Tendo como base as políticas de privacidade de alguns *sites* de pornografia, avaliaremos a compatibilidade dessas políticas com a lei de proteção de dados brasileira, no que diz respeito à classificação dos

9 No geral, esses estudos giram em torno dos seguintes tópicos: o acesso de crianças e adolescente a conteúdos eróticos, a questão da pornografia infantil e a pornografia de vingança (*revenge porn*).

dados pessoais a serem tratados. Analisaremos ainda as respectivas bases legais adotadas constantes nessas políticas de privacidade, bem como a sua adequação aos dados em questão.

Uma navegação permanentemente vigiada

Ao entrar na internet e acessar um *site* pornográfico, é natural a um indivíduo, sob a discrição inerente à sua intimidade, procurar um ambiente longe dos olhos de outras pessoas.[10] Pode parecer estranho, mas mesmo que tenha se certificando que esteja em um lugar reservado, ele não conseguirá evitar o fato de que seu comportamento será vigiado e que seus dados estão sendo tratados para os mais diversos fins, sendo compartilhados inclusive com terceiros.

Uma pesquisa americana realizada em 2019, tendo como objeto 22.484 *sites* de pornografia, apontou que destes *sites*, 93% vazam dados de seus usuários para terceiros. Do total, apenas 3.956 tinham política de privacidade, o que equivale a 17%. Os demais ou não possuíam ou apresentavam um grau de dificuldade elevado para o seu conhecimento.[11]

Em outro estudo similar, pesquisadores espanhóis, analisando 6.843 *sites*, concluíram que 72% deles utilizavam *cookies* de terceiros.[12] Entre os países que integram a União Europeia, o uso de *coo-*

10 Para o jurista argentino Ernesto Garzón Valdés, a zona íntima é reino total da liberdade dos indivíduos de pensar o que quiserem da forma que quiserem. Estaria livre de toda valoração moral, entendendo esta como um conjunto de regras que governam as relações interpessoais e não as relações entre homens e seres supra-empíricos como Deus. Em referência a Hobbes, afirma que o véu que protege a intimidade é a discrição e sua opacidade só seria reduzida em face da entrega ao amor ou ao cultivo de uma profunda amizade. GARZÓN VALDÉS, Ernesto. Privacidad y publicidade. *Doxa:* Cuadernos de Filosofía del Derecho, [*s. l.*], v. 1, n. 21, p. 223-244, 1998. p. 226.

11 MARIS, Elena; LIBERT, Timothy; HENRICHSEN, Jennifer. Tracking sex: the implications of widespread sexual data leakage and tracking on porn websites. *Cornell University,* New York, p. 1-11, 2019. p. 4.

12 São um tipo de *cookies* criados por terceiros (outros sites), presentes no site que o usuário estaria acessando (geralmente por meio de anúncios) e capazes de rastrear sua navegação.

kies é regulamentado pela *General Data Protection Regulation* (GDPR), que prescreve a necessidade do consentimento do usuário diante de qualquer meio que possa identificá-lo, o que geralmente é feito por formulários de consentimento. Deste universo de *sites* pornográficos que usam *cookies* de rastreamento, ainda segundo a pesquisa, apenas 4% possuíam *banners* de consentimento de *cookies*, dos quais 32% não apresentavam nenhuma possibilidade de controle por parte do usuário, tendo apenas natureza informativa.[13]

É certo que um *site* pornográfico não é menos seguro ou menos transparente do que as centenas de milhares de outros tipos de *sites* que cotidianamente são acessados na rede. Além da insegurança e falta de transparência, o que torna a navegação em um *site* deste gênero delicada *per si* é o tipo de lesão que um vazamento ou um tratamento abusivo pode causar.

Influenciado pela GDPR, o legislador brasileiro deu especial atenção aos dados referentes à vida sexual, elevando-os à categoria de dados sensíveis, tal qual expresso no art. 5º, II, da LGPD. Embora não definidos pelo diploma normativo em questão, os dados sensíveis, segundo entendimento doutrinário, se diferenciam dos demais dados pessoais pelo risco que sua manipulação proporcione relações discriminatórias e desiguais entre as pessoas. Estes dados integrariam, portanto, uma espécie de "núcleo duro" da privacidade.[14]

13 VALLINA, Pelayo *et al*. Tales from the Porn: A Comprehensive Privacy Analysis of the Web Porn Ecosystem. *In*: INTERNET MEASUREMENT CONFERENCE, 2019, Amsterdam. *Annals* [...]. Amsterdam: IMC, 2019. p. 10.

14 "Procura-se individuar o 'núcleo duro' da privacidade em torno de dados relativos a opiniões políticas, sindicais ou de qualquer outro gênero, fé religiosa, raça, saúde, hábitos sexuais...". RODOTÀ, Stefano. *A vida na sociedade de vigilância*: privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 78. Ver também: TEFFÉ, Chiara Spadaccini de; VIOLA, Mário. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*, Rio de Janeiro, ano 9, n. 1, 2020; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon; NEGRI, Sergio Marcos Carvalho de Ávila. A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias*, [s. *l*.], v. 5, n. 1, p. 63-85, 2019.

A ofensa a esse território da vida privada pode causar danos incalculáveis aos indivíduos. Um dos aspectos da privacidade, não o único, é resguardar justamente aquilo que queremos esconder, seja por simples opção individual ou por medo do descrédito social pautado pelo julgamento moral.[15] Em muitos casos, os efeitos discriminatórios podem ser desencadeados pelo próprio Estado.

Existem diversos locais do mundo em que a publicização de dados referentes à vida sexual do indivíduo pode trazer sérios riscos à sua integridade. Segundo relatório da *International Lesbian, Gay, Bisexual, Trans And Intersex Association* (ILGA), atualmente 71 países criminalizam a homossexualidade, dos quais 4 têm previsão de pena de morte.[16]

Temos aí uma questão delicada. Da já mencionada pesquisa americana realizada em 22.484 *sites* pornográficos, em 44,97% deles é possível inferir preferências de gênero tão somente a partir de suas URLs, ou seja, precisa-se de muito pouco para se chegar a conclusões sobre a vida sexual de uma pessoa.[17] É bem elucidativo o que revelam os autores:

> Many domains in our sample illustrate how quickly nuance might be lost in favor of exposure, panic and severe consequences. Sites like 'momboysex.ws,' 'freerapeporn.org,' and

15 SOLOVE, Daniel J. 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, San Diego, v. 44, n. 289, p. 7425-7772, 2007. p. 769.

16 São eles: Arábia Saudita, Nigéria, Sudão e Somália. MENDOS, Lucas Ramón. *Homofobia de Estado*: actualización del panorama global de la legislación. Genebra: ILGA, 2019.

17 Tal inferência, entretanto, não é necessariamente verdadeira. Pesquisas revelam que o consumo de pornografia não necessariamente equivale a identidade sexual, sendo possível uma pessoa consumir pornografia gay sem se identificar como gay (cf. MARIS, *op. cit.*). O consumo de pornografia é o campo de desejos e experiências que aparentemente podem ser estranhas, mas quando estudadas mostram muitas dimensões inexploradas do comportamento humano. Dados apresentados pelo Pornhub revelaram que 37% da audiência de vídeos com relações sexuais entre homens são de mulheres e que esse gênero pornô é o mais assistido entre as mulheres. Ver: NEVILLE, Lucy. *Girls who like boys who like boys*: women and gay male pornography and erótica. Cham: Palgrave Macmillan, 2018. p. 2.

> 'pornwithanimals.net' would create scandal amid revelations they were frequented by a public figure, as well as personal/professional fallout for an ordinary citizen.[18]

Dentro do quadro em que a internet ganhou forma nas últimas décadas, é comum que, assim como na TV aberta, a possibilidade de fornecimento e consumo dos mais diversos serviços, muitos deles gratuitos, seja acompanhada pelo interesse das empresas que atuam na rede em abrir espaço para formas de monetização de seus conteúdos. Mesmo quando o serviço é pago, não soa estranho o interesse comercial desses grupos em fidelizar o usuário, criando elos que possibilitem o conhecimento mais profundo dos seus hábitos.

Se a detenção de uma rica gama de dados pessoais vem se tornando o novo petróleo do século XXI, entretanto, é imperativo que o tratamento dessas informações seja efetivamente regulado e fiscalizado, não para impedir as relações descritas acima, uma vez que é possível que se trate de um processo inevitável. Deve-se impedir o abuso, garantindo aos usuários a primazia do controle e proteção de seus dados. É preciso assegurar não somente a privacidade dos indivíduos, mas também a autonomia deles em relação aos seus dados. Isso deve se dar em todas as esferas, mesmo naquelas que sejam objeto de controle e permanente contestação moral como o consumo de material pornográfico.

A questão dos dados sensíveis

No Brasil, onde a produção, comercialização e consumo de material erótico não é proibido pelo Estado, o advento da LGPD atingiu também as empresas deste ramo. Isso fez com que muitos *sites* de conteúdo pornográfico iniciassem um processo de adaptação às novas regras de proteção e controle de dados pessoais.

18 MARIS, *op. cit.*, p. 9.

Em análise preliminar sobre a política de privacidade de alguns deles, chamou atenção a utilização do legítimo interesse como base para o tratamento de dados pessoais. A utilização do termo em questão se dá de maneira expressa conforme podemos perceber na política de um famoso *site* pornográfico nacional:

> Só usaremos seus dados pessoais quando a lei local aplicável nos permitir. Geralmente, usaremos seus dados pessoais nas seguintes circunstâncias:
> • Para fins de prestação de serviços, gerenciamento de clientes e funcionalidade e segurança, conforme necessário para executar os serviços fornecidos a você sob nossos termos e condições e qualquer outro contrato que você tenha conosco.
> • Onde for necessário para *nossos interesses legítimos (ou de terceiros) e seus interesses e direitos fundamentais não os substituírem*.
> • Onde precisamos cumprir uma obrigação legal ou regulamentar. Observe que podemos processar seus dados pessoais por mais de um motivo legal, dependendo da finalidade específica para a qual estamos usando seus dados.[19]

O mesmo ocorre em outro *site* também muito acessado no Brasil:

> 3. Forma de utilização dos Dados Pessoais do usuário
> Utilizamos os Dados Pessoais do usuário para oferecê-lo produtos, serviços, enviá-lo comunicações, campanhas de marketing ou realizar outras operações, tais como a utilização de dados para melhorar e personalizar sua experiência. Segue alguns exemplos da forma de utilização de Dados Pessoais de usuários:
> [...]
> Sugestões e recomendações aos usuários de nosso Website sobre os produtos e serviços que possam ser de seu interesse (*sendo a base legal de tal processo nosso interesse legítimo, mais especificamente, nosso interesse econômico em desenvolver nossos produtos e serviços e expandir nossos negócios*).

19 POLÍTICA de Privacidade. *Brasileirinhas*, [*s. l.*], 1 jan. 2020, grifo nosso.

> Para fins do disposto acima,
> *interesse legítimo significa o nosso interesse em operar e administrar nossos negócios para que possamos oferecer ao usuário o melhor serviço/produto e a melhor e mais segura experiência. Analisamos e ponderamos todo e qualquer possível impacto (positivo e negativo) sobre o usuário e seus direitos antes de processar seus Dados Pessoais em nosso interesse legítimo*. Não utilizamos seus Dados Pessoais caso nossos interesses sejam sobrepujados pelo impacto sobre o usuário (a menos que o usuário dê sua autorização ou seja de outra forma obrigado ou autorizado por lei para tanto). Entre em contato para maiores informações sobre como avaliamos nossos interesses legítimos em detrimento de qualquer possível impacto sobre o usuário com relação a qualquer atividade específica.[20]

O legítimo interesse é uma das bases legais dispostas no inciso IX do art. 7º, da LGPD. É um dos meios que permite o tratamento de dados sem a necessidade de consentimento do titular, "quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso em que prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". O inciso em questão é complementado com o art. 10 do mesmo diploma normativo, que tenta definir algumas diretrizes para a aplicação dessa base legal.

Praticamente uma cópia do disposto na GDPR, para muitos juristas a noção legal de legítimo interesse peca pela vagueza, dando a ideia de que, com o receio de proibir situações futuras razoáveis, legítimas ou socialmente relevantes de tratamento por parte dos agentes que fossem imprevisíveis naquele momento, o legislador incluiu uma permissão aberta.[21]

20 POLÍTICA de Privacidade. *Cameraprive.Com*, [*s. l.*], 24 jul. 2018, grifo nosso.

21 MARCACINI, Augusto Tavares Rosa. Regras aplicadas ao tratamento de dados pessoais. *In*: LIMA, Cíntia Rosa Pereira de (coord.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020. p. 153.

Diferente do art. 7º, que trata de dados pessoais gerais, o art. 11, que versa sobre as bases legais para tratamento de dados sensíveis, não contemplou o legítimo interesse em seus incisos. Importante ter em mente que ambos os artigos possuem róis taxativos, segundo entendimento de muitos juristas.[22] Somos levados, portanto, a inferir que ou de imediato as políticas de privacidade por nós mencionadas seriam contrárias à LGPD ou existiria por parte delas um entendimento de que não estariam sujeitas ao art. 11, por não estarem se referindo ao tratamento de dados sensíveis. Conforme podemos perceber abaixo, é possível que prevaleça aqui o segundo entendimento.

> *Não coletamos categorias especiais de informações pessoais sobre você (isso inclui detalhes sobre sua raça ou etnia, crenças religiosas ou filosóficas, opiniões políticas, associação a sindicatos, informações sobre sua saúde e dados genéticos e biométricos)*. No entanto, dependendo de como você usa nosso site e serviços, suas informações pessoais podem incluir informações que permitem tirar conclusões sobre sua vida sexual ou orientação sexual ('informações pessoais sensíveis'). A coleta, o uso e a divulgação dessas informações pessoais sensíveis são necessárias para fornecer alguns de nossos serviços a você.[23]

Observe que essa política afirma que não se coleta informações pessoais sensíveis, no entanto, esclarece ser possível, pela forma que o usuário utiliza o *site*, incluir informações pelas quais podem ser deduzidos dados referentes à sua vida sexual, por isso, dados de natureza sensível. Isso nos leva a entender que alguns *sites* pornográficos estão fazendo uso do legítimo interesse para o tratamento de dados pessoais, sob alegação de que nem todos os dados a serem tratados por eles seriam sensíveis. Mais uma vez, as inferências que podem ser

22 TEFFÉ; VIOLA, *op. cit.*, p. 4.

23 POLÍTICA..., 2020.

geradas acerca da vida sexual dos usuários dependem tão somente da forma pela eles estes usam os serviços do *site*.

Dado a natureza de um *site* pornográfico, é possível separar dados pessoais de um usuário e tratá-los como dados não sensíveis? É preciso que retomemos algumas considerações sobre os dados sensíveis.

Como já exposto, existe um entendimento doutrinário majoritário que relaciona dados sensíveis à ideia de dados pelos quais há um potencial surgimento de comportamentos discriminatórios em seu tratamento. Não se trata, entretanto, somente de comportamentos discriminatórios. Segundo o Guia do Regulamento Geral de Proteção de Dados elaborado pela Information Commissioner's Office (ICO), autoridade de proteção de dados do Reino Unido, além do risco discriminatório, o tratamento dessa categoria de dados pode gerar diversos riscos que envolvem a liberdade de pensamento, consciência e religião; liberdade de expressão, liberdade de reunião e associação; direito à integridade corporal e direito à vida privada e familiar.[24]

Tendo em vista o potencial ofensivo a uma série de direitos fundamentais dessa categoria de dados, a LGPD conferiu maior proteção, restringindo as próprias bases legais para seu tratamento. Além disso, para casos em que o consentimento deva ser aplicado, tornou-o ainda mais substancial, exigindo forma específica, destacada e para determinados fins, conforme previsto no inciso I do art. 11 da referida lei.

Ante o esforço em interpretar o que são dados sensíveis no caso concreto ora aqui trazido, é possível afirmar que estamos diante de um quadro de textura aberta, não apenas no que diz respeito a determinar quais são esses tipos de dados, mas, ao que mais nos interessa, àquilo que podemos entender como dados referentes à vida sexual.

Textura aberta é uma espécie de imprecisão linguística. Conforme lição do jurista argentino Carlos Santiago Nino, "até mesmo as palavras

24 INFORMATION COMMISSIONER'S OFFICE. *Guide to the General Data Protection Regulation (GDPR). [S. l.: s. n.]*, 2018.

mais precisas podem suscitar dúvidas sobre sua aplicabilidade, perante circunstâncias insólitas e imprevistas".[25]

Uma norma jurídica, mesmo dotada de aplicação clara a uma série de situações concretas, em determinadas circunstâncias, poderá se deparar com casos imprecisos. Para Hart, "a incerteza nas zonas limítrofes é o preço a pagar pelo uso de termos classificatórios gerais em qualquer forma de comunicação referente a questões factuais".[26] Isso é compreensível, uma vez que os legisladores são homens do seu tempo. É humanamente impossível uma norma abarcar todas as circunstâncias fáticas de seu objeto *a priori*, mesmo porque muitas delas só se tornarão evidentes a partir de situações concretas estabelecidas *a posteriori*. Assim:

> Quando o caso imprevisto vier efetivamente a ocorrer, confrontaremos os problemas em pauta e então poderemos resolvê-lo escolhendo entre os interesses conflitantes da forma que melhor nos satisfazer. Ao fazê-lo, teremos tornado nosso objetivo inicial mais preciso e teremos ainda, incidentalmente, solucionado uma questão relativa ao sentido de um termo genérico para os efeitos dessa norma.[27]

A textura aberta de uma norma possibilita a atividade criadora de órgãos administrativos ou tribunais. Isso vai muito além daquilo que o referido jurista inglês chama criticamente de formalismo verbal e sua tentativa de "buscar a intenção do legislador e fazer referência ao direito já existente". A atividade criadora é um esforço de "equilíbrio entre pesos conflitantes, os quais estes variam de caso a caso".[28]

25 NINO, Carlos Santiago. *Introdução à análise do direito*. São Paulo: Martins Fontes, 2015. p. 314.

26 HART, Herbert Lionel Adolphus. *O conceito de direito*. São Paulo: Martins Fontes, 2012. p. 166.

27 HART, *op. cit.*, p. 167-168.

28 HART, *op. cit.*, p. 175-176.

Trazendo essa discussão ao nosso problema e até onde esta pesquisa caminhou, o acesso de usuários a *sites* pornográficos não permite uma concepção restrita do que sejam dados referentes à vida sexual. Registros de navegação indicando quais gêneros pornográficos um usuário acessou e mensagens em *chats* eróticos identificando suas preferências sexuais são casos claros que evidenciam esses tipos de dados. No entanto, dados comuns, como cartão de crédito, CPF, RG, nome do usuário, dados de geolocalização e IP, também devem ser considerados informações sensíveis, uma vez que a sua presença na base de dados de *sites* pornográficos por si só já revela elementos da vida sexual. No mínimo, já revela que seu titular faz uso de pornografia.

Os dois exemplos utilizados na parte inicial deste capítulo confirmam claramente isso. Para um pastor batista, o simples fato de seu e-mail, nome e cartão de crédito estarem vinculados a um *site* famoso por proporcionar aventuras extraconjugais já seria o suficiente para gerar grave dano à sua intimidade. Da mesma forma, a exposição de dados de geolocalização e endereço de IP quando relacionados com *sites* como "gaytube.com", levaria uma pessoa a potencialmente correr risco em países onde a homossexualidade é criminalizada ou socialmente reprimida. Essa visão mais ampla sobre dados sensíveis é harmônica com a de muitos juristas brasileiros e já vinha sendo defendida muito antes do advento da LGPD, no contexto das relações de consumo.[29] A título de reforço, mister são as considerações de Bioni:

> Ainda que, assim como um dado anônimo pode se tornar um dado pessoal, um dado 'trivial' pode também se transmudar em um dado sensível; particularmente, quando se têm disponíveis

29 "... Com as modernas técnicas estatísticas e de análise de dados, até mesmo informações pessoais que, em si, não são sensíveis podem causar tanto (I) um tratamento discriminatório em si, quanto (II) a dedução ou inferência de dados sensíveis obtidos a partir de dados pessoais não-sensíveis [...]". DONEDA, Danilo. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Brasília, DF: SDE: DPDC, 2010. p. 27.

> tecnologias (e.g., Big Data) que permitem correlacionar uma série de dados para prever comportamentos e acontecimentos, tal como ocorreu com a loja de departamentos que identificou quais consumidoras estariam grávidas, precisando, inclusive, o período gestacional.
> É possível, portanto, identificar individualidades mais sensíveis das pessoas, tais como orientação sexual, raça e estado de saúde, a partir de informações triviais. A título de exemplo, segundo um estudo da Universidade de Cambridge, as 'curtidas' em uma rede social podem criar um retrato fiel dos gostos e preferências dos usuários por meio do qual poderiam ser extraídos diversos tipos de inferências. A pesquisa identificou com exatidão a porcentagem dos usuários homossexuais e heterossexuais, os usuários brancos e negros e, por fim, quais teriam uma ligação partidária republicana ou democrata.[30]

Defender uma concepção mais ampla para os dados sensíveis, portanto, se mostra em perfeita consonância com os objetivos da própria LGPD, cuja preocupação em dotar de maior proteção uma categoria especial de dados é notória. Isso faz com que, em situações concretas, o quadro de possibilidades que aciona atividade criadora do juiz, decorrente da textura aberta da norma jurídica, deva ser sempre preenchido levando em consideração tal perspectiva.[31]

Por fim, se todos os dados pessoais tratados por operadores de *sites* pornográficos devem ser considerados sensíveis, não há que se falar de legítimo interesse como forma possível de tratamento destes dados. A LGPD é clara ao diferenciar as bases legais para tratamento de dados pessoais comuns, constantes no art. 7º, das bases legais para tratamento de dados sensíveis, previstas no art. 11.

30 BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Ed. Forense, 2019. p. 84.

31 "Com muita frequência, sua escolha é guiada pelo pressuposto de que o objetivo das normas que estão interpretando é razoável, de modo que estas não se destinam a perpetrar a injustiça ou ofender princípios morais estabelecidos". HART, *op. cit.*, p. 264.

Conclusão

De modo preliminar, constatamos que na política de privacidade de alguns *sites* pornográficos, há uma leitura própria acerca do que pode ser considerado dados sensíveis. Uma visão restrita, principalmente daquilo que se poderia entender como dados referentes à vida sexual. Essa opção é muito conveniente ao controlador, pois permite o uso do legítimo interesse como base de tratamento de dados, o que possibilita uma maior dinâmica em suas ações comerciais, de *marketing* e de fidelização, além de parcerias com terceiros. Para o usuário, no entanto, um sinal de alerta deve ser ligado. A perda de parte do controle direto dos seus dados para atender às finalidades únicas do controlador revela uma ofensa flagrante ao direito de controle das suas próprias informações, justamente aquelas que, se usadas de forma abusiva ou publicizadas, são capazes de causar graves prejuízos.

Alicerçados pela ideia de textura aberta proposta por Hart, que aponta para natureza incompleta das normas formadas a partir de termos genéricos e para a possibilidade de atividade criativa do juiz no preenchimento dessa incompletude, observamos que dados triviais também podem assumir a natureza de dados sensíveis quando avaliados à luz de casos concretos. Essa perspectiva já vem sendo defendida por boa parte dos pesquisadores dedicados ao estudo do controle e proteção de dados. É de se esperar, portanto, ou da Autoridade Nacional de Proteção de Dados (ANPD) ou do Poder Judiciário, o enfrentamento dessa questão.

Concluímos que se todos os dados pessoais obtidos por *sites* pornográficos devem ser considerados sensíveis, não será possível tratá-los com base no legítimo interesse por falta de previsão no art. 11, da LGPD.

Referências

ALVES, Paulo. Acesso a sites pornôs cresce 600% em período de home office, diz pesquisa. *Techtudo*, [*s. l.*], 8 ago. 2020. Disponível em: https://www.techtudo.com.br/noticias/2020/08/acesso-a-sites-pornos-cresce-600percent-em-periodo-de-home-office-diz-pesquisa.ghtml. Acesso em: 10 set. 2020.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709. Acesso em: 11 set. 2020.

DONEDA, Danilo. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Brasília, DF: SDE: DPDC, 2010. Disponível em: https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf. Acesso em: 11 set. 2020.

GARZÓN VALDÉS, Ernesto. Privacidad y publicidade. *Doxa:* Cuadernos de Filosofía del Derecho, [*s. l.*], n. 21-v1, p. 223-244, 1998. Disponível em: https://doxa.ua.es/article/view/1998-v1-n21-privacidad-y-publicidad. Acesso em: 17 dez. 2020.

GRAU, Eros Roberto. *O direito posto e o direito pressuposto*. São Paulo: Malheiros, 2014.

HART, Herbert Lionel Adolphus. *O Conceito de Direito*. São Paulo: Martins Fontes, 2012.

INFORMATION COMMISSIONER'S OFFICE. *Guide to the General Data Protection Regulation (GDPR)*. [*S. l.: s. n.*], 2018. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Acesso em: 12 set. 2020.

ISIDORE, Chris; GOLDMAN, David. Ashley Madison hackers post millions of customer names. *CNN Business*, New York, 19 ago. 2015. Disponível em: https://money.cnn.com/2015/08/18/technology/ashley-madison-data-dump/index.html?iid=EL. Acesso em: 12 set. 2020.

KELSEN, Hans. *Teoria Pura do Direito*. São Paulo: Martins Fontes, 2009.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon; NEGRI, Sergio Marcos Carvalho de Ávila. A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias*, *[s. l.]*, v. 5, n. 1, p. 63-85, 2019. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf. Acesso em: 10 out. 2020.

MAÇARANDUBA, Pedro Ernesto Rodrigues. *Encenações do desejo*: contribuições para a iconologia do pornô. 2017. Dissertação (Mestrado em Psicologia em Saúde e Desenvolvimento) – Faculdade de Filosofia, Ciências e Letras de Ribeirão Preto, Universidade de São Paulo, Ribeirão Preto, 2017. Disponível em: https://www.teses.usp.br/teses/disponiveis/59/59141/tde-12122017-110913/pt-br.php. Acesso em: 14 set. 2020.

MARCACINI, Augusto Tavares Rosa. Regras aplicadas ao tratamento de dados pessoais. *In*: LIMA, Cíntia Rosa Pereira de (coord.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020. p. 141-163.

MARIS, Elena; LIBERT, Timothy; HENRICHSEN, Jennifer. Tracking sex: the implications of widespread sexual data leakage and tracking on porn websites. *Cornell University*, New York, p. 1-11, 2019. Disponível em: http://arxiv.org/abs/1907.06520. Acesso em: 17 dez. 2020.

MENDOS, Lucas Ramón. *Homofobia de Estado*: actualización del Panorama Global de la Legislación. Genebra: ILGA, 2019. Disponível em: https://ilga.org/downloads/ILGA_World_Homofobia_de_Estado_Actualizacion_Panorama_global_Legislacion_diciembre_2019.pdf. Acesso em: 11 set. 2020.

NEVILLE, Lucy. *Girls who like boys who like boys*: women and gay male pornography and erótica. Cham: Palgrave Macmillan, 2018. Disponível em: https://link.springer.com/book/10.1007%2F978-3-319-69134-3. Acesso em: 11 nov. 2020.

NINO, Carlos Santiago. *Introdução à Análise do Direito*. São Paulo: Martins Fontes, 2015.

POLÍTICA de Privacidade. *Brasileirinhas*, [*s. l.*], 1 jan. 2020. Disponível em: https://www.brasileirinhas.com.br/politica-de-privacidade.html. Acesso em: 11 set. 2020.

POLÍTICA de Privacidade. *Cameraprive.Com*, [*s. l.*], 24 jul. 2018. Disponível em: https://cameraprive.com/br/legal/privacy-policy. Acesso em: 11 set. 2020.

RODOTÀ, Stefano. *A vida na sociedade de vigilância*: privacidade hoje. Rio de Janeiro: Renovar, 2008.

SEGALL, Laurie. Pastor outed on Ashley Madison commits suicide. *CNN Business*, New York, 8 set. 2015. Disponível em: https://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/. Acesso em: 12 set. 2020.

SOLOVE, Daniel J. 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, San Diego, v. 44, GWU Law School Public Law Research Paper No. 289, p. 7425-7772, 2007. Disponível em: https://ssrn.com/abstract=998565. Acesso em: 12 set. 2020.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mário. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*, Rio de Janeiro, ano 9, n. 1, 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd. Acesso em: 10 nov. 2020.

THORNHILL, Ted. Is the whole world looking at porn? Biggest site gets over four billion hits a month. *Dailymail*, [*s. l.*], 2012. Disponível em: https://www.dailymail.co.uk/sciencetech/article-2127201/Porn-site-Xvideos-worlds-biggest-4bn-hits-month-30-web-traffic-porn.html. Acesso em: 12 set. 2020.

VALLINA, Pelayo *et al.* Tales from the Porn: A Comprehensive Privacy Analysis of the Web Porn Ecosystem. *In*: INTERNET MEASUREMENT CONFERENCE, 2019, Amsterdam. *Annals* [...]. Amsterdam: IMC, 2019. Disponível em: http://doi.org/10.5281/zenodo.3462051. Acesso em: 17 dez. 2020.

VIEIRA, Nathan. Com a pandemia, aumenta a pornografia: faz mal passar horas em sites pornô?. *Canaltech*, [*s. l.*], 19 maio 2020. Disponível em: https://canaltech.com.br/saude/com-a-pandemia-aumenta-a-pornografia-faz-mal-passar-horas-em-sites-porno-163634/. Acesso em: 11 set. 2020.

DADOS PESSOAIS E POLARIZAÇÃO POLÍTICA: ANÁLISE ACERCA DA LIBERDADE DE INFORMAÇÃO NO MUNDO DIGITAL

Rafaela Lamêgo e Aquino Rodrigues de Freitas

Introdução

Na maioria das distopias já publicadas, o Estado é quem exerce o papel de vigilante autoritário e arbitrário. Nesse sentido, o desenvolvimento de governos totalitários, de fato, tem como um dos seus pilares o controle da população, principalmente no que se refere ao acesso e divulgação de informações.

Historicamente, houve diversas tentativas de controle das mídias tradicionais em ditaduras e até em democracias, por meio de *lobby* de grupos hegemônicos. Dessa maneira, o surgimento da internet trouxe uma esperança que beirava a euforia: era a promessa de um meio de comunicação popular, em que qualquer um poderia *acessar* e *disseminar* gratuitamente qualquer informação.

Contudo, o ambiente digital está longe de ser um paraíso democratizante, trata-se de um mercado muito lucrativo e governado por pouquíssimas empresas bilionárias. Nesse contexto, o preço do uso das redes é a concessão dos nossos dados pessoais, uma vez que estes são usados para criar perfis individualizados das nossas crenças, hábitos e opiniões. Assim, os *websites* tornam-se uma agência publicitária ideal,

direcionando os anúncios especificamente para os usuários propícios a estarem interessados.

Todavia, tal crivo não se limita a produtos propriamente ditos, ele abarca também notícias, artigos e conteúdos políticos. Dessa maneira, as infinitas informações contidas no mundo digital são filtradas e nossa autonomia informacional, por sua vez, limitada.

Nesse cenário, não é o governo que exerce – diretamente, ao menos – o papel de vigilante, mas empresas multinacionais que não obstante infringirem a privacidade do usuário, também interferem em sua autonomia política, limitando o acesso à informação de acordo com os parâmetros publicitários que regem suas redes. Ocorre que a manipulação da divulgação de informação na internet é realizada de forma oculta, escondida pelos longos termos de adesão dos *websites* e fantasiada sob o manto de um ambiente popular, livre e autônomo.

Dessa forma, o presente trabalho objetiva compreender o componente capitalista que dita a lógica do mundo digital, analisando se as consequências sociais do uso de filtros ideológicos por parte das grandes empresas interferem no processo de polarização política. Ademais, visa examinar a liberdade de informação e o direito da coletividade ao acesso à informação – considerando seus objetivos sociais e democráticos –, contrapondo os referidos preceitos constitucionais às práticas dos monopólios digitais. Por fim, analisa o papel da legislação brasileira como ferramenta de controle dos excessos das empresas privadas no ambiente digital.

Aplicou-se o método dedutivo e hipotético-dedutivo, por meio de pesquisas bibliográficas, legislativas e jurisprudenciais. Nesse sentido, de início questionou-se acerca da liberdade no mundo digital, frente à existência de monopólios e dos filtros ideológicos como norteadores da divulgação de informação nas redes. Posteriormente, foram propostas duas hipóteses submetidas ao processo de falseamento: a polarização política como resultado da bolha dos filtros e a lógica dos

algoritmos como violação aos objetivos democráticos intrínsecos à liberdade de informação.

Dados informacionais e os novos monopólios: a internet é um espaço politicamente livre?

O mundo digital e sua suposta oferta de conhecimento ilimitado, despertando uma sociedade de informação, apresentam-se como uma promessa muitas vezes utópica.[1] A internet surge como um ambiente aparentemente livre, onde qualquer cidadão comum tem, de forma inédita, o poder de apresentar-se como porta-voz de suas crenças e ser, de fato, ouvido – sem passar pelo crivo das mídias tradicionais, como redes de televisão, rádio ou jornais.[2] Dessa forma, as redes sociais, os *blogs* e os fóruns começam a ocupar um papel de extrema importância na participação política dos cidadãos, sendo palco do início de grandes revoltas sociais como a Primavera Árabe.[3] Contudo, até que ponto o ser virtual é, de fato, autônomo e independente?

Para Byung-Chul Han, estamos vivenciando uma crise de liberdade, escondida pelo falso sentimento de autodeterminação:

> Hoje, acreditamos que não somos sujeitos submissos, mas projetos livres, que se esboçam e se reinventam incessantemente. A passagem do sujeito ao projeto é acompanhada pelo sentimento

1 WERTHEIN, Jorge. A sociedade da informação e seus desafios. *Ciência da Informação*, Brasília, DF, v. 29, n. 2, p. 71-77, 2000. p. 74.

2 BENKLER, Yochai. *The wealth of networks*: how social production transforms markets and freedom. New Haven: Yale University Press, 2006. p. 130.

3 CASTELLS, Manuel. *Redes de indignação e esperança*: movimentos sociais na era da internet. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

> de liberdade. E esse mesmo projeto já não se mostra tanto como uma figura de coerção, mas sim de uma forma mais eficiente de subjetivação e sujeição.[4]

Nessa perspectiva, muito se discutiu acerca do caráter de esfera pública do âmbito cibernético. A esfera pública de Habermas[5] refere-se a um espaço no qual os cidadãos podem ser livres e deliberativos, agindo como críticos da autoridade vigente e impulsionando a formação da opinião pública, com a ausência de coerção. Ao lado de análises esperançosas que compreendem o poder da internet como democrático e inclusivo, apresentam-se opiniões mais céticas, que percebem o ambiente virtual como ineficaz em cumprir todos os aspectos necessários para constituir este espaço autônomo inerente à esfera pública.[6]

O próprio Habermas,[7] em 2006, aponta o advento da internet como um elemento que modifica as condições anteriormente determinadas na esfera pública tradicional. Ao passo que a era virtual teria o poder de produzir "um efeito subversivo em regimes que dispensam um tratamento autoritário à esfera pública",[8] o filósofo vislumbrou uma inédita e prejudicial dispersão dos focos políticos.[9]

Anos mais tarde, é possível notar que além das diferenças iniciais da esfera pública tradicional para a esfera pública em rede – tais quais maior conectividade e mais rápida disseminação de informação –, o cidadão comum talvez não exerça um papel tão autônomo quanto

4 HAN, Byung-Chul. *Psicopolítica*: o neoliberalismo e as novas técnicas de poder. Belo Horizonte: Editora Âyiné, 2018. p. 9.

5 HABERMAS, Jürgen. *Consciência moral e agir comunicativo*. 2. ed. Rio de Janeiro: Tempo Brasileiro, 2003. p. 43.

6 BARROS, Charlini Torquato Gonçalves de; SAMPAIO, Rafael Cardoso. *Internet como esfera pública?* Análise de usos e repercussões reais das discussões virtuais. Salvador: Democracia e Interfaces Digitais para a Participação Pública, 2010. v. 9, p. 87.

7 HABERMAS, Jürgen. *O caos da esfera pública*. Tradução Peter Naumann. *Acessa.com*, [*s. l.*], 2006.

8 *Ibidem*.

9 *Ibidem*.

era previsto nesse novo modelo de esfera pública.[10] Dessa forma, é necessário pontuar que a promessa da esfera pública na rede como um grande potencial subversivo, porta-voz do cidadão comum, independente da coerção das forças tradicionalmente dominantes do capitalismo, pena em se cumprir. Em contrapartida, as dinâmicas virtuais se desenvolvem, hodiernamente, no seio das maiores empresas do mundo. A exemplo, entre as cinco redes sociais mais usadas no Brasil – Youtube, *Facebook*, WhatsApp, *Instagram* e *Facebook Messenger*[11] –, quatro pertencem a uma mesma corporação (*Facebook*).

No cenário atual, a maioria dos subsídios tecnológicos utilizados, diariamente, por usuários das redes são fornecidos pelas *Big Five*: os novos grandes monopólios mundiais. Assim, ilustra Parra:[12]

> São apenas cinco grandes empresas – conhecidas como as *Big Five* ou GAFAM – que se tornaram intermediárias poderosas de nossa vida digital: Apple, Google, Microsoft, *Facebook* e Amazon. Em 2017, essas empresas passaram a ocupar as cinco primeiras posições no ranking das companhias mais valiosas do mundo, deixando para trás gigantescas corporações globais, que durante décadas tinham posições de liderança como Exxon, Nestlé, Samsung, General Electric e Johnson & Johnson. Em pouco mais de dez anos, essas empresas, que quase não produzem bens físicos, se tornaram as maiores da história do capitalismo global, superando as corporações multinacionais da indústria automobilística, petrolífera e de alimentos.

10 BEÇAK, Rubens; LONGHI, João Victor Rozatti. Populismo digital e princípio democrático: o problema da censura reversa como método de comunicação. *In*: LISBOA, Roberto Senise (coord.). *O direito na sociedade da informação IV*: movimentos sociais, tecnologia e atuação do Estado. Almedina: São Paulo, 2020. p. 175.

11 KEMP, Simon. Digital 2020: Brazil. *Data Reportal*, [*s. l.*], 17 fev. 2020. p. 43.

12 PARRA, Henrique Zoqui Martins *et al*. Infraestruturas, economia e política informacional: o caso do Google Suite for Education. *Mediações*, Londrina, v. 23, n. 1, p. 63-99, 2018. p. 66.

O monopólio dessas empresas apresenta os perigos que qualquer monopólio clássico apresentaria: aumento na desigualdade social, desregulamento do mercado e a concentração de poder econômico como instrumento de consolidação do poder político.[13] Contudo, o problema singular e revolucionário do domínio dessas grandes empresas ocorre devido à hiper concentração dos dados pessoais de milhões de pessoas, em um processo paradoxal no qual os dados informacionais dos usuários são utilizados para reafirmar e ampliar o próprio monopólio.[14] Assim, quanto mais dados informacionais, mais poder; quanto mais poder, mais usuários e, por conseguinte, mais dados informacionais.

Ao analisar o *modus operandi* da Amazon, percebeu-se que a corporação utiliza os dados dos usuários do seu serviço Marketplace para potencializar seu domínio no mercado.[15] O Marketplace da Amazon é um sistema de assinatura que uma outra empresa ou indivíduo assina mensalmente para vender seus produtos por meio das plataformas *on-line* da própria Amazon.[16] Nesse sentido, uma vez que o monopólio tem acesso a todas as informações das vendas que são realizadas no seu *website*, pode rastrear e delimitar as ideias que fazem sucesso comercialmente, seus preços, seu público e outras diversas informações necessárias para criar um plano de mercado infinitamente superior ao da empresa de origem.[17] Como exemplo, Khan discorre sobre uma fábrica que vendia suporte de alumínio para *laptops* há mais de uma década no Marketplace e, em 2019, viu surgir um suporte

13 KHAN, Lina. Amazon's antitrust paradox. *The Yale Law Journal*, New Haven, v. 126, n. 710. p. 710-805, 2016. p. 740.

14 NEWMAN, Nathan. Search, antitrust, and the economics of the control of user data. *Yale Journal on Regulation*, New Haven, v. 30, n. 3, p. 1-73, 2014. p. 407.

15 KHAN, *op. cit.*, p. 781.

16 Informação fornecida pela Amazon em seu *website*: https://services.amazon.com.br/venda-na-amazon.html?ld=SEBRSOA_inst_inst-rlsa_marketplace-na-amazondesk_asret_observacao&gclid=CjwKCAiAq8f-BRBtEiwAGr3DgbqQJwBm3wIxj5xODiBzN3uEMZimUl-dwaNCmCjbO7E80Y0wSgFS-hoCFOUQAvD_BwE.

17 KHAN, *op. cit.*, p. 783.

similar sendo vendido pela metade do preço. Mais tarde, a fábrica descobriu que a marca responsável era a AmazonBasics, uma linha privada desenvolvida pela Amazon.[18]

À primeira vista, pode parecer mais simples visualizar de que forma o acúmulo de capital e de dados informacionais por parte da Amazon ou da Apple, empresas que produzem e vendem bens materiais, pode influenciar em seu maior domínio no mercado – em contrapartida com as redes sociais como o *Facebook* e *websites* como o Google, os quais fornecem serviços "gratuitos". Contudo, insta pontuar que, para que alguém possa navegar por esses *websites* há, de fato, uma permuta. Em troca dos serviços fornecidos, os usuários ofertam sua privacidade e seus dados pessoais,[19] ao assinar os longos termos de adesão que impõem condições das mais abusivas, como o direito da empresa em manter seus dados informacionais mesmo após o cancelamento do contrato.[20]

Nesse contexto, todas as informações reunidas sobre cada uma das contas inscritas naquela rede, retroalimentam seu outro serviço – e o mais rentável –, o de publicidade.[21] Os verdadeiros clientes dessas empresas não são os seus usuários, aqueles que usufruem diretamente das plataformas, que têm contas nas redes sociais ou usam suas ferramentas de busca. Seus reais clientes são os anunciantes.[22] O Google, por exemplo, tem uma receita que depende, essencialmente, dos publicitários.[23] Assim descreve Bioni:

18 *I*KHAN, *op. cit.,* p. 782.

19 NEWMAN, *op. cit.*, p. 406.

20 POULLET, Yves. Data protection legislation: what's at stake for our society and our democracy?. *Computer Law & Security Review*, Namur, v. 25, p. 211-226, 2009. p. 214.

21 BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. São Paulo: Forense, 2019. p. 17.

22 NEWMAN, *op. cit.*, p. 405.

23 *Ibidem*, p. 406.

> Uma vez logado, o usuário passa a fornecer um rico perfil de si, que é o que viabiliza o direcionamento da publicidade. Diversos outros serviços utilizam da mesma técnica, catalogando o comportamento do usuário para, a partir daí, direcionar uma publicidade condizente ao seu perfil inferido. O usuário da rede é, portanto, monitorado, acumulando-se uma série de dados (comportamentais), que são aplicados para a personalização da abordagem publicitária.[24]

Essa técnica de monitoramento é denominada *profiling*, um método estatístico usado para deduzir o comportamento de um indivíduo com base em seu perfil nas redes.[25] Por meio dessa prática, o presente cenário se estabelece e empresas como as *Big Five* se consolidam um monopólio: o *profiling* é tão valioso para os anunciantes que esse profundo conhecimento acerca da informação pessoal dos consumidores torna quase impossível que exista competição.[26]

Estabelecido o caráter monopolista que rege o mundo virtual, retornamos ao problema inicial. O indivíduo é de fato livre na internet?

Por mais que a infinidade de informação disponível na era digital fantasie uma autonomia ilimitada, os resultados de uma pesquisa no Google, por exemplo, são elencados com base no que a própria empresa acha que é melhor para o usuário.[27] Os algoritmos indicam qual conteúdo será consumido primeiro, qual será o mais adequado para cada indivíduo e, dessa forma, limitam o acesso à informação.[28] Ocorre que quanto mais notícias de determinado espectro político ou ideologia consumimos, mais conteúdo desse mesmo viés nos é indicado, por meio da técnica do *profiling*. De tal forma discorrem Beçak e Longhi:

24 BIONI, *op. cit.*, p. 17.

25 POULLET, *op. cit.*, p. 14.

26 NEWMAN, *op. cit.*, p. 407.

27 *Ibidem*, p. 410.

28 BEÇAK; LONGHI, *op. cit.*, p. 186.

> Como dimensão política do fenômeno, dessa forma, surge um ambiente informacional marcado por 'bolhas de informação' em que o cidadão se atenta cada vez mais para conteúdos que corroborem sua atual opinião e reiterem suas convicções ideológicas naquele momento, levando a um ambiente de contínua radicalização e polarização. Em última análise, tal situação enfraquece a base da democracia deliberativa: a esfera pública.[29]

Nesse sentido, as comunicações na esfera pública das redes caminham para uma interatividade mediada cada vez mais pela coerção e menos pela livre deliberação. Os algoritmos passam a exercer o papel que antes era basilar dos grupos sociais, tomando para si o cargo de formador da opinião pública, mediado pelo interesse de uma comunidade seleta de empresas bilionárias. Assim, a função da esfera pública de ferramenta de mudança dos governos estatais é viciada pelo filtro informacional dos algoritmos, uma vez que nos é limitado o acesso pleno à informação e a polarização política é potencializada.

Polarização política: o radicalismo ideológico impulsionado pelos algoritmos

Como discutido anteriormente, o grande número de informações circulando na rede de computadores não significa um maior acesso do cidadão a uma variedade de opiniões políticas. O algoritmo que rege a lógica dos famosos *websites* precisa filtrar qual conteúdo é o mais adequado para cada usuário.

Nesse sentido, Eli Pariser[30] criou o termo "bolhas dos filtros"[31] em referência ao filtro realizado pelos algoritmos para a disseminação de

29 BEÇAK; LONGHI, *op. cit.*, p. 186.

30 PARISER, Eli. *The filter bubble*: how the new personalized web is changing what we read and how we think. London: Penguin, 2011. p. 9.

31 Tradução para o termo, originalmente em inglês, "*filter bubble*".

notícias na internet. Segundo o autor, apesar da tendência histórica do ser humano em consumir conteúdos com os quais já é familiarizado e que reafirmam suas convicções prévias, o filtro ideológico dos ambientes digitais é perigoso por conta de três fatores inéditos que o diferem do acesso à informação tradicional: 1. o fato de o usuário estar sozinho na sua própria "bolha"; 2. a "invisibilidade" da bolha dos filtros; e 3. o fato de que o usuário não escolhe entrar na bolha.[32]

Façamos uma comparação com as mídias tradicionais para melhor compreensão. Ao comprar a Veja, por exemplo, uma revista tradicionalmente de direita, o leitor terá acesso a todas as notícias daquela edição, as quais são mesmas notícias que serão disponibilizadas para todos os outros compradores da revista. Durante a leitura, é possível que o consumidor encontre um ou dois artigos dos quais ele discorde, ainda que, no geral, compartilhe da mesma visão política dos editores. Já no ambiente digital, os algoritmos são organizados de forma personalizada, em uma lógica publicitária feita especificamente para agradar o usuário – e os anunciantes –, o que afasta ainda mais as pessoas de visões sociais divergentes e as realoca em grupos de opinião extremamente restritos.[33]

Não obstante, "a maioria dos espectadores de fontes de notícias liberais ou conservadoras sabe que estão indo a uma plataforma organizada para servir um determinado ponto de vista político",[34] contudo, na internet essa delimitação é invisível.[35] Assim, perde-se a noção do que é uma notícia parcial e do que são fatos verídicos. Um leitor da Veja sabe que a revista tenderia, por exemplo, a apoiar o PSDB em uma eleição, logo, uma coluna que criticasse um adversário de um

32 PARISER, *op. cit.*, p. 9-10.

33 PARISER, *op. cit.*, p. 10.

34 PRISER, *op. cit.*, p. 10. Tradução nossa, do original: "Most viewers of conservative or liberal news sources know that they're going to a station curated to serve a particular political view-point".

35 PARISER, *op. cit.*, p. 10.

candidato tucano não seria algo espantoso. Contudo, tal parcialidade não é prevista quando, em uma rede social como o *Facebook*, o usuário inesperadamente se depara com a "notícia" (falsa), compartilhada por um amigo, de que Guilherme Boulos, militante do Movimento dos Trabalhadores Sem Teto (MTST), seria dono de um jatinho.[36]

Nesse sentido, partimos também para o terceiro ponto: a inevitabilidade dos filtros ideológicos. Comprar a Veja ou a revista Piauí é uma escolha feita conscientemente pelo consumidor; já as informações que aparecem quando o usuário abre sua página inicial do *Instagram* ou pesquisa uma palavra-chave no Google – cujos resultado são diferentes a depender do perfil do usuário ou até do bairro onde a pessoa está[37] – não foram conscientemente escolhidas pelo consumidor para aparecerem de forma parcial ou politicamente delimitada.[38]

Nesse contexto, os usuários da internet acessam um conteúdo informativo cada vez mais radical e tendencioso – sugerido de forma individual e personalizada -, sem a consciência de que essa informação recebida é uma informação previamente filtrada e sem a autonomia para escolher se aceita esse crivo ideológico ou não. Dessa forma, a polarização política se concretiza de forma imperceptível, como na interessante análise de McLuhan sobre o mito de narciso e a sociedade tecnológica:

> O jovem Narciso tomou seu próprio reflexo na água por outra pessoa. A extensão de si mesmo pelo espelho embotou suas percepções até que ele se tornou o servomecanismo de sua própria imagem prolongada ou repetida. [...] Seja como for, a sabedoria do mito de Narciso de nenhum modo indica que ele se tenha enamorado de algo que ele tenha considerado como sua própria pessoa. É claro que seus sentimentos a respeito da imagem refletida teriam sido bem diferentes, soubesse ele que

36 MACÁRIO, Carol. #Verificamos: é falso que Guilherme Boulos seja dono de um jatinho. *Piauí*, Rio de Janeiro, 4 nov. 2020.

37 PARISER, *op. cit.*, p. 33.

38 *Ibidem*, p. 10.

> se tratava de uma extensão ou repetição de si mesmo. E não deixa de ser um sintoma bastante significativo das tendências de nossa cultura marcadamente tecnológica e narcótica o fato de havermos interpretado a história de Narciso como um caso de auto-amor e como se ele tivesse imaginado que a imagem refletida fosse a sua própria.[39]

Similarmente, o cidadão digital, que sofre uma assimetria informacional acerca do uso e funcionamento da coleta dos seus dados pessoais,[40] ao consultar a internet como meio de obtenção de notícias, é sorrateiramente alocado em bolhas ideológicas. Assim, contempla opiniões que são apenas um espelho das suas próprias, sem saber que elas passaram por um filtro personalizante das grandes corporações.

Dessa forma, consome-se informações tendenciosas como nunca, mas com uma roupagem inovadora. Como discorre Abido:

> É nesse âmbito que os algoritmos possuem uma atuação que tenderia a influenciar, direta ou indiretamente os processos democráticos. [...] Se um usuário é adepto de uma determinada posição, ideologia ou partido político, a tendência dele interagir com notícias ou publicações que se relacionam e concordam com essa ideologia é maior. Ao interagir com tais publicações, o algoritmo gera para esse usuário cada dia mais conteúdo semelhante, em um círculo vicioso. Entretanto, este não é o ponto de maior preocupação, mas sim o fato de que, o algoritmo irá ocultar deste usuário, as publicações contrárias a essa posição ou ideologia, passando-se a impressão ao utilizador de que toda a rede social (ou sua imensa maioria) apresenta uma posição de concordância com a sua visão ideológica.[41]

39 MCLUHAN, Marshall. *Os meios de comunicação como extensão do homem*. São Paulo: Cultrix, 1971, p. 59.

40 BIONI, *op. cit.*, p. 144.

41 ABIDO, Leonardo. Algoritmos e democracia: reflexões sobre a influência da inteligência artificial nos processos democráticos contemporâneos. *In*: MAPELLI, Aline; GIONGO,

Ocorre que, se no ambiente digital o usuário passa a ser exposto somente a outras extensões de si – pessoas com as mesmas opiniões políticas –, ao consumir a mídia tradicional e encontrar pontos de vista um pouco divergentes dos seus, essa pessoa tende a descredibilizar a fonte conflitante.[42] Nesse diapasão, as bolhas de informação da internet se reafirmam como verdadeiras fontes de notícias, ao passo que as mídias tradicionais passam a ser vistas com descrédito.[43] Nessa lógica, há a promoção de um processo de polarização política e o estabelecimento de um paradoxo que empodera os monopólios, pois quanto mais conteúdo é consumido nas bolhas digitais, mais conteúdo se quer consumir nas bolhas digitais.

Como consequência, as diferenças entre opinião e fato ficam nebulosas, dando espaço para que teorias da conspiração cada vez mais absurdas se disseminem no mundo virtual, tal qual o crescente movimento de defensores do formato plano da terra. Segundo um estudo da *Texas Tech University*, a fonte de informação da maioria dos terra-planistas entrevistados na Conferência Internacional da Terra Plana, em 2017, era o Youtube[44] e o maior motivo para afirmar que a terra era plana não se baseava em argumentos propriamente ditos, mas na crença de que o Youtube revelava aquilo que as instituições tradicionais, como imprensa, governo e NASA, tentavam esconder.[45]

Marina; CARNEVALE, Rita (org.). *Os impactos das novas tecnologias no Direito e na Sociedade*. Erechim: Deviant, 2018. p. 164.

42 WARDLE, Claire; DERAKHSHAN, Hossein. Thinking About 'Information Disorder': Formats of Misinformation, Disinformation, and Mal-Information. *In*: IRETON, Cherilyn; POSETTI, Julie. *Journalism, 'Fake News' and Disinformation*. Paris: UNESCO, 2018. p. 43-54. (Handbook for Journalism Education and Training: UNESCO Series on Journalism Education). p. 43.

43 WARDLE; DERAKHSHAN, *op. cit.*, p. 43.

44 OLSHANSKY, Alex. *Conspiracy theorizing and religious motivated reasoning*: why the earth 'must' be flat. 2018. Thesis (Masters in Arts) – Texas Tech University, Lubbock, 2018. p. 32-35.

45 *Ibidem*.

Liberdade de informação frente aos algoritmos

A liberdade de informação é uma das liberdades públicas salvaguardadas pela Constituição Federal de 1988[46] e abarca duas grandes vertentes: o direito de informar e o direito de ser informado.[47] Enquanto a liberdade de imprensa surge como um direito subjetivo do indivíduo de manifestar seu pensamento, nascendo como uma liberdade individual, o desdobramento do direito à informação trata-se de um direito de toda a coletividade à informação.[48] Assim, a garantia do acesso à informação é estabelecida no artigo 5º, XIV:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> XIV – *é assegurado a todos o acesso à informação* e resguardado o sigilo da fonte, quando necessário ao exercício profissional.[49]

Quanto à sua reserva legal, insta pontuar que este direito fundamental é expressamente limitado pela proteção ao sigilo da fonte no mesmo artigo 5º, XIV da Carta Magna. Ademais, o acesso a informações não engloba aquelas consideradas imprescindíveis à segurança do Estado e da sociedade.[50] Não obstante, a Constituição Federal, em seu

46 BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: Presidência da República, 1988.

47 SILVA, José Afonso da. *Comentário Contextual à Constituição*. 3. ed. Brasil: Malheiros, 2007. p. 109, citando Chiola, *L'Informazione nella Costituzione*, p. 28.

48 SILVA, *op. cit.*, p. 109.

49 BRASIL. Constituição (1988), *op. cit.*

50 CUNHA JÚNIOR, Dirley da. *Curso de direito constitucional*. 13. ed. Salvador: Juspodivm, 2019. p. 610.

artigo 5º, X, também estabelece a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas.[51] Nesse sentido, a liberdade de informação pode ser restringida frente aos direitos da personalidade.

Contudo, mesmo a proteção dos direitos personalíssimos é capaz de ser limitada em uma situação de colisão de princípios caso a informação em questão seja de interesse público, "se a liberdade de informação for de relevante interesse social, o direito à vida privada deve ser afastado em detrimento do interesse público-social dessa mesma liberdade de informação plenamente definida e delimitada".[52] Ao compreender a valoração da informação de interesse público – como conceito que infere a existência de notícias cuja divulgação à população é imperiosa –, resta claro o papel do acesso à informação como ferramenta indispensável para o exercício da cidadania e a reafirmação da democracia.

A sua importância reside no fato de que o direito de obter informações é uma forma de reafirmar a democracia participativa, visando fornecer "os subsídios para a formação de convicções relativas a assuntos públicos".[53] Dessa forma, a liberdade de informação permite a criação de uma opinião esclarecida, ensejando a transparência, não só dos negócios públicos, mas também nas decisões sociais que influenciam nos direitos essenciais da pessoa humana.[54]

O aspecto coletivo do direito ao acesso à informação, assegurado a todos, está intrinsecamente ligado à importância política da

51 BRASIL. Constituição (1988), *op. cit*. "Art. 5° Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
[...]
X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

52 LEYSER, Maria Fátima Vaquero Ramalho. *Direito à liberdade de imprensa*. São Paulo: Juarez de Oliveira, 1999. p. 68.

53 MORAES, Alexandre de. *Direitos humanos fundamentais*. São Paulo: Atlas, 2016. p. 161.

54 MIRANDA, Rosângelo Rodrigues. *A proteção constitucional da vida privada*. São Paulo: LED, 1996. p. 145-146.

informação como exercício de cidadania, referindo-se ao direito do povo de ser bem informado.[55] Nesse sentido, o acesso à informação objetiva evitar a manipulação da opinião pública por parte de grupos hegemônicos – públicos ou privados –, assim,

> a liberdade de expressão e informação contribui para a formação da opinião pública pluralista – esta cada vez mais essencial para o funcionamento dos regimes democráticos, a despeito dos anátemas eventualmente dirigidos contra a manipulação da opinião pública.[56]

Nesse diapasão, o artigo 220 proíbe os monopólios, diretos ou indiretos, dos meios de comunicação:

> Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo, não sofrerão qualquer restrição, observado o disposto nesta Constituição.
> [...]
> § 5º Os meios de comunicação social não podem, direta ou indiretamente, ser objeto de monopólio ou oligopólio.[57]

Tal dispositivo objetiva proteger, dentre outros direitos – tais quais a liberdade de pensamento e expressão –, a garantia do exercício da liberdade de informação sem restrições.[58] Tendo em vista o poder de influência dos meios de comunicação na opinião pública, a concentração desse poder em poucas mãos poderia gerar um quadro

55 NOBRE, José Freitas. *Imprensa e liberdade*: os princípios constitucionais e a nova legislação. São Paulo: Saraiva, 1988. p. 33-34.

56 FARIAS, Edilsom Pereira de. *Colisão de direitos*: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. 2. ed. atual. Porto Alegre: Sérgio Antônio Fabris, 2000. p. 166-167.

57 BRASIL. Constituição (1988), *op. cit.*

58 SILVA, *op. cit.*, p. 827.

de manipulação e coação, intervindo na lógica democrática de forma pouco saudável.[59]

Nesse contexto, de acordo com o *Digital News Report 2020*, realizado pela Universidade de Oxford e pelo *Reuters Institute for the Study of Journalism*, pela primeira vez desde o início da pesquisa (o *Digital News Report* é feito anualmente) as redes sociais ultrapassaram a televisão como meio de obtenção de notícias.[60] Assim, depreende-se que o acesso à informação do cidadão brasileiro deslocou-se das mídias tradicionais para a internet e, com isso, o direito à informação passa a ser diretamente afetado.

O conceito de acesso à informação como exercício de cidadania torna-se nebuloso, uma vez que a internet – um ambiente onde reinam os monopólios – é regida por algoritmos baseados no perfil do usuário, visando atender não ao interesse público, mas ao dos anunciantes – e o interesse que ele crê ser dos próprios usuários. Dessa forma, a informação passa a ser hierarquizada não com base em um critério de emergência social, qualidade de pesquisa ou veracidade, mas no que, supostamente, vai agradar o usuário que utiliza as plataformas digitais. Nesse cenário, um pesquisa do *Institute for Strategic Dialogue* apontou que o algoritmo do *Facebook* promovia conteúdos negacionistas quanto à existência do holocausto para os usuários que já seguiam outras páginas de conteúdo similar – que alegavam ter sido uma grande mentira o genocídio do povo judeu.[61]

Assim, o usuário que segue um padrão de acesso a um determinado conteúdo, receberá mais conteúdo vinculado a esse espectro,

59 SARAVIA, Enrique. O novo papel regulatório do Estado e suas consequências na mídia. *In*: SARAVIA, Enrique; MARTINS, Paulo Emílio Matos; PIERANTI, Octavio Penna (org.). *Democracia e regulação dos meios de comunicação em massa*. Rio de Janeiro: Ed. FGV, 2008. p. 64.

60 REUTERS INSTITUTE FOR THE STUDY OF JOURNALISM. *Digital News Report 2020*. [*S. l: s. n.*], 2020.

61 INSTITUTE FOR STRATEGIC DIALOGUE. Hosting the 'holohoax': a snapshot of holocaust denial on social media Institute for Strategic. Dialogue London, 10 ago. 2020.

"assim, eventuais '*fake news*' que explorem esse padrão para a sua disseminação terão maior êxito, já que ele não terá acesso a outras informações que poderiam contradizer ou até esclarecer os fatos".[62] Nesse sentido, discorre Lima:

> A migração do centro das discussões políticas para Internet conduz à reflexão sobre as consequências da mediação corporativa das relações políticas, num ambiente que segue modelos de negócios da publicidade. Aliás, observa-se que o mecanismo de segmentação de informações, inerente ao funcionamento das redes sociais, como *Facebook*, *Instagram* e *Twitter*, é um dos pilares da desordem informacional.[63]

No ambiente digital o potencial viral do conteúdo é privilegiado em detrimento da sua qualidade:[64] quanto mais acessado, mais indicado para outros usuários. Tal lógica abre espaço para o estabelecimento cada vez maior das *fake news* ou *junk news*, uma vez que suas chamadas sensacionalistas são muito mais apelativas do que uma notícia regular. Nesse sentido, analisando a eleição americana de 2016, *fake news* a favor de Trump e contra Hillary Clinton eram compartilhadas até três vezes mais do que as notícias verdadeiras.[65] Na eleição brasileira de 2018 não foi diferente, diversas *fake news* foram divulgadas em massa contra o candidato do Partido dos Trabalhadores (PT),

62 SASTRE, Angelo; CORREIO, Claudia Silene de Oliveira; CORREIO, Francisco Rolfsen Belda. A influência do "filtro bolha" na difusão de fake news nas mídias sociais: reflexão sobre as mudanças nos algoritmos no Facebook. *Revista GEMInIS*, São Carlos, v. 9, n. 1, p. 4-17, 2018. p. 8.

63 LIMA, Cíntia Rosa Pereira de; SOUSA, Maria Eduarda Sampaio de. LGPD e combate às fake news. *Migalhas*, [Rio de Janeiro], 4 set. 2020.

64 MARTÍN, María. Com o novo algoritmo do Facebook, as 'fake news' ganham. *El País*, Rio de Janeiro, 11 fev. 2018.

65 SCHRADIE, Jen. *The revolution that wasn't*: how digital activism favors conservatives. Cambridge: Harvard University Press, 2019.

Fernando Haddad, que foi acusado de tentar sexualizar crianças nas escolas públicas com a distribuição de um suposto "kit gay".[66]

Destarte, a lógica empresarial que rege os monopólios da internet, que tem sido o meio de comunicação social mais usado pelos brasileiros para obtenção de notícias, não coaduna com os objetivos democráticos e de construção popular da opinião pública do direito ao acesso à informação. Nesse sentido, o interesse público e a importância social da liberdade de informação são desconsiderados, impulsionando a disseminação de notícias falsas em um processo de verdadeira desinformação do cidadão. Todo o cenário que se desenvolve por meio de filtros e bolhas de informação, programados por multinacionais bilionárias, evidencia que há tudo, menos autonomia e liberdade, no universo digital.

Direito e os mecanismos de controle

Em face de um cenário que desconsidera a liberdade de informação e o direito da coletividade ao acesso à informação, é necessário que o Estado intervenha para regular as condutas abusivas dos monopólios nas redes e proteger os espaços de exercício democráticos, sejam eles esferas públicas tradicionais ou não. Nesse sentido, o Brasil avançou muito rumo a uma legislação que atua tanto no que se refere ao uso dos dados pelas empresas digitais, quanto em um combate à desinformação popular no mundo virtual.

O Marco Civil da Internet, Lei nº 12.965 de 2014[67], estabelece como fundamentos do uso da internet no Brasil, dentre outros, o respeito à liberdade de expressão, exercício da cidadania em meios digitais, a

66 BARRAGÁN, Almudena. Cinco 'fake news' que beneficiaram a candidatura de Bolsonaro. *El País*, Rio de Janeiro, 16 out. 2018.

67 BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União:* seção 1, Brasília, DF, ano 151, n. 77, p. 1-3, 24 abr. 2014.

pluralidade e a diversidade, os direitos humanos, a livre iniciativa, a livre concorrência e a defesa do consumidor, assim como a finalidade social da rede.[68] Dessa maneira, são determinados os princípios que devem reger o funcionamento da internet, objetivando proteger o usuário da rede de computadores e regulamentar o uso digital à luz dos preceitos constitucionais.

Não obstante, o manejo dos dados pessoais dos usuários, ferramenta essencial para as técnicas de *profiling* e elaboração das bolhas de filtro, passou a ser regulamentado pela Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709 de 2018. A LGPD também criou a Autoridade Nacional de Proteção de Dados (ANPD), que, segundo a notícia veiculada no *website* do Senado Federal, "tem a atribuição de zelar pela proteção dos dados pessoais, assegurar a observância de segredos comerciais e industriais e punir eventuais descumprimentos à legislação".[69]

Ademais, além da regulamentação do uso de dados pessoais por parte das empresas, um grande passo foi dado com a aprovação do Projeto de Lei nº 2.630/2020 no Senado Federal. Apelidada de Lei das *Fake News*, o PL impõe aos provedores de redes sociais e de serviços de mensageria privada diversos deveres, tais quais o uso de verificadores de fatos independentes, a rotulação e a limitação do compartilhamento de conteúdo desinformativo, a interrupção de promoção artificial do conteúdo e o envio de informação verificada aos usuários alcançados

68 BRASIL. Lei nº 12.965, *op. cit.* "Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
I – o reconhecimento da escala mundial da rede;
II – os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
III – a pluralidade e a diversidade;
IV – a abertura e a colaboração;
V – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VI – a finalidade social da rede".

69 SENADO confirma primeira diretoria da Autoridade Nacional de Proteção de Dados. *Senado Notícias*, Brasília, DF, 20 out. 2020.

pelo conteúdo.[70] Como sanção em caso de descumprimento, as empresas podem ser submetidas a multa de até 10% do seu faturamento no Brasil no seu último exercício, de acordo com o artigo 31.

Tal Projeto de Lei foi muito criticado pelo presidente Jair Bolsonaro.[71] Similarmente, em seu voto, o senador Fernando Bezerra Coelho, do Movimento Democrático Brasileiro (MDB), afirmou que a liberdade de expressão estaria sendo limitada.[72] Todavia, evitar a disseminação de desinformação nas redes não é uma violação à livre manifestação, mas sim uma proteção à democracia na medida em que engloba o direito coletivo do acesso à informação, respeitando a função social do ambiente digital, celebrada no Marco Civil da Internet.

Não obstante – apesar de regulamentar questões importantíssimas, promover a liberdade de informação sob a ótica democrática e responsabilizar as grandes empresas por possíveis violações –, as sanções do projeto de lei brasileiro são bem limitadas se comparado a outras legislações internacionais. Na Alemanha, por exemplo, a sua lei regulatória, *Netzwerkdurchsetzungsgesetz*, prevê uma multa que pode chegar a 50 milhões de euros para empresas digitais que não deletam conteúdos ilegais (como discurso de ódio e *fake news*) em até 24 horas.[73]

Por fim, o combate ao monopólio propriamente dito também precisa ser realizado. Nesse sentido, em dezembro de 2020, a Comissão Federal do Comércio dos Estados Unidos e de 40 estados acusaram o *Facebook* de violar as leis antitruste.[74] Assim se pronunciou a procuradora geral de Nova York, Letitia James:

70 BRASIL. *Projeto de Lei nº 2630, de 2020*. Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Senado Federal: Brasília, DF, 2020.

71 SENADO aprova projeto de lei das fake news. *BBC Brasil*, São Paulo., 30 jun. 2020.

72 SENADO..., 2020.

73 ALEMANHA. *Network Enforcement Act Regulatory Fining Guidelines*: Guidelines on setting regulatory fines within the scope of the Network Enforcement Act (Netzwerkdurchsetzungsgesetz – NetzDG) *[S. l.: s. n.]*, 2018.

74 KANG, Cecilia; ISAAC, Mike. U.S. and States Say Facebook Illegally Crushed Competition. *The New York Times*, New York, 9 dez. 2020a.

> O Facebook tem passado seu tempo vigiando as informações pessoais dos seus usuários, lucrando com isso. Nenhuma empresa deveria ter todo esse poder descontrolado sobre as nossas informações pessoais e nossas interações sociais e é por isso que estamos agindo hoje e defendendo os milhões de consumidores e diversas pequenas empresas que foram prejudicadas pelo comportamento ilegal do Facebook.[75]

Similarmente, também em dezembro de 2020, 38 procuradores gerais estadunidenses ingressaram com uma ação judicial contra o Google, alegando que a empresa está mantendo um monopólio ilegal no mercado de buscas *on-line*.[76] A plataforma já havia sido acusada de violar as leis antitruste pelo Departamento de Justiça e por mais 11 estados.[77] Todavia, o novo processo vai além, alegando que o comando do Google sobre uma vasta quantidade de dados – obtidos devido à falta de opção dos consumidores – fortificou o monopólio da empresa e criou novas barreiras para a competição.[78]

Dessa maneira, diante dos abusos das empresas privadas no ambiente digital, em um desrespeito aos preceitos constitucionais, aos direitos da personalidade do usuário e ao pleno exercício democrático, é imprescindível que haja uma interferência estatal a fim de regulamentar o uso das redes. Nesse contexto, o Brasil tem estabelecido normas legais que visam proteger o cidadão no âmbito

75 KANG, Cecilia; ISAAC, Mike. U.S. and States Say Facebook Illegally Crushed Competition. *The New York Times*, New York, 9 dez. 2020a. Tradução nossa do original: "Facebook has been spending its time surveilling user's personal information, profiting from it. No company should have this much unchecked power over our personal information and our social interactions and that's why we are taking action today and standing up for the millions of consumers and many small businesses that have been harmed by Facebook's illegal behaviour".

76 FUNG, Brian. The antitrust lawsuits against Google just keep coming. *CNN*, [Atlanta]., 17 dez. 2020.

77 KANG, Cecilia; MCCABE, David; WAKABAYASHI, Daisuke. U.S. Accuses Google of Illegally Protecting Monopoly. *The New York Times*, New York, 20 out. 2020b.

78 FUNG, *op. cit.*

virtual. Contudo, faz-se necessário também um maior controle dos mecanismos de manutenção do poder, tendo em vista, inclusive, que o estabelecimento de monopólios nos meios de comunicação social é inconstitucional.

Conclusões

Diante de todo o exposto, resta claro que a aplicação da lógica mercadológica nos meios de comunicação e disseminação de informação traz efeitos nocivos para a democracia, ao passo que vicia a construção da opinião pública e obsta o processo orgânico e deliberativo do exercício da cidadania. Nesse sentido, considerando a internet como uma grande agência de publicidade, todas as benesses que vêm atreladas ao seu uso não são gratuitas, pois, em troca, fornecemos nossa autonomia.

Em seus algoritmos mercadológicos não há uma análise que sopese as consequências sociais; o objetivo é tornar o usuário cada vez mais ativo, satisfeito e vigiado. Assim, o mais alarmante neste processo de sujeição e submissão, reside em sua natureza cíclica: o sistema se retroalimenta.

Um *website* relevante recebe muitos usuários e, portanto, tem acesso a um número coincidente de dados pessoais. Quanto mais dados, é possível aplicar melhores técnicas de *profiling*, agradando os anunciantes e tornando-se ainda mais relevante. Práticas de *profiling* eficientes também desenvolvem filtros ideológicos mais eficientes, os quais promovem a alienação do usuário em uma redoma individualmente personalizada de opiniões políticas idênticas às dele.

Por sua vez, o usuário busca cada vez mais se informar pelo único meio de comunicação com o qual nunca vai discordar, duvidando inclusive da credibilidade de notícias oriundas de qualquer outra fonte. Dessa maneira, os monopólios digitais fidelizam seus clientes, recebendo cada vez mais usuários, acessando e utilizando seus dados para manipular a divulgação de conteúdos informativos e, portanto,

se estabelecendo como empresas cada vez mais relevantes e absurdamente poderosas.

Destarte, é imperioso proteger a liberdade de informação sem restrições, tendo em vista o direito à informação como um direito coletivo e essencial, não somente para a formação autônoma de uma opinião individual, mas para o livre exercício democrático, na construção de esferas públicas comunitárias, pluralistas e heterogêneas. Portanto, torna-se imprescindível a regulamentação estatal para evitar os abusos por parte de entes privados.

Referências

ABIDO, Leonardo. Algoritmos e democracia: reflexões sobre a influência da inteligência artificial nos processos democráticos contemporâneos. *In*: MAPELLI, Aline; GIONGO, Marina; CARNEVALE, Rita (org.). *Os impactos das novas tecnologias no Direito e na Sociedade*. Erechim: Deviant, 2018. p. 153-166.

ALEMANHA. *Network Enforcement Act Regulatory Fining Guidelines*: Guidelines on setting regulatory fines within the scope of the Network Enforcement Act (Netzwerkdurchsetzungsgesetz – NetzDG) *[S. l.: s. n.]*, 2018. Disponível em: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/NetzDG_Bu%C3%9Fgeldleitlinien_engl.pdf?___blob=publicationFile&v=2. Acesso em: 30 nov. 2020.

BARRAGÁN, Almudena. Cinco 'fake news' que beneficiaram a candidatura de Bolsonaro. *El País*, Rio de Janeiro, 16 out. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/10/18/actualidad/1539847547_146583.html. Acesso em: 22 out. 2020.

BARROS, Charlini Torquato Gonçalves de; SAMPAIO, Rafael Cardoso. *Internet como esfera pública?*. Análise de usos e repercussões reais das discussões virtuais. Salvador: Democracia e Interfaces Digitais para a Participação Pública, 2010. v. 9.

BEÇAK, Rubens; LONGHI, João Victor Rozatti. Populismo digital e princípio democrático: o problema da censura reversa como método de comunicação. *In*: LISBOA, Roberto Senise (coord.). *O direito na sociedade da informação IV*: movimentos sociais, tecnologia e atuação do Estado. São Paulo: Almedina, 2020. p. 170-191.

BENKLER, Yochai. *The wealth of networks*: how social production transforms markets and freedom. New Haven: Yale University Press, 2006.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. São Paulo: Forense, 2019.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: Presidência da República, 1988.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União:* seção 1, Brasília, DF, ano 151, n. 77, p. 1-3, 24 abr. 2014.

BRASIL. *Projeto de Lei nº 2630, de 2020*. Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Senado Federal: Brasília, DF, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01fn8erw6shem0wq90r038xu9q887735.node0?codteor=1909983&filename=PL+2630/2020. Acesso em: 30 nov. 2020.

CASTELLS, Manuel. *Redes de indignação e esperança*: movimentos sociais na era da internet. Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

CUNHA JÚNIOR, Dirley da. *Curso de direito constitucional*. 13. ed. Salvador: Juspodivm, 2019.

FARIAS, Edilsom Pereira de. *Colisão de direitos*: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. 2. ed. atual. Porto Alegre: Sérgio Antônio Fabris, 2000.

FUNG, Brian. The antitrust lawsuits against Google just keep coming. *CNN*, [Atlanta], 17 dez. 2020. Disponível em: https://edition.cnn.com/2020/12/17/tech/google-antitrust-lawsuit/index.html. Acesso em: 20 dez. 2020.

HABERMAS, Jürgen. *Consciência moral e agir comunicativo*. 2. ed. Rio de Janeiro: Tempo Brasileiro, 2003.

HABERMAS, Jürgen. *O caos da esfera pública*. Tradução: Peter Naumann. *Acessa.com*, [*s. l.*], 2006. Disponível em: https://www.acessa.com/gramsci/?page=visualizar&id=561. Acesso em: 7 nov. 2020.

HAN, Byung-Chul. *Psicopolítica*: o neoliberalismo e as novas técnicas de poder. Belo Horizonte: Âyiné, 2018.

INSTITUTE FOR STRATEGIC DIALOGUE. Hosting the 'holohoax': a snapshot of holocaust denial on social media *Institute for Strategic Dialogue*, London, 10 ago. 2020. Disponível em: https://www.isdglobal.org/wp-content/uploads/2020/08/Hosting-the-Holohoax.pdf. Acesso em: 28 nov. 2020.

KANG, Cecilia; ISAAC, Mike. U.S. and States Say Facebook Illegally Crushed Competition. *The New York Times*, New York, 9 dez. 2020a. Disponível em: https://www.nytimes.com/2020/12/09/technology/facebook-antitrust-monopoly.html. Acesso em: 10 dez. 2020.

KANG, Cecilia; MCCABE, David; WAKABAYASHI, Daisuke. U.S. Accuses Google of Illegally Protecting Monopoly. *The New York Times*, New York, 20 out. 2020b. Disponível em: https://www.nytimes.com/2020/10/20/technology/google-antitrust.html. Acesso em: 20 dez. 2020.

KEMP, Simon. Digital 2020: Brazil. *Data Reportal*, [*s. l.*], 17 fev. 2020. Disponível em: https://datareportal.com/reports/digital-2020-brazil. Acesso em: 7 nov. 2020.

KHAN, Lina. Amazon's antitrust paradox. *The Yale Law Journal*, New Haven, v. 126, n. 710, p. 710-805, 2016.

LEYSER, Maria Fátima Vaquero Ramalho. *Direito à liberdade de imprensa*. São Paulo: Juarez de Oliveira, 1999.

LIMA, Cíntia Rosa Pereira de; SOUSA, Maria Eduarda Sampaio de. LGPD e combate às fake news. *Migalhas*, [*s. l.*], 4 set. 2020. Disponível em: https://migalhas.uol.com.br/coluna/migalhas-de-protecao-de-dados/332907/lgpd-e-combate-as-fake-news. Acesso em: 17 nov. 2020.

MACÁRIO, Carol. #Verificamos: é falso que Guilherme Boulos seja dono de um jatinho. *Piauí*, Rio de Janeiro, 4 nov. 2020. Disponível em: https://piaui.folha.uol.com.br/lupa/2020/11/04/verificamos-guilherme-boulos-jatinho/. Acesso em: 22 nov. 2020.

MARTÍN, María. Com o novo algoritmo do Facebook, as 'fake news' ganham. *El País*, Rio de Janeiro, 11 fev. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/02/11/politica/1518373215_479582.html. Acesso em: 22 nov. 2020.

MCLUHAN, Marshall. *Os meios de comunicação como extensão do homem*. São Paulo: Cultrix, 1971.

MIRANDA, Rosângelo Rodrigues. *A proteção constitucional da vida privada*. São Paulo: LED, 1996.

MORAES, Alexandre de. *Direitos humanos fundamentais*. São Paulo: Atlas, 2016.

NEWMAN, Nathan. Search, antitrust, and the economics of the control of user data. *Yale Journal on Regulatio*n, New Haven, v. 30, n. 3, p. 1-73, 2014.

NOBRE, José Freitas. *Imprensa e liberdade*: os princípios constitucionais e a nova legislação. São Paulo: Saraiva, 1988.

OLSHANSKY, Alex. *Conspiracy theorizing and religious motivated reasoning*: why the earth 'must' be flat. 2018. Thesis (Masters in Arts) – Texas Tech University, Lubbock, 2018. Disponível em: https://ttu-ir.tdl.org/bitstream/handle/2346/82666/OLSHANSKY-THESIS-2018.pdf?sequence=1&isAllowed=y. Acesso em: 15 nov. 2020.

PARISER, Eli. *The filter bubble*: how the new personalized web is changing what we read and how we think. London: Penguin, 2011.

PARRA, Henrique Zoqui Martins *et al.* Infraestruturas, economia e política informacional: o caso do Google Suite for Education. *Mediações*, Londrina, v. 23, n. 1, p. 63-99, 2018.

POULLET, Yves. Data protection legislation: what's at stake for our society and our democracy?. *Computer Law & Security Review*, Namur, v. 25, p. 211-226, 2009.

REUTERS INSTITUTE FOR THE STUDY OF JOURNALISM. *Digital News Report 2020*. [*S. l.: s. n.*], 2020. Disponível em: https://www.digitalnewsreport.org/survey/2020/brazil-2020/. Acesso em: 17 nov. 2020.

SARAVIA, Enrique. O novo papel regulatório do Estado e suas consequências na mídia. *In*: SARAVIA, Enrique; MARTINS, Paulo Emílio Matos; PIERANTI, Octavio Penna (org.). *Democracia e regulação dos meios de comunicação em massa*. Rio de Janeiro: Ed. FGV, 2008. p. 59-70.

SASTRE, Angelo; CORREIO, Claudia Silene de Oliveira; CORREIO, Francisco Rolfsen Belda. A influência do "filtro bolha" na difusão de fake news nas mídias sociais: reflexão sobre as mudanças nos algoritmos no Facebook. *Revista GEMInIS*, São Carlos, v. 9, n. 1, p. 4-17, 2018.

SCHRADIE, Jen. *The revolution that wasn't*: how digital activism favors conservatives. Cambridge: Harvard University Press, 2019.

SENADO aprova projeto de lei das fake news. *BBC Brasil*, São Paulo, 30 jun. 2020. Disponível em: https://www.bbc.com/portuguese/brasil-53244947. Acesso em: 30 nov. 2020.

SENADO confirma primeira diretoria da Autoridade Nacional de Proteção de Dados. *Senado Notícias*, Brasília, DF, 20 out. 2020. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/10/20/senado-confirma-primeira-diretoria-da-autoridade-nacional-de-protecao-de-dados. Acesso em: 30 nov. 2020.

SILVA, José Afonso da. *Comentário Contextual à Constituição*. 3. ed. São Paulo: Malheiros, 2007.

WARDLE, Claire; DERAKHSHAN, Hossein. Thinking About 'Information Disorder': Formats of Misinformation, Disinformation, and Mal-Information. *In*: IRETON, Cherilyn; POSETTI, Julie. *Journalism, 'Fake News' and Disinformatio*n. Paris: UNESCO, 2018. p. 43-54. (Handbook for Journalism Education and Training: UNESCO Series on Journalism Education).

WERTHEIN, Jorge. A sociedade da informação e seus desafios. *Ciência da Informação*, Brasília, DF, v. 29, n. 2, p. 71-77, 2000.

TIK TOK – DÁ-ME TEUS DADOS E TE DIREI QUEM ÉS: A SOCIALDIGITALIDADE E A POSSÍVEL FLEXIBILIZAÇÃO DE CONCEITOS FUNDAMENTAIS

Laura Lucia da Silva Amorim

Introdução

Nesta era digital, uma grande quantidade de pessoas diverte-se com aplicativos que lhes prometem dizer quem eram em um passado longínquo, como serão seus futuros, o que seus signos revelam, entre outras curiosidades. O ditado popular "a curiosidade matou um gato" é um alerta para situações que podem ser desastrosas, porque nesse ditado, toma-se a morte do gato como azar. Mas o que isso tem a ver com esse trabalho? Depende muito do observador. A ideia aqui é conversar sobre assuntos seríssimos com leveza, mas também aguçando a curiosidade. É pela curiosidade humana que o mundo evoluiu não só em aspectos materiais, mas também em aspectos morais.

Aqui nos interessa o crescimento tecnológico, logo, a evolução material, no contexto econômico, social e jurídico, porque para compreensão da era digital é imprescindível a leitura multidisciplinar de conceitos como: dados pessoais, tratamento de dados, sociedade digital e de consentimento.

E existe correlação entre o ditado popular e tais contextos? Veremos.

Desde a época de Adam Smith,[1] criador do liberalismo econômico e que fomentou, com suas ideias, o crescimento tecnológico, até o Adam robô digital que utiliza inteligência artificial de *machine learning* – por exemplo, detectando possíveis doenças a partir do que aprende com fotografias de olhos –, o foco continua sendo o mesmo: o uso dos dados visando o lucro.

No contexto social, o ditado popular é um alerta também no âmbito das atitudes da "socialdigitalidade", porque desde os tempos de espreitar pelas janelas para saber das novidades alheias até hoje, quando substituímos a janela pela olhadinha no *Facebook*, *Instagram* e *Twitter* para ver as últimas publicações e socializar, o resultado não mudou. Onde mora o perigo de a curiosidade do gato dar azar? Na espiada, a mexeriqueira captava dados que não guardava para si, mas contava a todos; agora quem os guarda é a *Cloud* de plataformas do "*Big Other*", que não só conta os dados de sua vida toda, mas os monetiza.

Você deve estar pensando que o ditado popular não cabe no contexto jurídico, pois cabe! A sua curiosidade e vontade de interagir na internet matam o gato mais precioso de sua vida, a privacidade, quando você simplesmente consente quando é incitado a dar liberação incentivada de seus dados sensíveis, acreditando estar no uso e gozo de sua autodeterminação.

Fabiano Peixoto diz que "as tecnologias de Inteligência Artificial estão amplamente distribuídas no cotidiano da vida moderna, sendo usualmente utilizadas em aplicações que incluem reconhecimento de

1 SMITH, Adam. *A riqueza das nações*: investigação sobre sua natureza e suas causas. Tradução João Luiz Baraúna. São Paulo: Nova Cultural, 1996. p. 9. A importância da grande obra econômica de Adam Smith é usualmente definida pelos efeitos de sua influência como, alternativamente, o marco do início do enfoque científico dos fenômenos econômicos ou a Bíblia da irresistível vaga livre-cambista do século XIX. "[...] a riqueza ou o bem-estar das nações é identificado com seu produto anual per capita que, dada sua constelação de recursos naturais, é determinado pela produtividade do trabalho "útil" ou "produtivo" — que pode ser entendido como aquele que produz um excedente de valor sobre seu custo de reprodução — e pela relação entre o número de trabalhadores empregados produtivamente e a população total".

voz nos telefones e tradução de idiomas por máquinas online" entre tantos outras, mas destaca que "ela combina as propriedades das tecnologias digitais em geral com as propriedades que se pensava serem unicamente humanas, como a competência"[2]. Essa criação tecnológica só foi possível porque existe a captação de dados humanos na internet.

A Lei Geral de Proteção de Dados (LGPD), que vige desde 18 de setembro de 2020[3], não esclarece como deve ser o consentimento ao tratamento dos dados. E muito embora tenha como objetivo o respeito à privacidade e a autodeterminação informativa, percebe-se que existe um elo perdido nessa intenção legal, por isso, entende-se ser necessário uma análise visando esclarecer essa falta de clareza do que é e como deve ocorrer o consentimento ao uso de dados pessoais, bem como uma compreensão da lógica do uso da internet na era digital e de possíveis consequências desastrosas.

Este trabalho é parte integrante de uma tese doutoral que pretende ponderar "os dados pessoais e jurídicos, sob uma nova percepção de conceitos fundamentais, podem ser um possível instrumento a formatação de solução de conflitos por meio de inteligências artificiais". Nesse sentido, este trabalho ainda é um ensaio, um estudo prévio com a pretensão de ganho de conhecimento para a pesquisa doutoral.

Na construção deste capítulo, o método de interpretação jurídica é o teleológico,[4] ponto de referência a aplicação diária do direito e que se utilizará dos instrumentos metodológicos: legislativo, livros, artigos, filmes, vídeos, documentos, entre outros. Guiamo-nos pela problemática: a liberação incentivada é uma espécie de consentimento?

2 HARTMANN PEIXOTO, Fabiano. *Inteligência artificial e direito*. Curitiba: Alteridade, 2019. p. 75.

3 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União:* seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

4 KRELL, Andreas J. Entre desdém teórico e aprovação na prática: os métodos clássicos de interpretação jurídica. *Revista Direito GV*, São Paulo, v. 10, n. 1, p. 295-320, 2014.

É o que descobriremos, embora também se aborde outros pontos relevantes para a compreensão.

Nessa proposta, apresenta-se uma breve análise de conceitos legais de dados pessoais que denomino de diamante bruto, de socialdigitalidade e de liberação incentivada – ou consentimento na era digital

Dados pessoais: diamante bruto

É senso comum que o diamante bruto não tem um valor monetário tão elevado quanto o do já lapidado, trabalhado, tratado. Também se sabe que para alcançar o diamante bruto, o minerador precisa, geralmente, de muita escavação. O comparativo com dados pessoais é possível, porque eles também são minerados no fluxo mediado por computadores.

Dora Kaufman diz que os dados são rastros deixados pelo uso de tecnologias digitais, especificando que alguns são "voluntários- como as publicações em rede sociais e outros involuntários, como as informações armazenadas nos bancos de dados digitais na compra com cartão de crédito, na movimentação bancária online e inúmeras outras ações presentes em nossa rotina"[5]. Informa ainda que

> "por meio dos dados é possível revelar uma infinidade de questões relacionadas à população, desde quais grupos são mais suscetíveis a determinadas doenças até qual é o perfil do cidadão propenso a honrar um empréstimo bancário, até segmentar os consumidores em perfis".[6]

E continua dizendo que o "desafio colocado é encontrar um equilíbrio entre a abertura de dados, pré-requisito para o avanço da IA; a proteção aos dados pessoais; e a transparência sobre o uso dos dados".[7]

5 KAUFMAN, Dora. *A inteligência artificial irá suplantar a inteligência humana?* São Paulo: Estação das Letras e Cores, 2018.

6 *Ibidem.*

7 *Ibidem.*

Kai-Fu-Lee é um investidor de capital de risco que alerta que os dados dos "pagamentos móveis estão atualmente gerando os mais ricos mapas de atividades de consumo que o mundo já conheceu" e que esses dados coletados no momento do pagamento móvel "serão inestimáveis na criação de empresas voltadas para IA no varejo, no mercado imobiliário e em vários outros setores"[8].

Com a mesma concepção de que os dados são derivados das transações econômicas, Shoshana Zuboff diz que o banco de dados flui de dados governamentais e corporativos, incluindo aqueles associados aos bancos, em intermediações, avaliações e pagamentos, às companhias aéreas, aos registros censitários e fiscais, às operações de planos de saúde, informando ainda que eles

> são adquiridos, agregados, analisados, acondicionados e por fim vendidos por *data brokers*, que operam de forma sigilosa, sem seu consentimento e conhecimento, ignorando seus direitos à privacidade e aos devidos procedimentos legais".[9]

Bruno e demais autores[10] entendem que a coleta de quantidade massiva de dados constitui os *datawarehouses* (armazéns de dados) e que os dados não classificados chamam-se *dataveillance* (vigilância de dados), que é constitutiva do *big data*.[11] Dizem que os "governos os coletam para fins de segurança, controle, gestão dos recursos,

8 LEE, Kai-Fu. *Inteligência Artificial*: como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos. Tradução: Marcelo Barbão. Rio de Janeiro: Globo, 2019.

9 BRUNO, Fernanda *et al*. (org.). *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018. p. 27.

10 *Ibidem*, p. 111.

11 É o termo em Tecnologia da Informação (TI) que trata sobre grandes conjuntos de dados que precisam ser processados e armazenados, o conceito do *Big Data* se iniciou com 3 Vs: Velocidade, Volume e Variedade. Existem perfis diferentes de trabalho em *big data* (vamos falar isso mais para o final do capítulo), dentre os quais encontramos: engenheiros de dados, cientistas de dados, administradores de *big data* etc. Ver: https://www.cetax.com.br/blog/big-data/.

otimização das despesas etc.; as empresas privadas recolhem para fins de *marketing* e publicidade, com vistas a aumentar sua eficácia comercial; os cientistas coletam para aquisição e aperfeiçoamento do conhecimento" quanto aos indivíduos "compartilham benevolamente".

Os dados armazenados são acessíveis a todo momento a partir de qualquer computador conectado à internet, qualquer que seja o lugar do globo onde se encontre.

A LGPD,[12] em seu art. 5º, também conceitua dado pessoal como informação relacionada a pessoa natural identificada ou identificável. Esses dados podem ser classificados como sensíveis quando dizem respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Portanto, por terem um potencial discriminatório, devem ser protegidos de maneira mais rigorosa. O dado é anonimizado quando diz respeito a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. E, por fim, banco de dados é o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Em síntese: dado pessoal é todo comportamento digital subjugado à mercantilização. Ou seja, todo comportamento que o usuário de internet tem é um dado armazenado, seja um *like* ou *dislike*, seja um comentário ou uma postagem, tudo é armazenado. Todos os comportamentos geram dados, que são valiosíssimos para o *e-commerce* e também servem como parâmetros de serviços a serem ofertados, após o tratamento.

12 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

Tratamento de dados: *data mining*

Como dito anteriormente, comparamos o diamante bruto aos dados captados que precisam de lapidação para que lhe agregue valor comercial. E esse tratamento vem sendo motivo de preocupação internacional.

A União Europeia é a percussora no assunto da proteção de dados. A Convenção 108[13] foi o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais. Existe a possibilidade de países não europeus aderirem a essa Convenção, o que é o caso dos latino-americanos que ratificaram a Convenção: Argentina (em 2019), México (em 2018) e Uruguai (em 2013). O Brasil passou a ser país observador na Convenção 108 em 2005.

Em outubro de 2018, em Estrasburgo, foi assinado novo tratado, o Protocolo 223, que altera a Convenção para a Proteção de Pessoas com relação ao Processamento Automático de Dados Pessoais, com o objetivo de modernizar e melhorar a Convenção 108. Desse modo, aborda os desafios à privacidade resultantes de novas tecnologias de informação e fortalece a Convenção fornecendo um quadro jurídico multilateral para facilitar o fluxo através das fronteiras, bem como apresenta inovações que incluem dados sensíveis genéticos, biométricos, filiação sindical e origem étnica.

O Brasil, como observador da Convenção desde 2005, fez uma ótima observação, porque a LGPD (Lei nº 13.709/2018), que entrou em vigor em 18 de setembro de 2020, já trouxe as inovações da Convenção europeia, no corpo da lei, bem como apresenta dez princípios – mandamentos de otimização[14] – que precisam ser observados, em graus

13 PARLAMENTO EUROPEU. *Proteção de dados pessoais*. [*S. l.*: *s. n.*], 2021.

14 ALEXY, Robert. *Teoria dos direitos fundamentais*. Tradução Virgílio Afonso da Silva. São Paulo: Malheiros, 2006. p. 90. "O ponto decisivo na distinção entre regras e princípios é que princípios são normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes. Princípios são, por

variados, na medida fática e conforme as possibilidades jurídicas no momento do tratamento de dados, além da boa-fé.

Assim, tem-se a finalidade como primeiro princípio elencado, que visa a realização do tratamento com propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. O segundo é o da adequação, que tem como escopo a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. O terceiro é o da necessidade, que limita o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. O quarto princípio é o livre acesso como garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. O quinto é o da qualidade dos dados, que dará garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. O sexto princípio é o da transparência que é garantida, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. O sétimo princípio é o da segurança, que visa a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. O oitavo diz respeito à prevenção que suscita a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. O nono é um dos que se entende de extrema relevância, pois é o de não discriminação, ou seja, a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou

conseguinte, mandamentos de otimização, que são caracterizados por poderem ser satisfeitos em graus variados e pelo fato de que a medida devida de sua satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídicas".

abusivos. Por fim, o décimo e último princípio é o da responsabilização e prestação de contas, que determina que ocorra a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas.

O tratamento de dados, então, é a operação que se utiliza de técnicas para coleta, agregação e utilização dos dados pessoais; técnicas que deverão ser observadas pelos agentes de tratamento – o controlador e o operador –, que se responsabilizam de forma solidária pela observância e o cumprimento das normas de proteção de dados pessoais, inclusive, da eficácia dessas medidas.

Como temos dito, os dados são diamantes brutos que sofrem a mineração, o *data mining*, que, segundo Antoniette Rouvroy e Thomas Berns, "é aquele momento, a saber, o tratamento automatizado dessas quantidades massivas de dados de modo a fazer emergir correlações sutis entre eles".[15] As correlações sutis são a ponte de convergência entre as necessidades do usuário e a oferta de produtos dos ofertantes – milhares de empresas privadas.

A LGPD determina que o tratamento é toda operação realizada com dados pessoais, como as que se referem a

> coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".[16]

Quanto aos agentes, controlador e operador, podem ser tanto pessoa física (natural) ou jurídica, de direito público ou privado. Ao controlador competem as decisões referentes ao tratamento de dados pessoais e ao operador, a realização do tratamento dos dados pessoais

15 BRUNO *et al.*, *op. cit.*, p. 112.

16 BRASIL. Lei nº 13.709, *op. cit.*

em nome do controlador. Ainda se tem a figura do encarregado, pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

É possível que ocorra a transferência internacional de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro – por exemplo, ONU, OEA, OMS, OIT e Unesco –, bem como é possível que ocorra o uso compartilhado de dados pessoais na comunicação, difusão, na própria transferência internacional, nas interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais, por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privado. A modalidade é termo que oferece dois sentidos, primeiro quanto ao tipo: tipo, categoria, espécie, gênero, qualidade, variedade, variante, forma, modo, modelo; e quanto ao modo de ser específico de uma pessoa: particularidades, peculiaridades, especificidade, circunstância.

Pois bem, até aqui verificou-se como ocorre a mineração dos dados e o tratamento deles, percebendo-se que esses dois fatos ocorrem porque existem pessoas conectadas na rede mundial de internet, convivendo nos mais variados espaços virtuais. Essa convivência social é o que veremos a seguir.

Socialdigitalidade

Aquela olhadinha na página alheia pela janela da internet é uma nova maneira de atitude social, que chamo de "socialdigitalidade". Ela é composta por todos os cidadãos que acessam a rede mundial de computadores, a internet, para comunicar algo ou comunicar-se com alguém.

Internet como Espaço Social é descrita por Jair Ramos como sendo

> mais do que um mundo virtual, tomado como oposto do mundo real, estamos diante da contínua produção humana de novos mundos e de sua colonização por meio de um duplo movimento de produção de conexões e de sua ordenação.

Isso é uma verdade, pois o mundo virtual se baseia "na comunicação mediada por computador, cada vez mais difundida, implica que estes computadores fixos ou móveis sejam produto e produtores de redes, é a distância e relação entre os nós formados por eles que constitui o que chamamos de ciberespaço"[17]. E continua o autor:

> o que é chamado um tanto equivocadamente de virtual – e o equívoco – reside na oposição entre real e virtual – é essa experiência de existir e agir em um espaço cuja matéria é informação. Os ambientes de realidade virtual, [...] são a expressão mais bem acabada dessa experiência de ser, viver e agir com base em uma matéria toda feita de bytes.[18]

Portanto, a ideia que se tinha de espaço social, de sociedade delimitada por um espaço geográfico físico, no ciberespaço, é produzida pela rede de computadores. E neste espaço de "socialdigitalidade" a informação e seus modos de transmissão se tornam a via de comunicação, estreita, rápida e precisa, da nova era digital.

Shoshana Zuboff chama essa nova arquitetura universal de *Big Other*, onde o revigoramento humano dá lugar ao vazio da submissão perpétua, pois essa nova arquitetura

17 *Ibidem*.

18 RAMOS, Jair de Souza. Subjetivação e poder no ciberespaço: da experimentação à convergência identitária na era das redes sociais. *Revista de Antropologia Vivência*, Natal, n. 45, 2015. p. 57-76.

> configura-se como um ubíquo regime institucional em rede que registra, modifica e mercantiliza a experiência cotidiana, desde o uso de um eletrodoméstico, até seus próprios corpos, da comunicação ao pensamento, tudo com vista a estabelecer novos caminhos para a monetarização e o lucro.[19]

Portanto, essa "socialdigitalidade" é a dinastia da "*Big Other*", que é o poder soberano já posto e que suprime a liberdade obtida pelo Estado de direito. No miasma cibernético formado pelo emaranhado de medos, alegrias, ódio e amores, imagens lindas e horripilantes, legalidades e ilegalidades, tudo está lá, e o usuário súdito, sem nenhuma resistência, só e encapsulado em si, acredita estar usufruindo de sua liberdade de autodeterminação e informação. É o *cocooning* (do inglês "*cocoon*", "casulo") do qual Henry Jenkins diz ser o "termo cunhado nos anos 1990 para definir a tendência de isolamento social nas últimas décadas: as pessoas preferem ficar em casa a interagir socialmente"[20]. Hoje, o cidadão da "socialdigitalidade" vive ensimesmado, concentrado, recolhido em seu mundo digital.

No ciberespaço, vivenciando a "socialdigitalidade", o usuário tem à sua disposição todos os serviços e as distrações digitais imaginadas e desejadas, mas sob uma condição, a liberação incentivada de seus dados pessoais.

Liberação incentivada e consentimento

O consentimento exigido na LGPD não surgiu no contexto do uso e coleta de dados pessoais (dados humanos como aqueles referentes a vida, saúde, educação, etnia, opção sexual, gênero, entre outros) por plataformas digitais. É um documento essencial a qualquer pesquisa (mineração e tratamento de dados) e foi difundido inicialmente na pesquisa médica.

19 BRUNO *et al.*, *op. cit.*, p. 43.

20 JENKINS, Henry. *Cultura da convergência*. São Paulo: Aleph, 2008. p. 42-43.

O primeiro código internacional de ética para pesquisas envolvendo seres humanos – o Código de Nuremberg[21] – surgiu em 1947, a partir do conhecimento das atrocidades cometidas por médicos pesquisadores nazistas, que foram reveladas nos julgamentos de crimes de guerra. Nele encontra-se dez pontos a serem observados pelo pesquisador (neste caso, aos agentes controlador e operador).

No ponto um, destacam-se: a capacidade para consentir, o direito de escolha sem qualquer intervenção de elementos de força, fraude, mentira, coação, astúcia ou outra forma de restrição posterior, a informação e o dever e o fato de a responsabilidade de garantir a qualidade do consentimento repousar sobre o pesquisador que inicia ou dirige um experimento ou se compromete nele.

> O consentimento voluntário do ser humano é absolutamente essencial. Isso significa que as pessoas que serão submetidas ao experimento devem ser legalmente capazes de dar consentimento; essas pessoas devem exercer o livre direito de escolha sem qualquer intervenção de elementos de força, fraude, mentira, coação, astúcia ou outra forma de restrição posterior; devem ter conhecimento suficiente do assunto em estudo para tomarem uma decisão. Esse último aspecto exige que sejam explicados às pessoas a natureza, a duração e o propósito do experimento; os métodos segundo os quais será conduzido; as inconveniências e os riscos esperados; os efeitos sobre a saúde ou sobre a pessoa do participante, que eventualmente possam ocorrer, devido à sua participação no experimento. O dever e a responsabilidade de garantir a qualidade do consentimento repousam sobre o pesquisador que inicia ou dirige um experimento ou se compromete nele. São deveres e responsabilidades pessoais que não podem ser delegados a outrem impunemente.[22]

21 TRIBUNAL INTERNACIONAL DE NUREMBERG. Código de Nuremberg. Trials of war criminal before the Nuremberg Military Tribunals. *Control Council Law*, [*s. l.*], v. 10, n. 2, p. 181-182, 1949.

22 *Ibidem*, p. 181-182

Nos seguintes tópicos do Código Internacional de Ética envolvendo seres humanos, ressalta-se: a preocupação com resultados vantajosos para a sociedade; que o estudo deve ser conduzido de maneira a evitar todo sofrimento e danos desnecessários; e que o grau de risco aceitável deve ser limitado pela importância do problema que o pesquisador se propõe a resolver. Ademais, o participante do experimento deve ter a liberdade de se retirar no decorrer do experimento.

Goldim[23] diz que data de 19 de outubro de 1833 o primeiro registro científico de que se tem notícia sobre o uso de um documento estabelecendo uma relação entre um pesquisador e um indivíduo pesquisado.

> O pesquisador era o médico William Beaumont (1785-1853) e o sujeito da pesquisa era Alexis St. Martin. Esta pessoa receberia, além de casa e comida, US$150,00 para estar disponível por um ano para todos os experimentos que fossem realizados. Este caso ficou famoso pelas suas peculiaridades. O paciente, Alexis St. Martin ficou com uma sequela de um tiro acidental de uma arma de fogo, que permitia a observação do interior de seu estômago por anos a fio. O Dr. William Beaumont, responsável pelo atendimento do paciente e posterior realização de experiências é tido como sendo o primeiro fisiologista norte-americano e fundador da Gastroenterologia.[24]

Esse acontecimento tem sido relatado como sendo precursor do Termo de Consentimento Informado; na Declaração Universal dos Direitos Humanos, de 1948, constitui o marco da preocupação com a proteção do ser humano, onde foram ressalvados princípios universais que dizem sobre o mínimo respeito à questão vida. O consentimento livre e informado teve como paradigma uma das capacidades humanas

23 GOLDIM, José Roberto. *Primeira utilização de um contrato de pesquisa*. [*S. l.*: *s. n.*], 1997-2004.

24 *Ibidem*.

que é protegida pela bioética e pelo direito civil, qual seja, a liberdade de escolha, reconhecida no princípio da autonomia.

O Princípio da Autonomia da Vontade diz respeito à capacidade que tem o ser humano, por sua racionalidade, de fazer escolhas e de limitar ações por meio de regramentos que entende melhor para si, avaliando suas possibilidades, direitos e deveres, sem restrições. A racionalidade não se afasta da ética, mas o que é ético para uns não é para outros, muito embora seja uma questão filosófica e moral que tangencia as ações de cada ser humano. Assim, mesmo dentro da liberdade de pensamento, atitudes e escolhas não podem invadir a privacidade e o direito alheio.

A normatização do uso do consentimento informado no Brasil se inicia na década de 1980,[25] na área de saúde. Em 1981 a Divisão de Vigilância Sanitária de Medicamentos do Ministério da Saúde baixou a Portaria nº 16/1981,[26] que instituía o uso de um Termo de Conhecimento de Risco para todos os projetos de pesquisa com drogas não registradas. Não havia qualquer menção sobre os critérios de capacidade do indivíduo para consentir nem sobre os riscos específicos de cada droga. O texto proposto era genérico e padronizado. O Conselho Federal de Medicina, com a Resolução CFM nº 1.081/1982,[27] instituiu que todas as provas necessárias para o diagnóstico e a terapêutica deverão ser realizadas apenas com o consentimento do paciente. E ainda que superficialmente, como diz Goldim, "Esta Resolução já utilizava, os dois componentes, o de informação e a capacidade para consentir".

Não é diferente na Lei nº 13.709/2018, que tem entre seus fundamentos a autodeterminação informativa, que, segundo Doneda,[28] serve

25 GOLDIM, José Roberto. *Primeira utilização de um contrato de pesquisa*. [*S. l.*: *s. n.*], 1997-2004.

26 BRASIL. Ministério da Saúde. Portaria nº 16, de 27 de novembro de 1981. *Diário Oficial da União*: seção 1, Brasília, DF, 14 dez. 1981.

27 CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.081, de 12 de março de 1982. *Diário Oficial da União*: seção 1, Brasília, DF, 23 mar. 1982.

28 DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. Rio de Janeiro: Renovar, 2006.

"para designar o direito dos indivíduos de decidirem por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados". Ademais, o art. 5º, XII da LGPD expressa que o consentimento é "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"; sendo assim, é possível entender que a maioria dos consentimentos não são consentimentos no correto dizer da lei, por não trazerem uma ampla informação sobre o que aquela ação do usuário estará permitindo, pois quase impossível será dizer se houve por parte dos controladores dos dados um esclarecimento, o que leva a pensar que se está diante de outro instituto, a liberação incentivada, e não o consentimento livre e esclarecido.

Diz-se liberação incentivada porque para que o usuário tenha acesso a um determinado espaço social no ciberespaço ele se vê obrigado a oferecer dados pessoais, a título de cadastro ou acesso – às vezes para o *login* é exigido o que são os tais CPF, data de nascimento, sexo, entre outros dados; o que astutamente é praticado nas plataformas digitais. O incentivo decorre da própria necessidade de fazer uso daquele serviço digital ou interação. O que se ganha – o incentivo – é o acesso, a possibilidade de compartilhar o conhecimento, que me são oferecidos em forma de serviços. O incentivo é a informação que é trazida de qualquer assunto a qualquer momento quando você é o pesquisador, quando você está dando aquela espiadinha no mundo. O incentivo é sentir-se incluído no ciberespaço.

A inclusão na socialdigitalidade já é uma necessidade humana, sim, a própria ONU já declarou ser a internet um Direito Humano;[29]

29 Em maio de 2011, reúne-se o Conselho de Direitos Humanos (CDH) na décima sétima sessão, que tem como objetivo a promoção e proteção de todos os direitos humanos, civis, direitos políticos, econômicos, sociais e culturais, incluindo o direito ao desenvolvimento. Dessa reunião surge um relatório com cinco capítulos relatados por Frank La Rue, que destaca a "natureza transformadora da internet não apenas para permitir que os indivíduos exerçam seu direito à liberdade de opinião e expressão, mas também um gama de outros direitos humanos e para promover o progresso da sociedade

mas também são inúmeros os alertas de dependência psíquica ao uso de plataformas digitais. Hoje, para milhões de cidadãos do mundo, existir é sentir-se incluído e interagindo no ciberespaço.

E o consentimento tão aclamado por todos, que é o direito de escolha sem qualquer intervenção de elementos de força, fraude, mentira, coação, astúcia ou outra forma de restrição posterior, transmuta-se em liberação incentivada. Não é consentimento porque não é devidamente informado e sequer esclarecido. Não se entende termos como este: nós e nossos parceiros utilizamos tecnologia do tipo *cookies* e coletamos dados durante a navegação para lhe proporcionar a melhor experiência online e para personalizar o conteúdo e os anúncios publicitários que são exibidos para você. Diga-nos se concorda com o uso de todos estes tipos de *cookies*. Não se sabe de que dados estão falando e o que são os tais "*cookies*", efetivamente, mas, como geralmente não se tem muito tempo para saber mais detalhes, simplesmente aceita-se. "Os *cookies* permitem que as páginas carreguem mais rápido e facilitam a navegação", explica o Google em seu *blog* "Se você os apaga do navegador, apagará a configuração de *sites*, como nomes de usuário e senhas, e é possível que algumas páginas funcionem mais lentamente, já que será necessário carregar todas as imagens novamente".[30] E o que menos o usuário quer é que a página fique lenta, que não consiga navegar, que não possa ver rapidamente o que deseja.

como um todo". Ler a íntegra do relatório em: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

30 A BBC News em matéria jornalística informa: "Esses programas 'espiões' coletam informações-chave para a publicidade online, especialmente no que diz respeito aos anúncios exibidos de forma personalizada para cada usuário. Os cookies 'contam' às marcas e empresas como nos comportamos na internet para que possam exibir propaganda de acordo com nossos gostos e interesses. Entre outras coisas, podem registrar: Links de páginas; Senhas; Números de telefone; Endereço; Tipo de navegador e sistema operacional usados; Histórico de sites visitados". O QUE acontece quando você aceita os cookies de um site e por que é bom apagá-los de tempos em tempos. *BBC News*, London, 27 jul. 2017.

Assim, pelo incentivo de que sua própria necessidade seja satisfeita – sua autocompensação (des)informativa –, o usuário na dinastia do "*Big Other*" queda como um súdito plácido, oferecendo seus dados. E o "*Big Other*", em suas diversas plataformas, de forma astuta e muito bem estudada, oferece em troca benesses, pois conhece seus súditos/usuários mais que eles próprios se conhecem, e levam-nos a oferecer cada vez mais seus dados de forma não plenamente consentida, mas incentivada pelo mundo de informações que compartilha.

Considerações finais

Começamos de forma leve e terminaremos de forma leve. Dissemos que "a curiosidade matou um gato", mas o cidadão da socialdigitalidade não tem medo disso e, ironicamente, também não tem medo de chuva, pois age como aquele que diz "já que estou na chuva vou me molhar". Ou seja, se esbalda e clica em tudo, dá *likes* e *dislike*, usa *emojis* dos mais variados, demonstrando seus sentimentos de aprovação ou desaprovação sem nenhuma percepção ou clareza de que seus dados estão sendo minerados e que serão moeda de troca. O cidadão da socialdigitalidade talvez não tenha a privacidade como seu bem mais precioso, porque com facilidade a renuncia em troca de informação, exibição, exposição.

Como disse no início deste capítulo, esse tema é parte integrante de uma abordagem maior, objeto de pesquisa para a conclusão de doutorado, motivo que não permite que sejam aqui apontadas considerações finais, mas apenas considerações preliminares. Espera-se que a Ciência do Direito tenha fôlego para ficar a par das Ciência da Computação, entendendo que como Ciência Social Aplicada, o Direito precisa urgentemente ter uma visão multidisciplinar sobre o tema de proteção de dados, sob pena de não atender às necessidades da sociedade futura. Quem sabe por meio de políticas públicas de educação

digital, deve-se informar a sociedade dando suporte não só à informação sobre direitos e deveres, mas também à prevenção e precaução, a fim de que sejam adotadas atitudes sustentáveis no ciberespaço e que não se perca a humanidade.

Referências

ALEXY, Robert. *Teoria dos direitos fundamentais*. Tradução: Virgílio Afonso da Silva. São Paulo: Malheiros, 2006.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 15 jun. 2019.

BRUNO, Fernanda *et al.* (org.). *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018.

CONSELHO FEDERAL DE MEDICINA. Resolução nº 1081, de 12 de março de 1982. *Diário Oficial da União*: seção 1, Brasília, DF, 23 mar. 1982.

DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. Rio de Janeiro: Renovar, 2006. Disponível em: https://www.academia.edu/23345535/Da_privacidade_%C3%A0_prote%C3%A7%C3%A3o_de_dados_pessoais. Acesso em: 5 nov. 2019.

FERNANDES, J. P. *Ética e cidadania*: o desafio dos novos valores. Porto: [*s. n.*], 2005.

GOLDIM, José Roberto. *Consentimento informado no Brasil*: primeiras normas. [*S. l.: s. n.*], 1997. Disponível em: http://www.ufrgs.br/bioetica/consbras.htm. Acesso em: 25 set. 2007.

GOLDIM, José Roberto. *Primeira utilização de um contrato de pesquisa*. [*S. l.: s. n.*], 1997-2004. Disponível em: https://www.ufrgs.br/bioetica/beaumont.htm. Acesso em: 3 set. 2007.

HARTMANN PEIXOTO, Fabiano. *Inteligência artificial e direito*. Curitiba: Alteridade, 2019.

JENKINS, Henry. *Cultura da convergência*. São Paulo: Aleph, 2008.

KAUFMAN, Dora. *A inteligência artificial irá suplantar a inteligência humana?*. São Paulo: Estação das Letras e Cores, 2018.

KRELL, Andreas J. Entre desdém teórico e aprovação na prática: os métodos clássicos de interpretação jurídica. *Revista Direito GV*, São Paulo, v. 10, n. 1, p. 295-320, 2014.

LEE, Kai-Fu. *Inteligência Artificial*: como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos. Tradução: Marcelo Barbão. Rio de Janeiro: Globo, 2019.

BRASIL. Ministério da Saúde. Lei 13.709. Portaria nº 16, de 27 de novembro de 1981. *Diário Oficial da União*: seção 1, Brasília, DF, 14 dez. 1981.

O QUE acontece quando você aceita os cookies de um site e por que é bom apagá-los de tempos em tempos. *BBC News*, London, 27 jul. 2017. Disponível em: https://www.bbc.com/portuguese/geral-40730996#. Acesso em: 15 nov. 2021.

PARLAMENTO EUROPEU. *Proteção de dados pessoais*. [*S. l.: s. n.*], 2021. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em: 15 nov. 2021.

RAMOS, Jair de Souza. Subjetivação e poder no ciberespaço: da experimentação à convergência identitária na era das redes sociais. *Revista de Antropologia Vivência*, Natal, n. 45, p. 57-76, 2015. Disponível em: https://periodicos.ufrn.br/vivencia. Acesso em: 5 set. 2020.

SMITH, Adam. *A riqueza das nações*: investigação sobre sua natureza e suas causas. Tradução: João Luiz Baraúna. São Paulo: Nova Cultural, 1996.

TRIBUNAL INTERNACIONAL DE NUREMBERG Código de Nuremberg. Trials of war criminal before the Nuremberg Military Tribunals. *Control Council Law*, [*s. l.*], v. 10, n. 2, p. 181-182, 1949. Disponível em: https://www.ufrgs.br/bioetica/nuremcod.htm. Acesso em: nov. 2020.

LINHAS BÁSICAS DA LEI GERAL DE PROTEÇÃO DE DADOS NA RELAÇÃO DE EMPREGO

Edilton Meireles

Introdução

A Lei Geral de Proteção de Dados (LGPD), a Lei nº 13.709/2018[1], com certo atraso, introduz no ordenamento jurídico brasileiro regras de proteção à vida privada e íntima regulamentando o tratamento de dados que lhes são pertinentes.

Essa nova lei afeta diretamente as relações de emprego, já que, por sua própria natureza, o empregador se utiliza de dados pessoais dos trabalhadores.

Diante de sua importância e mesmo certa ignorância sobre o tema, neste trabalho procura-se apontar suas noções básicas.

Noções preliminares

A Lei nº 13.709/2018 (LGPD)[2] dispõe sobre a utilização (tratamento) de dados de pessoa física por qualquer outra pessoa (física ou jurídica) que não seu titular (dos dados pessoais).

1 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União:* seção 1, Brasília, DF, p. 59, 15 ago. 2018.

2 *Ibidem*.

A Lei tem por objetivo, em especial, a proteção da intimidade e a privacidade das pessoas físicas.

Vale lembrar que por intimidade se tem tudo que se refere à pessoa física em sua individualidade e que não decorra de qualquer relação jurídica mantida com outra pessoa. São os exemplos das convicções religiosas ou políticas da pessoa. Se a pessoa acredita ou não em Deus ou se ela é fascista ou socialista, por exemplo. Tais informações se referem à pessoa em sua individualidade, uma vez que ela não necessita manter relações jurídicas com qualquer outra pessoa para ter essas convicções. Isso também pode ser dito, por exemplo, da imagem da pessoa, suas opiniões filosóficas, seu peso, sua altura, seus gostos pessoais (por tipo de comida, esportes, bebidas etc.), doenças ou deficiências de que seja portador e outros dados decorrentes da sua individualidade em si.

Já por privacidade se tem tudo que se refere à pessoa física em sua relação com outra pessoa física ou jurídica. São os dados que se referem à pessoa natural, mas que decorrem da relação que mantém com outra pessoa, física ou jurídica. Podem ser citados como exemplos o valor do salário contratado, a função exercida numa empresa, o grau de escolaridade, o número do CPF, o número da carteira de identidade, a filiação ou parentesco etc.

Ou seja, nesse segundo caso, os dados que se referem à pessoa, mas que somente surgem em decorrência da sua relação com outra pessoa (inclusive com o Poder Público), são considerados de natureza privada. E, no caso, em regra, salvo os públicos (por exemplo, número do CPF), esses dados somente interessam às pessoas que integram a relação jurídica da qual se extrai a informação (como o valor do salário).

O que são dados?

Para compreender a aplicação da lei é preciso, primeiro, definir os dados pessoais.

A lei fala na proteção de dado pessoal considerando este como a "informação relacionada a pessoa natural identificada ou identificável"[3] (inciso I do art. 5º).

Em resumo, tem-se por dado pessoal toda e qualquer informação que se refere a uma determinada pessoa identificada ou que possa ser identificável. Aqui se inclui todos os dados/informações relacionados à pessoa, seja à sua intimidade ou à sua vida privada. Esses dados podem ser privados ou públicos.

Dentre outros, são dados relacionados à pessoa física: seu nome, data de nascimento, filiação, paternidade (se é pai ou mãe), parentesco, peso, altura, sexo, número do CPF, número da CTPS, número do PIS, número da carteira de identidade, número do SUS, dados relativos ao patrimônio, valor do salário, rendas diversas, grau de escolaridade, formação profissional, experiência profissional, origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, antecedentes criminais, dados de localização etc.

Por dados biométricos se deve entender, conforme disposto no n. 14, do art. 4º da RGPD da União Europeia, os

> dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.[4]

Já por dados genéticos se compreende

3 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União:* seção 1, Brasília, DF, p. 59, 15 ago. 2018.

4 UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016*. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). [*S. l.: s. n.*], 2016.

> os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.[5]

Ou seja, dado pessoal é qualquer informação relativa a uma pessoa natural identificada ou identificável. É identificável uma pessoa que possa ser identificada, direta ou indiretamente, em face de um identificador relacionado com a sua identidade física (inclusive imagem), sexual, fisiológica, genética, psíquico-mental, econômica, cultural, social ou quaisquer outros elementos, informações ou circunstâncias com conteúdo que possa transmitir conhecimento sobre uma pessoa, a exemplo dos dados de sua localização, residência, domicílio, inclusive o endereço IP[6] etc.

Deve-se interpretar de forma ampliativa o conceito de dado pessoal, já que acoberta qualquer informação relacionada a pessoa natural identificada ou identificável. Logo, a imagem-retrato de uma pessoa é considerada um dado pessoal.[7] Assim, o tratamento de dados relacionados à imagem da pessoa natural, desde sua coleta, seja por foto, vídeo ou outro meio qualquer, deve respeitar os princípios e as regras da LGPD.

5 UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016*. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). [*S. l.*: *s. n.*], 2016.

6 ALVES, Lurdes Dias. *Proteção de dados pessoais no contexto laboral*. Coimbra: Almedina, 2020. p. 38. "Um Endereço de Protocolo da Internet (Endereço IP), do inglês Internet Protocol address (IP address), é um rótulo numérico atribuído a cada dispositivo (computador, impressora, smartphone etc.) conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação. Um endereço IP serve a duas funções principais: identificação de interface de hospedeiro ou de rede e endereçamento de localização". ENDEREÇO IP. *In*: WIKIPÉDIA: a enciclopédia livre. [San Francisco, CA: *Wikimedia Foundation*, 2010].

7 REINALDO FILHO, Demócrito. A imagem do indivíduo é dado pessoal: a decisão da autoridade francesa de proteção de dados e suas consequências. *Boletim Jurídico*, Recife, ano 3, n. 134, 2005. LOPES, Marcelo Frullani. A lei geral de proteção de dados pessoais e o direito de imagem. *Jota*, [*s. l.*], 17 ago. 2019.

Isso também pode ser dito, por exemplo, em relação aos dados biométricos, bem como o controle da jornada de trabalho, seja qual for o meio utilizado, pois com este último, no mínimo, obtêm-se dados pessoais sobre o horário, o tempo, a frequência e o local de trabalho do empregado.

Da mesma forma, enquadra-se neste campo o tratamento de dados a partir das comunicações eletrônicas (internet, correio eletrônico, por aplicativos etc.). Isso porque, a partir dessas informações, pode-se obter dados pessoais sobre seu usuário (*site* que acessou, aplicativo utilizado etc.).

Cabe esclarecer, ainda, que o alcance dessa definição significa que os dados pessoais incluem não só os dados ou informações resultantes de fatores objetivos, que podem ser verificados ou retificados, mas também quaisquer outros elementos, informações ou circunstâncias com um conteúdo que possa aumentar o conhecimento sobre uma pessoa identificada ou identificável.

Assim, por exemplo,

> as avaliações e os julgamentos subjetivos podem, na realidade, conter dados pessoais passíveis de incluir elementos específicos da identidade física, fisiológica, psíquica, econômica, cultural ou social do titular dos dados. Isto é igualmente verdade se um julgamento ou uma avaliação forem resumidos em classes ou escalas ou expressos através de outros critérios de avaliação.[8]

Daí se tem que mesmo as avaliações dos empregados, realizadas pelos empregadores, constituem dados pessoais do trabalhador, até porque se referem à sua vida privada.

Deve ficar claro que a lei fala em "dados" (coisas que são dadas) no sentido de coisa-informação, que, tratadas, tornam-se informações. Por exemplo: a altura de uma pessoa é um dado físico. Quando mensurada

8 UNIÃO EUROPEIA. Comissão Europeia. Grupo de Trabalho do Artigo 29° para a proteção de dados. GT 42. *Recomendação 1/2001 relativa aos dados de avaliação dos trabalhadores*. [*S. l.*: *s. n.*], 2001b.

(coletada/tratada), ela se torna uma informação. Assim, a lei protege tanto o dado em si, como a informação extraída de seu tratamento.

O Decreto nº 8.771/2016[9], que regulamenta a Lei nº 12.965/2014[10] (Marco Civil da Internet), em seu art. 14, inciso I, por sua vez, define dado pessoal como aquele relacionado à pessoa natural, "inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa". Logo, os diversos números de registros em cadastros públicos e privados também são dados pessoais (CPF, CTPS, CNH etc.).

Pode-se, assim, resumir que tudo que se refira à pessoa natural em si e em suas relações jurídicas é considerado dado pessoal.

Do tratamento de dados

Também importante a definição de tratamento de dados.

A Lei nº 13.709/2018, em seu art. 5º, inciso X, dispõe que por tratamento entende-se

> toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.[11]

9 BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. *Diário Oficial da União*: seção 1, Brasília, DF, ano 153, n. 89-A, p. 7, 11 maio 2016. Edição extra.

10 BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: seção 1, Brasília, DF, ano 151, n. 77, p. 1-3, 24 abr. 2014.

11 O RGPD da União Europeia define o tratamento como "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais,

Ou seja, tratamento de dados é toda operação que vai desde a sua coleta (obter a informação/dado) até a sua eliminação, passando por sua utilização, modificação (ex.: da informação obtida/registrada), arquivamento, reprodução ou transmissão a outrem etc. Isto é, tudo que se refira ao uso da informação pessoal, desde a coleta à eliminação, é considerado tratamento de dados.

A lei fala em tratamento por qualquer meio, seja ele físico, eletrônico, digital ou qualquer outro. Ou seja, tanto se refere a uma informação coletada a partir do preenchimento de um formulário físico (no papel) quanto àquela obtida *on-line*. Tanto se refere a uma modificação feita em registros físicos (ex.: fichas, livros, formulários, registros de empregados etc.), como àquela realizada em banco de dados digital ou eletrônico (arquivado fisicamente num "HD" ou nas "nuvens").

Ressalte-se que a lei não considera como dados pessoais aqueles que são anonimizados, "salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido" (art. 12)[12].

Dado anonimizado é aquele "relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (inciso III do art. 5º)[13]. Ou seja, é uma informação/dado que se obtém a partir do tratamento de outros dados, mas que, mediante utilização de meios técnicos,

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", conforme o n. 2 do art. 4°. UNIÃO EUROPEIA. Comissão Europeia. Grupo de Trabalho do Artigo 29° para a proteção de dados. GT 42. *Recomendação 1/2001 relativa aos dados de avaliação dos trabalhadores*. [*S. l.: s. n.*], 2001b.

12 *Ibidem*.

13 *Ibidem*.

impossibilita-se que se tenha conhecimento da origem do dado extraído,[14] de modo que não se identifica a pessoa a que o dado se refere.

Por exemplo, uma empresa pode elaborar um relatório estatístico com a indicação de quantas pessoas maiores de sessenta anos de idade acessam o seu *site*. Se na elaboração desse dado ele for desvinculado dos titulares dos dados originais (as pessoas maiores de 60 anos que acessaram o *site*), sem se poder identificá-los, estar-se-á diante de um dado não pessoal, anonimizado (anônimo). Logo, os dados que serviram para elaboração do relatório não serão protegidos pela lei.

Se, porém, neste exemplo, de algum modo, a partir do novo dado obtido (o percentual de pessoas maiores de 60 anos que acessam o *site*) se puder identificar quem são as pessoas a que ele se refere, essa nova informação estará submetida à disciplina da LGPD.[15] Seriam dados pseudoanonimizados, ou seja, aqueles que possibilitam a sua reversão ou a identificação do seu titular.

Cabe esclarecer, ainda, que são considerados dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, identificada ou identificável (§2º do art. 12)[16], inclusive para fins de avaliação na relação de emprego, como já dito acima.

Campo de aplicação da lei

As normas brasileiras de proteção de dados (art. 3º) se aplicam a qualquer operação de tratamento realizada por pessoa natural ou jurídica,

14 Sobre as dificuldades de uma real anonimização dos dados, Ver: NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and fallacies of "personally identifiable information". *Communications of the ACM*, New York, v. 53, n. 6, p. 24, 2010. OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, Los Angeles, v. 57, p. 1701-1778, 2010. REINO UNIDO. UK Information Commissioner Office. *Anonymisation*: managing data protection risk code of practice summary. [*S. l.*: *s. n.*], 2012.

15 Destaque-se, ainda, que se tem por pseudoanonimizados os dados que possibilitam a sua reversão ou identificação do titular do dado.

16 BRASIL. Lei nº 13.709, *op. cit.*

independentemente do país de sede da empresa ou do país onde estejam localizados os dados, desde que:

> I – a operação de tratamento seja realizada no Brasil; II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no Brasil; ou III – os dados pessoais objeto do tratamento tenham sido coletados no Brasil.[17]

Ou seja, aplicar-se-á a lei brasileira se: o tratamento, inclusive a coleta *on-line*, ocorreu no Brasil; se o tratamento tenha sido realizado no exterior (inclusive a coleta da informação), contanto que ele vise ofertar ou fornecer de bens ou serviços; ou se trate-se de tratamento de dados de indivíduos localizados no Brasil.

Vale frisar que se consideram coletados no Brasil os dados pessoais cujo titular aqui se encontre no momento da coleta (§1º do art. 3º)[18].

Cumpre destacar, ainda, que essas regras se aplicam para defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral. Logo, as normas postas na LGPD se aplicam desde a fase de recrutamento (seleção/contratação) à cessação da relação de trabalho, passando pela execução do contrato de trabalho (incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas), gestão, planeamento e organização do trabalho, igualdade e diversidade no local de trabalho, saúde e segurança no trabalho, proteção dos bens do empregador ou do cliente, exercício e gozo (individual) dos direitos e benefícios relacionados com o emprego, dentre outros.

17 BRASIL. Lei nº 13.709, *op. cit.* p. 59.

18 *Ibidem*.

Da exclusão de incidência

A lei prevê, no entanto, situações nas quais ela não se aplica.

Uma hipótese é aquela na qual a operação de tratamento é realizada no Brasil, mas os dados são

> provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto[19].

Ou seja, não se aplica a lei brasileira se o tratamento ocorrer no Brasil, mas os dados sejam provenientes do exterior e não sejam objeto de comunicação ou compartilhamento com agentes de tratamento brasileiro ou, ainda, não sejam objeto de transferência internacional de dados com outro país que não o de origem, desde que este tenha uma legislação de proteção de dados pessoais semelhante ao previsto na lei brasileira.

Assim, por exemplo, se o dado foi coletado no exterior, mas seu tratamento ocorreu no Brasil, não sendo compartilhado com agentes de tratamento brasileiro, e desde que o país de origem tenha uma lei de proteção de dados semelhante à brasileira, à respectiva operação não será aplicável a lei nacional.

Também são excluídos da incidência da lei de proteção de dados o tratamento (art. 4º):

> I – realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II – realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos; ou III – realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; e d) atividades de investigação e repressão de infrações penais".[20]

19 BRASIL. Lei nº 13.709, *op. cit.* p. 59.

20 *Ibidem*.

Ressalte-se que, quando realizado o tratamento para fins acadêmicos, aplicam-se as regras relacionadas ao consentimento de uso dos dados.

Veja que a lei exclui de sua incidência o tratamento de dados "realizado por pessoa natural para fins exclusivamente particulares e não econômicos"[21] (inciso I do art. 4º da LGPD).

Aqui cabe um esclarecimento. Quando a lei fala que não se aplica à pessoa que faz o tratamento para fins "exclusivamente particulares e não econômicos" ela não exclui a pessoa, física ou jurídica, que desenvolve uma atividade que "tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional"[22] (art. 3º, inciso II) e que não tenha fins lucrativos. Ou seja, mesmo as entidades filantrópicas ou outras que não tenham por finalidade obter lucro, a exemplo de igrejas,[23] associações etc., estão submetidas à LGPD. Isto porque estas entidades, ainda que sem fins econômicos, desenvolvem atividade econômica, ofertando bens ou serviços a terceiros. É o que ocorre, por exemplo, com as próprias pessoas de direito público (União, Estados, Distrito Federal, Municípios etc.), que não visam lucro, mas ofertam bens e serviços a terceiros. Logo, desenvolvem atividade econômica.

Dúvida pode existir em relação ao empregador doméstico. Isso porque, de fato, o empregador doméstico faz uso dos dados pessoais do empregado doméstico para fins "exclusivamente particulares e não econômicos".

O RGPD da União Europeia é expresso em excluir de sua incidência o tratamento de dado realizado "por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas" (alínea "c" do n. 2 do art. 2º).[24]

21 BRASIL. Lei nº 13.709, *op. cit.* p. 59.

22 *Ibidem*.

23 Art. 91 da RGPD da União Europeia. UNIÃO EUROPEIA. Comissão Europeia. Grupo de Trabalho do Artigo 29° para a proteção de dados. GT 42. *Recomendação 1/2001 relativa aos dados de avaliação dos trabalhadores*. [*S. l.: s. n.*], 2001b.

24 *Ibidem*.

A LGPD brasileira, porém, não é expressa em relação ao doméstico, podendo-se assim concluir a partir da sua não incidência às pessoas que tratam dos dados apenas para fins "exclusivamente particulares e não econômicos".

Contudo, ainda que a LGPD não se aplique às relações de trabalho doméstico, é certo que a CF, em seu art. 5º, inciso X, assegura a todos, sem distinção, a proteção à intimidade e à privacidade. Logo, mesmos os trabalhadores domésticos estão protegidos em sua intimidade e privacidade contra atos que sejam ofensivos a este direito fundamental. A violação desse direito, portanto, também gera a responsabilidade civil do ofensor.

Dos requisitos

A lei estabelece os requisitos que devem estar presentes para o tratamento de dados (desde sua coleta à eliminação).

Basicamente, os requisitos se dividem entre o que exige o consentimento informado do seu titular (da pessoa física a quem está relacionado o dado) e o que não exige o consentimento.

A lei disciplina, ainda, de forma especial, o tratamento de dados considerados sensíveis e aqueles relacionados à criança e ao adolescente.

Contudo, é preciso destacar que, em qualquer caso, as atividades de tratamento devem observar, além do princípio da boa-fé e outros, o trinômio finalidade, adequação e necessidade (art. 6º)[25].

Ou seja, cumpre a sua finalidade a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades"[26] (inciso I do art. 6º da LGPD).

25 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

26 *Ibidem*.

Observa-se, outrossim, a adequação quando se esteja diante da "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento"[27] (inciso II do art. 6º da LGPD).

E, por fim, respeita-se o princípio da necessidade quando o tratamento de dado se limita "ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados"[28] (inciso III do art. 6º da LGPD).

Daí se tem que, ainda que diante das hipóteses legais de tratamento de dados, este deve ser realizado conforme seus "propósitos legítimos, específicos, explícitos e informados ao titular", observando a efetiva compatibilidade com a sua finalidade, limitando-se, para seu alcance (da finalidade), o tratamento "ao mínimo necessário" dos dados "pertinentes, proporcionais e não excessivos" em relação aos seus objetivos (finalidades do tratamento de dados).

Dispensa do consentimento

A lei estabelece que é dispensável o consentimento do titular do dado pessoal nas seguintes hipóteses (art. 7º, incisos II a X):

1. para o cumprimento de obrigação legal ou regulatória pelo controlador;
2. pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
3. para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

27 *Ibidem*, p. 59.

28 *Ibidem*, p. 59.

4. quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
5. para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
6. para a proteção da vida ou da incolumidade física do titular ou de terceiro;
7. para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
8. quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
9. para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.[29]

Já nas outras hipóteses, é necessário o consentimento informado do titular do dado/informação.

Assim, por exemplo, na relação de trabalho, a empresa pode coletar e fazer o tratamento de dados, independentemente do consentimento do empregado, quando seja necessário para cumprimento de obrigação legal ou regulatória.

Nessa hipótese, a empresa pode tratar os dados necessários, por exemplo, ao preenchimento da Relação Anual de Informações Sociais (Rais)[30] ou todos os outros dados a que se refiram obrigação imposta pelo Poder Público ou por decisão judicial. Aqui se inclui o registro de todos os dados do empregado que, por força de lei, a empresa deva manter.

29 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

30 Ver: BRASIL. Ministério da Economia. Secretaria Especial de Previdência e Trabalho. Portaria nº 1.127, de 14 de outubro de 2019. *Diário Oficial da União*, Brasília, DF, n. 200, p. 26, 15 out. 2019.

Vale frisar que na Rais a empresa deve fazer constar, entre outros dados, alguns de natureza sensível, a exemplo da raça (indígena, branca, preta/negra, amarela, parda),[31] da eventual deficiência (física, auditiva, visual, intelectual (mental), múltipla ou reabilitada).

Da mesma forma, mesmo sem consentimento do titular do dado, pode a empresa realizar o tratamento de dado quando necessário para a execução de contrato ou execução de procedimentos preliminares relacionados a contrato do qual seja parte o titular do dado, desde que haja pedido deste.

Nessa hipótese, se necessário à execução do contrato firmado com o empregado (titular do dado), a empresa poderá realizar o tratamento do dado mesmo sem o consentimento do trabalhador, mas somente naquilo que seja indispensável à execução do contrato. É o caso de a empresa tratar os dados relacionados ao desempenho profissional do empregado para fins de quantificação, por exemplo, do valor do prêmio.

Isso também pode ser dito em relação aos procedimentos preliminares relacionados à celebração do contrato, do qual seja interessado o titular do dado, desde que haja pedido deste. Neste caso, desde que haja pedido do titular do dado para celebrar o contrato, a empresa poderá tratar os dados fornecidos sem o consentimento informado daquele (coletar os dados pessoais do pretendente ao emprego, as informações sobre sua escolaridade, experiência etc.).

Por óbvio, ainda, a empresa poderá fazer uso dos dados "para o exercício regular de direitos em processo judicial, administrativo ou arbitral".

Da mesma forma, mesmo sem consentimento do titular do dado, a empresa pode fazer uso do dado "para a proteção da vida ou da incolumidade física do titular ou de terceiro". Por exemplo, a empresa, ciente da doença do empregado, para proteção de sua própria vida ou de terceiro, pode tratar o dado obtido (doença) sem o consentimento do seu titular.

31 Na categoria de pardos se enquadra quem se declara de raça mulata, cabocla, cafuza, mameluca ou mestiça de preto com pessoa de outra cor ou raça. BRASIL. Ministério da Economia. *Manual de Orientação da Relação Anual de Informações Sociais (RAIS)*: ano-base 2019. Brasília, DF: ME: SEPT: STRAB: SPPT: CGCIPE: 2019. p. 27.

Igualmente, a empresa pode fazer uso do dado "para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária".

Deve ser ressaltado, portanto, que os dados que não são necessários "para o cumprimento de obrigação legal ou regulatória pelo controlador", "para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados", "para o exercício regular de direitos em processo judicial, administrativo ou arbitral" ou "para a proteção da vida ou da incolumidade física do titular ou de terceiro". Salvo se enquadrado em outra hipótese permitida, não poderá ser tratada sem o devido consentimento do trabalhador.

Em todos esses casos, no entanto, mesmo que autorizado o tratamento, o controlador deve observar os três princípios básicos já mencionados aqui, quais sejam, da finalidade, adequação e necessidade. Ou seja, basicamente somente pode fazer o tratamento para a finalidade específica, no limite do necessário.

Por fim, mesmo sem consentimento, é válido o tratamento de dado "quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". Aqui a lei é imprecisa, não definindo claramente o que se pode ter como "interesses legítimos do controlador ou de terceiro".

A lei, porém, dispõe que o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, entre outros, o apoio e promoção de atividades do controlador e a proteção, "em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais" (art. 10)[32].

32 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

Nesse caso, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados (§1º do art. 10)[33], cabendo ao controlador adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse (§2º do art. 10)[34].

Alguns exemplos práticos podem ser mencionados para melhor esclarecer o que seja legítimo interesse do controlador (da empresa que possui o dado pessoal do empregado), lembrando que a autorização para tratamento de dado neste caso, sem o consentimento informado da pessoa, não prevalece quando diante de direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Vale frisar, no entanto, que, na relação de emprego, ao empregador já é dado o direito de tratamento de dado "para o cumprimento de obrigação legal ou regulatória pelo controlador" e "quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato". Logo, muitas das operações de tratamento realizadas pelo empregador a partir dos dados pessoais dos empregados estão respaldadas nestas duas hipóteses.

Assim, como exemplo pode ser citado o uso/tratamento do dado/informação para a detecção de fraudes, quando se pode usar dados pessoais para monitorar, detectar e preveni-las. Por exemplo, pode ser necessário tratar dados pessoais (coletar imagens etc.) para validar a identidade de uma pessoa envolvida numa fraude.

Da mesma forma, tem legítimo interesse no tratamento de dados quando ele é necessário para analisar o uso de sistemas de tecnologia da informação, de modo a protegê-los contra incidentes em geral (cybersegurança), inclusive para investigar e apurar o ocorrido, além de aprimorar a segurança do respectivo produto e/ou serviço. Ou seja, por exemplo, a empresa tem legítimo interesse em obter os dados registrados a partir do acesso de uma pessoa ao seu *site* enquanto

33 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

34 *Ibidem*, p. 59.

informação necessária para aprimorar o sistema de tecnologia. Logo, para tanto não precisa o consentimento do titular do dado.

Igualmente, o tratamento de dados de empregados pode ser necessário (legítimo interesse) para consolidar informações para gerenciamento e administração da empresa. Também valem as situações nas quais a empresa pode realizar o monitoramento do empregado, controlar entrada e saída, fiscalizar o cumprimento de políticas internas, realizar avaliação do empregado, controlar deslocamento em viagens, entre outras situações, desde que pertinentes e não ofendam direitos fundamentais.

Também se enquadra no conceito de interesses legítimos do controlador o tratamento de dados para operações rotineiras da empresa, auditorias, realização de análises de risco e análises estratégicas do negócio, compartilhamento de informações entre empresas afiliadas para fins de gestão do grupo econômico, em operações reestruturação societária e outras atividades corporativas.

A literatura jurídica europeia aponta, ainda, diversas situações nas quais, mesmo à luz da legislação brasileira, o tratamento de dados pessoais do empregado pode ser realizado pelo empregador em face dos seus legítimos interesses. Os exemplos seriam:

> acesso e operações do escritório; ferramentas e aplicativos de gerenciamento de desastres e emergências; diretórios internos, sites de compartilhamento de funcionários, sites internos e outras ferramentas de cooperação e compartilhamento de negócios; linhas de conduta e ética nos negócios; conformidade com políticas internas, requisitos de responsabilidade e governança e investigações corporativas; gravação e monitoramento de chamadas para fins de treinamento e desenvolvimento dos funcionários da central de atendimento; programas de retenção de funcionários; gerenciamento de força de trabalho e número de funcionários, previsões e planejamento; administração profissional de aprendizado e desenvolvimento; administração de viagens; processamento dos dados dos membros da família no

> contexto dos registros de RH (parentes próximos, contato de emergência, benefícios e seguro, etc.); verificações adicionais e específicas de histórico exigidas por clientes específicos em relação aos funcionários dos processadores que têm acesso aos sistemas e instalações dos clientes; defesa de reivindicações (compartilhamento de imagens de CFTV de instalações com seguradoras, quando necessário para processar, investigar ou defender reivindicações devido a incidentes que ocorreram em nossas instalações); contratos entre empresas para operações internas.[35]

A lei fala, ainda, em interesses legítimos de terceiro. Seria o caso de a empresa, em face de contrato celebrado com um terceiro, fornecer a este os dados do trabalhador daquela primeira (empresa terceirizada) que irá prestar serviço para este último (tomador dos serviços). Aqui se enquadraria a hipótese, portanto, de o empregador transmitir à empresa tomadora dos serviços os dados do trabalhador que presta serviços a ele, especialmente quando na sede desta segunda empresa (da tomadora dos serviços terceirizados).

Contudo, em qualquer caso de tratamento de dados com base no interesse legítimo do controlador é preciso, inicialmente, a ponderação de valores. Cabe, então, nesta ponderação, identificar o interesse legítimo, a necessidade do tratamento de dados para atingir a finalidade buscada e a eventual prevalência dos direitos e liberdades fundamentais do titular dos dados pessoais.

Mas, ainda que se justifique o tratamento de dados por este fundamento (interesse legítimo), o controlador deve reduzir ao máximo o impacto negativo à esfera da intimidade e privacidade da pessoa titular do dado pessoal. Para tanto, poderá adotar as seguintes medidas, quando possam ser asseguradas, sem exclusão de outras, se necessárias: 1. assegurar o direito ao *opt-out*, isto é, garantir ao titular dos

35 CENTRE FOR INFORMARTION POLICY LEADERSHIP. *Examples of legitimate interest grounds for processing of personal data*. [*S. l.*: *s. n.*], 2017.

dados pessoais o direito de se opor ao tratamento de dados; 2. maior transparência, ou seja, elevar o grau de transparência no tratamento dos dados; e 3. medidas técnicas de anonimização, pseudonimização ou uso apenas de dados agregados.

Já na hipótese de transmissão de dados para uma terceira pessoa (exemplo: da empresa prestadora de serviços terceirizados para a empresa tomadora dos serviços em relação aos dados pessoais dos trabalhadores terceirizados) impõe-se a adoção de cautelas para se evitar danos e responsabilidade por eles.

Nesse caso, exige-se que o titular do dado a ser transmitido forneça o consentimento expresso para este fim, se a informação é daquelas na qual se exige o consentimento para tratamento dos dados (§5º do art. 7º)[36]. Ou seja, não basta o consentimento originário para o tratamento de dados por parte de outrem. Se aquele quiser transmitir para um terceiro, cabe exigir novo consentimento expresso e específico para este fim.

Esse consentimento expresso e específico, no entanto, é dispensável nas hipóteses previstas na LGPD. Contudo, no mínimo por cautela, cabe ao empregador pedir o consentimento expresso do trabalhador para que, em qualquer hipótese, seus dados pessoais sejam transmitidos a terceiros (a exemplo da empresa tomadora dos serviços).

Por outro lado, à empresa prestadora dos serviços cabe, ainda, exigir da empresa tomadora dos serviços, o compromisso de que não fará tratamento dos dados transmitidos relacionados aos trabalhadores terceirizados fora do âmbito consentido, permitido e com respeito à LGPD.

Já a empresa tomadora dos serviços, que for destinatária da transmissão dos dados coletados pela empresa fornecedora da mão de obra, cabe exigir desta última a documentação relacionada ao consentimento dado pelo trabalhador para essa operação (de tratamento de dados). Cabe-lhe, ainda, se for o caso, solicitar do trabalhador terceirizado o pertinente consentimento para tratamento dos seus dados pessoais, como, por

36 BRASIL. Lei nº 13.709, *op. cit.*

exemplo, para coletar a sua imagem em câmeras de vídeo-segurança, os dados relacionados à entrada e saída do local de trabalho, frequência etc.

Exigência do consentimento informado

Quando não se está diante de uma hipótese na qual a empresa pode realizar as operações de tratamento de dados sem prévio consentimento do titular do dado, é indispensável que haja o consentimento expresso deste. Um exemplo que se pode apontar são os dados sensíveis relacionados à saúde do trabalhador, ou, ainda, aqueles relacionados à sua identidade genética ou os dados biométricos.

Por exemplo, nenhuma lei impõe que a empresa, na fase pré-contratual, deva ter conhecimento sobre as condições de saúde (salvo quanto aos resultados do exame admissional), a identidade genética ou os dados biométricos do trabalhador que deseja contratar.

Como esses dados estão relacionados aos direitos fundamentais de proteção à intimidade ou vida privada da pessoa, também não se pode afirmar que a empresa possuiria um legítimo interesse em poder ter acesso e tratar esses dados quando da fase pré-contratual de seleção do trabalhador, salvo situações especiais devidamente justificadas. Logo, neste caso, exige-se o consentimento do titular do dado para que se possa tratá-los, inclusive em sua coleta, salvo no que for pertinente aos procedimentos "relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados" (art. 7º, inciso V, da LGPD)[37], nos limites da finalidade e da necessidade.

Em qualquer hipótese, no entanto, por medida de cautela, é prudente a empresa solicitar o consentimento, inclusive para evitar alegações de abuso.

Vejam que a lei dispõe que é desnecessário o consentimento "quando necessário para a execução de contrato ou de procedimentos

37 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados" (inciso V, art. 7º, LGPD)[38].

São duas hipóteses: fase preliminar e fase de execução do trabalho.

Na fase contratual, várias são as situações que o consentimento expresso do titular é desnecessário, já que o tratamento é necessário para a própria execução do contrato. É o caso do controle de ponto.

Lembre-se que, nesse caso, o controle da jornada de trabalho pode ser feito com uso de dado biométrico (digital, controle pela íris etc.). Neste caso, essa coleta de dados se enquadra na hipótese em que ela é necessária para a execução de contrato (fiscalização do trabalhador). Logo, dispensa-se o consentimento expresso.

Quanto à fase preliminar, questiona-se: é necessário o consentimento expresso ou se deve entender que o tratamento, neste caso, está autorizado no inciso V do art. 7º da LGPD?

Nesse ponto, a lei fala em dispensa do consentimento "quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados".

A redação não é das melhores. Mas se deve entender que, nesse caso, em relação aos procedimentos preliminares, apenas deve ser tratado (exigido/coletado) o dado que seja necessário, em seu mínimo, para que as tratativas possam chegar a um bom termo, diante de pedido do titular dos dados neste sentido, dado seu interesse em celebrar o contrato. Aqui se deve entender que o titular do dado tenha fornecido e requerido o tratamento do dado quando este seja indispensável para a eventual contratação.

Se a empresa, porém, exigir o fornecimento de algum dado que não seja pertinente à celebração do contrato, ainda que ele tenha sido fornecido pelo titular do dado, salvo expresso consentimento em contrário deste (e ainda assim questionável), é de se ter o tratamento como ilegal ou abusivo.

38 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

No caso, a empresa estaria abusando do seu direito de solicitar o fornecimento de dados quando não guarda pertinência com as diligências necessárias à celebração do contrato. Um exemplo simples e tão comum é revelador dessa desnecessidade. Basta lembrar dos formulários preenchidos por candidatos a emprego nos quais se exige que se informe a raça/cor da pessoa.[39] A pergunta é: qual a importância da cor da pessoa para sua contratação? Se pertinente (ex.: candidato a emprego de ator em filme no qual irá interpretar um escravizado negro), o dado não será coletado de forma abusiva. Se impertinente o dado pessoal, o tratamento é desnecessário. Logo, ilegal.

Questionável, pois, nesse caso, será o próprio consentimento dado pelo titular (§1º do art. 9º)[40], especialmente se ele se encontrar numa situação de vulnerabilidade. Isso porque, ainda que o consentimento tenha sido dado em "manifestação livre, informada e inequívoca" do titular do dado, seu tratamento não terá pertinência com a sua finalidade (selecionar empregado), daí porque deve ser tido por excessivo, não guardando proporcionalidade "em relação às finalidades do tratamento de dados" (art. 6º, inciso III, LGPD)[41].

O que for público, porém, dispensa o consentimento, seja porque se trate de característica inerente à sua categoria (pública) em sua origem (número do CPF, do número da carteira de habilitação etc.), seja em razão de ato do titular do dado que o tornou público (§4º do art. 7º)[42]. Assim, por exemplo, se o titular do dado publica em redes sociais opiniões sobre suas convicções religiosas, políticas etc., o tratamento do dado (coleta etc.) dispensa o consentimento. Contudo, o uso desses

39 Vide um exemplo: http://webcache.googleusercontent.com/search?q=cache:kfKQLcvoMDMJ:www.tecelagemsaogeraldo.com.br/site/rh/RH%2520-%2520Formulario%2520de%2520Solicita%25C3%25A7%25C3%25A3o%2520de%2520Emprego.docx+&cd=14&hl=pt-BR&ct=clnk&gl=br&client=firefox-b-d.

40 BRASIL. Lei nº 13.709, *op. cit.*

41 *Ibidem*, p. 59.

42 *Ibidem*.

dados deve considerar a finalidade, a boa-fé, adequação, necessidade e o interesse público que justificaram sua disponibilização (§3º do art. 7º)[43].

Óbvio, assim, que, por exemplo, a empresa não pode fazer uso da opinião política do empregado para o discriminar, punir, despedir etc. Há de se ter um legítimo interesse no tratamento desse dado tornado público para que se possa fazer seu uso. Ou seja, o tratamento posterior dos dados pessoais que são públicos poderá ser realizado para novas finalidades, "desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos"[44] na Lei de Proteção de Dados (§7º do art. 7º).

Quando exigível, o consentimento há de ser fruto da "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[45] (art. 5º, inciso XII).

Consentimento informado é aquele efetivo, nunca presumido, espontâneo, consciente e esclarecido, isto é, há de ser produto inequívoco de uma vontade livre e esclarecida, isenta de erros e equívocos.

No caso, não basta a pessoa consentir; ela deve ter plena consciência das consequências de seu ato, que deve, para tanto, ser informado e esclarecido. Isto é,

> a declaração de vontade só é válida quando emitida consciente e voluntariamente, numa situação em que quem enuncia está em condições de avaliar todas as consequências da sua decisão e decide tanto quanto possível livre de constrangimentos, ameaças ou coações.[46]

43 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

44 *Ibidem*, p. 59.

45 *Ibidem*, p. 59.

46 NOVAIS, Jorge Reis. Renúncia a direitos fundamentais. *In*: NOVAIS, Jorge Reis. *Direitos fundamentais*: trunfos contra a maioria. Coimbra: Coimbra Ed., 2006. p. 256.

Nesse caso,

> a manifestação de vontade deve ser esclarecida, baseando-se no conhecimento concreto de todas as consequências relevantes da limitação, e isenta de erro, em especial no caso de dolo (de outrem), tal como deve ser inequívoca, não bastando, em regra, o consentimento presumido, mesmo que aparentemente possa invocar-se o interesse da pessoa.[47]

Daí porque a lei dispõe que será nulo o consentimento se as "informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca"[48] (§1º do art. 9º).

Nesse mesmo sentido, a lei exige que o consentimento deve ser específico. Ou seja, deve se referir a finalidades determinadas, sendo que as autorizações genéricas para o tratamento de dados pessoais são absolutamente nulas (§4º do art. 8º)[49].

E uma vez dado o consentimento,

> se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações[50] (§2º do art. 9º).

Deve ser esclarecido também que, como já dito acima, mesmo que já obtido o consentimento, se o controlador "necessitar comunicar ou

47 ANDRADE, José Carlos Vieira de. *Os direitos fundamentais na Constituição Portuguesa de 1976*. 5. ed. Coimbra: Almedina, 2012. p. 308.

48 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

49 *Ibidem*.

50 *Ibidem*, p. 59.

compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim"[51] (§5º do art. 7º).

A lei ainda exige que o consentimento deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º)[52]. Se fornecido por escrito, o consentimento deverá constar em cláusula destacada das demais cláusulas contratuais (§1º do art. 8º)[53], sendo ônus do controlador do dado que o consentimento seja obtido em conformidade com a lei.

Por outro lado, o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ficando ratificados, porém, os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (§5º do art. 8º)[54].

Nesse ponto, cabe destacar, ainda, que, em caso de alteração de informação cujo consentimento foi dado para finalidade específica de tratamento ou quando consentido em determinada forma ou duração, bem como haja modificação do controlador ou sobre informações acerca do uso compartilhado de dados pelo controlador e a sua finalidade, o controlador deverá informar ao titular, com destaque e de forma específica, do teor das alterações, podendo aquele revogar o consentimento caso discorde da modificação (§6º do art. 8º)[55].

Tratamento de dados sensíveis

A lei trata de forma específica o que se tem por dados pessoais sensíveis.

Ela define como dados pessoais sensíveis aqueles relacionados com a origem racial ou étnica, convicção religiosa, opinião política,

51 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

52 *Ibidem*.

53 *Ibidem*.

54 *Ibidem*.

55 *Ibidem*.

filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual e dado genético ou biométrico (inciso II do art. 5º)[56].

Nesses casos, o tratamento dos dados sensíveis somente pode ocorrer quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades definidas.

Contudo, esses dados sensíveis podem ser tratados, mesmo sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para "a) cumprimento de obrigação legal ou regulatória pelo controlador"; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (inciso I do art. 7º 167, LGPD)[57].

Assim, por exemplo, o dado sensível relativo à origem racial do empregado pode ser tratado pelo empregador para o preenchimento de cadastros (Rais etc.) quando exigível pelo Poder Público.

A lei, no entanto, veda a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose

56 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

57 *Ibidem*.

e terapia, em benefício dos interesses dos titulares de dados, e para permitir a portabilidade de dados quando solicitada pelo titular ou as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de saúde (§4º do art. 11, LGPD)[58].

Tratamento de dados pessoais de crianças e adolescentes

A lei trata especificamente, ainda, do tratamento de dados pessoais de crianças e adolescentes, que deverá ser realizado em seu melhor interesse, conforme a legislação pertinente.

De especial, o que se exige é que o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (§1º do art. 14)[59].

Poderão, porém, ser coletados dados pessoais de crianças sem o consentimento quando forem necessários para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento (§3º do art. 14)[60].

Outrossim, as informações sobre o tratamento de dados deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança ou do adolescente.

58 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

59 *Ibidem*.

60 *Ibidem*.

Dos direitos do titular do dado pessoal

O titular dos dados pessoais tem direito de obter do controlador dos dados por ele tratados, a qualquer momento e mediante requisição, as seguintes informações ou medidas, na forma da LGPD, art. 18:

> I – confirmação da existência de tratamento;
> II – acesso aos dados;
> III – correção de dados incompletos, inexatos ou desatualizados;
> IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei;
> VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX – revogação do consentimento [...].[61]

Vale ressaltar que esses direitos podem ser exercidos a qualquer tempo, não sujeitos a prazo decadencial ou prescricional.

Observa-se daí, por exemplo, que um empregado despedido há mais de 20 anos pode hoje pedir que a empresa elimine os dados pessoais que coletou do trabalhador à época da relação de emprego.

Daí se tem ainda que, a qualquer tempo, eventual tratamento de dados indevido pode gerar danos ao titular dos dados, atraindo a responsabilidade civil, cujo prazo prescricional começará a correr a partir

61 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

do momento em que o lesionado tomar conhecimento da violação ao seu direito de proteção.

Do acesso aos dados pessoais

Em relação aos dados pessoais, a lei assegura (art. 9º) ao seu titular, de forma específica o amplo acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva, sobre:

> I – finalidade específica do tratamento;
> II – forma e duração do tratamento, observados os segredos comercial e industrial;
> III – identificação do controlador;
> IV – informações de contato do controlador;
> V – informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI – responsabilidades dos agentes que realizarão o tratamento;
> VII – direitos do titular, com menção explícita aos seus direitos.[62]

É assegurado, ainda, ao titular do dado, ainda que haja dispensa de consentimento, o direito de se opor ao tratamento se ele for realizado em descumprimento do disposto na Lei nº 13.709/2018 (LGPD)[63].

Os direitos acima mencionados, todavia, devem ser exercidos mediante requerimento expresso do titular ou de seu representante legalmente constituído, dirigido ao agente de tratamento (§3º do art. 18)[64], cabendo a este, se for o caso, "indicar as razões de fato ou de direito que impedem a adoção imediata da providência"[65] (inciso II do §4º do art. 18).

62 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

63 *Ibidem*.

64 *Ibidem*.

65 *Ibidem*, p. 59.

O pedido do titular dos dados, por sua vez, deve ser atendido sem custos e nos prazos e nos termos previstos em eventual regulamento (§5º do art. 18).

Se for a hipótese, diante do requerimento do titular do dado,

> o responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional[66] (§6º do art. 18).

Cabe destacar que os dados pessoais devem ser armazenados em formato que favoreça o exercício do direito de acesso[67] (§1º do art. 19) e as informações e dados pertinentes serão fornecidos ao seu titular, quando requeridos, por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa[68] (§2º do art. 19).

A lei assegura, ainda, ao titular do dado pessoal, quando o tratamento tiver origem no seu consentimento ou em contrato, o direito de solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento[69] (§3º do art. 19).

Da revisão

O titular dos dados tem, ainda, o direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas aquelas (decisões)

66 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

67 *Ibidem*.

68 *Ibidem*.

69 *Ibidem*.

destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou sobre os aspectos de sua personalidade[70] (art. 20).

Nesse caso, o controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial[71] (§1º do art. 20).

Nessa hipótese, negado o fornecimento sob a justificativa de preservação de segredo comercial ou industrial, a autoridade pública poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais[72] (§2º do art. 20).

Obviamente, ainda, que essa auditoria poderá ser procedida por ordem judicial.

Término do tratamento de dados

A LGPD, em seu art. 15, ainda dispõe que o tratamento de dados pessoais será encerrado quando: A LGPD, em seu art. 15, ainda dispõe que o tratamento de dados pessoais será encerrado quando 1. da verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; 2. fim do período ou prazo de tratamento; 3. a pedido do titular do dado pessoal, inclusive no exercício de seu direito de revogação do consentimento; ou 4. por determinação da autoridade pública quando houver violação ao disposto na respectiva lei (LGPD)[73].

Somente se admite, no entanto, a conservação dos dados para as seguintes finalidades, na forma do art. 16 da LGPD:

70 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

71 *Ibidem*.

72 *Ibidem*.

73 *Ibidem*, p. 59.

> I – cumprimento de obrigação legal ou regulatória pelo controlador; II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na Lei; ou IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados[74].

Vale observar, porém, que esses dados somente devem ser conservados pelo tempo necessário ao fim que se destina. Assim, por exemplo, em relação aos dados conservados para cumprimento de obrigação legal ou regulatória pelo controlador ou mesmo para seu uso em processo judicial, administrativo ou arbitral, há de se observar o prazo prescricional em relação a cada obrigação que se busca comprovar.

Transferência internacional de dados

A lei regula também a hipótese de transferência internacional de dados pessoais (art. 33)[75]. Neste caso, somente é permitida essa transmissão ou transferência, nas seguintes hipóteses:

> I – para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei brasileira; II – quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei brasileira, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; III – quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de

74 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

75 *Ibidem*.

> direito internacional; IV – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; V – quando a autoridade nacional autorizar a transferência; VI – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII – quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público; VIII – quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades"; IX – para o cumprimento de obrigação legal ou regulatória pelo controlador; X – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; e, XI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral.[76]

Assim, por exemplo, uma empresa brasileira somente poderá transmitir os dados pessoais de seus empregados para sua matriz, sucursal, filial, subsidiária etc., localizada no exterior, se o empregado, titular do dano pessoal, de forma expressa, consentir com a transferência internacional (inciso VIII do art. 33)[77], salvo se enquadrar essa operação em outro permissivo legal, por exemplo, para o exercício regular de direitos em processo judicial, administrativo ou arbitral no exterior, conforme permitido no inciso XI do art. 33 da LGPD[78].

Dos agentes de tratamento de dados pessoais

A lei distingue, além do titular dos dados pessoais, ou seja, da pessoa a quem se referem os dados ou informações pessoais, as figuras do 1.

76 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

77 *Ibidem*.

78 *Ibidem*.

controlador, do 2. operador e do 3. encarregado pelo tratamento de dados pessoais.

Controlador é a pessoa natural ou jurídica, de direito público ou privado, que passa a deter os dados pessoais de outrem e a quem compete as decisões referentes ao tratamento de dados pessoais[79] (inciso VI do art. 5º).

Ele (controlador) se distingue do operador, que é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador[80] (inciso VII do art. 5º).

Essas duas pessoas são consideradas os agentes de tratamento (inciso IX do art. 5º)[81]. O primeiro controla os dados pessoais de outrem e o segundo realiza o tratamento em nome do controlador.

A lei prevê, ainda, a existência obrigatória do encarregado, isto é, da pessoa física indicada pelo controlador ou pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), conforme inciso VIII do art. 5º da LGPD[82].

Assim, por exemplo, numa relação de emprego, o controlador do tratamento de dados seria o empregador (pessoa física ou jurídica). Já o operador seria a pessoa que realiza o tratamento de dado em nome do controlador-empregador. Este operador pode ser tanto uma pessoa física, como jurídica. Pode ser o sócio, administrador ou empregado da empresa, como pode ser um terceiro contratado.

O operador seria a pessoa que tem acesso aos dados, podendo tratá-los em nome do operador. Pode ser mais de um. Numa empresa, em relação aos dados dos empregados, por exemplo, os operadores seriam os trabalhadores que têm acesso aos dados para proceder em algum registro, elaborar folhas de pagamento etc.

79 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

80 *Ibidem*.

81 *Ibidem*.

82 *Ibidem*.

Já o encarregado é a pessoa física, designada pelo controlador-empregador ou, eventualmente, pelo operador, com a responsabilidade de manter a comunicação entre o controlador e os titulares dos dados (empregados) ou com a ANPD. O encarregado, por sua vez, tanto pode ser o sócio, acionista, administrador ou empregado da empresa, como pode ser uma terceira pessoa física contratada para exercer essa função.

As atribuições do encarregado, além de outras contratadas, são:

> I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II – receber comunicações da autoridade nacional e adotar providências; III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares[83] (art. 41, §2º).

Controlador, operador e encarregado podem ser a mesma pessoa, desde que natural (pessoa física). Ou seja, nada impede de o empregador pessoa física atuar como controlador, operador e encarregado do tratamento de dados pessoais de terceiro.

No caso de o controlador ser pessoa jurídica, no entanto, o encarregado deve ser indicado por aquele (controlador), já que este (encarregado) deve ser, necessariamente, uma pessoa física.

Em relação ao encarregado, a lei impõe que o controlador, ao indicá-lo, torne pública sua identidade e as informações para contato, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

Da responsabilidade

A lei é clara ao tratar da responsabilidade do controlador e do operador quando do tratamento de dados pessoais de outrem.

83 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

No caso, tanto o controlador como o operador, em razão do exercício de atividade de tratamento de dados pessoais, quando causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, será obrigado a repará-lo (art. 42)[84].

A princípio, numa relação de emprego, o controlador-empregador responde de forma individual. Porém, o operador (inclusive, eventualmente, o empregado da empresa que atua nesta função) responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador (inciso I, §1º, art. 42)[85].

Óbvio, ainda, que respondem de forma solidária todos os controladores que estiverem diretamente envolvidos no tratamento de dados por eventuais danos causados ao titular dos dados pessoais (inciso II, §1º, art. 42)[86].

Vale frisar que o juiz poderá inverter o ônus da prova a favor do titular dos dados quando for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa (§2º do art. 42)[87].

O controlador e operador, no entanto, só não serão responsabilizados quando provarem:

> I – que não realizaram o tratamento de dados pessoais que lhes é atribuído; II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro[88] (art. 43).

84 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

85 *Ibidem*.

86 *Ibidem*.

87 *Ibidem*.

88 *Ibidem*, p. 59.

Diga-se, ainda, que se considera irregular o tratamento de dados pessoais quando não se observa a legislação pertinente ou quando ele (tratamento) não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais figuram: "I – o modo pelo qual é realizado; II – o resultado e os riscos que razoavelmente dele se esperam; III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado"[89] (art. 44).

Destaque-se também que o controlador ou o operador responde pelos danos decorrentes da violação da segurança dos dados ao deixar de adotar as medidas de segurança previstas em lei e der causa ao dano (parágrafo único do art. 44).

Das sanções

Por fim, cabe esclarecer que tanto o controlador como o operador, em razão das infrações às normas previstas na LGPD, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional, na forma do art. 52:

> I – advertência, com indicação de prazo para adoção de medidas corretivas;
> II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III – multa diária, observado o limite total a que se refere o inciso II;
> IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI – eliminação dos dados pessoais a que se refere a infração;
> .....

89 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

> VII – suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> VIII – suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.[90]

Das sanções acima mencionadas, cabe destacar que ao operador pessoa física, quando muito e com bastante reservas, somente se aplicam as indicadas nos incisos I, IV e VIII, pois as demais se dirigem à pessoa jurídica do controlador ou do operador.

Conclusão

A partir do todo exposto, conclui-se que, de fato, a LGPD irá impactar fortemente as relações de emprego, daí deriva a importância de seu estudo e debate.

Com a vigência, por sua vez, impõe-se a adoção de todas as cautelas para que o empregador se enquadre nos ditames da lei, sob pena de responder civilmente em caso de descumprimento das normas de proteção de dados pessoais.

Referências

ALVES, Lurdes Dias. *Proteção de dados pessoais no contexto laboral*. Coimbra: Almedina, 2020.

ANDRADE, José Carlos Vieira de. *Os direitos fundamentais na Constituição Portuguesa de 1976*. 5. ed. Coimbra: Almedina, 2012.

90 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 4 maio 2020.

BRASIL. Medida Provisória nº 959, de 29 de abril de 2020. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 29 abr. 2020. Edição extra. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Mpv/mpv959.htm. Acesso em: 4 maio 2020.

BRASIL. Ministério da Economia. *Manual de orientação da Relação Anual de Informações Sociais (RAIS)*: ano-base 2019. Brasília, DF: ME: SEPT: STRAB: SPPT: CGCIPE, 2019. Disponível em: http://www.rais.gov.br/sitio/rais_ftp/ManualRAIS2019.pdf. Acesso em: 21 set. 2020.

BRASIL. Ministério da Economia. Secretaria Especial de Previdência e Trabalho. Portaria nº 1.127, de 14 de outubro de 2019. *Diário Oficial da União*: seção 1, Brasília, DF, n. 200, p. 26, 15 out. 2019. Disponível em: http://trabalho.gov.br/images/Noticias/Out-2019/portaria-1127-2019.pdf. Acesso em: 20 mar. 2020.

CENTRE FOR INFORMARTION POLICY LEADERSHIP. *Examples of legitimate interest grounds for processing of personal data*. [*S. l.: s. n.*], 2017. Disponível em: https://iapp.org/media/pdf/resource_center/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_16_march_2017.pdf. Acesso em: 19 mar. 2020.

ENDEREÇO IP. In: WIKIPÉDIA: a enciclopédia livre. [San Francisco, CA: Wikimedia Foundation, 2010]. Disponível em: https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP. Acesso em: 20 set. 2020.

LOPES, Marcelo Frullani. A lei geral de proteção de dados pessoais e o direito de imagem. *Jota*, [*s. l.*], 17 ago. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-lei-geral-de-protecao-de-dados-pessoais-e-o-direito-de-imagem-17082019. Acesso em: 18 mar. 2020.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and Fallacies of "Personally Identifiable Information". *Communications of the ACM*, New York, v. 53, n. 6, p. 24, 2010. Disponível em: www.cs.utexas.edu/~shmat/shmat_cacm10.pdf. Acesso em: 4 maio 2020.

NOVAIS, Jorge Reis. Renúncia a direitos fundamentais. *In*: NOVAIS, Jorge Reis. *Direitos fundamentais*: trunfos contra a maioria. Coimbra: Coimbra Ed., 2006.

OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, Los Angeles, v. 57, p. 1701-1778, 2010. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006. Acesso em: 4 maio 2020.

REINALDO FILHO, Demócrito. A imagem do indivíduo é dado pessoal: a decisão da autoridade francesa de proteção de dados e suas consequências. *Boletim Jurídico*, Recife, ano 3, n. 134, 2005. Disponível em: https://www.boletimjuridico.com.br/doutrina/artigo/713/a-imagem-individuo-dado-pessoal-decisao-autoridade-francesa-protecao-dados-consequencias. Acesso em: 18 mar. 2020.

REINO UNIDO. UK Information Commissioner Office. *Anonymisation*: managing data protection risk code of practice summary. [*S. l.: s. n.*], 2012. Disponível em: https://ico.org.uk/media/1042731/anonymisation_code_summary.pdf. Acesso em: 4 maio 2020.

UNIÃO EUROPEIA. Comissão Europeia. Grupo de Trabalho do Artigo 29º para a proteção de dados. WP 55. *Documento de trabalho sobre a vigilância das comunicações electrónicas no local de trabalho*. [*S. l.: s. n.*], 2002. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Acesso em: 20 mar. 2020.

UNIÃO EUROPEIA. Comissão Europeia. Grupo de Trabalho do Artigo 29º para a proteção de dados. GT 249. *Parecer 2/2017 sobre o tratamento de dados no local de trabalho*. [*S. l.: s. n.*], 2017. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Acesso em: 20 mar. 2020.

UNIÃO EUROPEIA. Comissão Europeia. Grupo de Trabalho do Artigo 29º para a proteção de dados. WP 217. *Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7º da Diretiva 95/46/CE*. [*S. l.: s. n.*], 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Acesso em: 20 mar. 2020.

UNIÃO EUROPEIA. Comissão Europeia. Grupo de Trabalho do Artigo 29º para a proteção de dados. *Parecer do Grupo de Trabalho do artigo 29º sobre o tratamento de dados pessoais no âmbito do emprego.* Relatório de síntese. [*S. l.: s. n.*], 2001a. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Acesso em: 20 mar. 2020.

UNIÃO EUROPEIA. Comissão Europeia. Grupo de Trabalho do Artigo 29º para a proteção de dados. GT 42. *Recomendação 1/2001 relativa aos dados de avaliação dos trabalhadores*. [*S. l.: s. n.*], 2001b. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Acesso em: 20 mar. 2020.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016*. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). [*S. l.: s. n.*], 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 20 set. 2020.

O PAPEL DO ESTADO NA PROTEÇÃO DE DADOS DOS SEUS SERVIDORES E SUAS CONSEQUÊNCIAS PARA O ENDIVIDAMENTO DA CATEGORIA

Daniel de Araújo Paranhos

Introdução

O encorajamento do consumo, o crescimento dos serviços bancários e a concessão irresponsável do crédito por parte das instituições financeiras, baseados, sobretudo em extensos bancos de dados de consumidores, ocasionam hodiernamente os altos índices de inadimplência e consequentemente o endividamento do consumidor brasileiro.

Bauman[1] atribui esse consumismo exagerado ao que denomina "sociedade de consumidores", que promove, encoraja ou reforça a escolha de um estilo de vida e uma estratégia existencial consumista, bem como rejeita todas as opções culturais alternativas.

Como consequência, "todos precisam se equipar com um ou outro produto fornecido pelas lojas se quiserem ter a capacidade de alcançar e manter a posição social que desejam, desempenhar suas obrigações sociais e proteger a autoestima – assim como serem vistos

1 BAUMAN, Zygmunt. *Vida para consumo*: a transformação das pessoas em mercadorias. Rio de Janeiro: Zahar, 2008. p. 71.

e reconhecidos por fazerem tudo isso –, e aqueles assim não agem serão rotulados como inadequados, deficientes e abaixo do padrão."[2]

No entanto, para atingir os anseios sociais de consumo, o consumidor necessita possuir crédito e, em uma sociedade capitalista, "onde a função da oferta é criar demanda, aplicável em todos os produtos, incluindo empréstimos, a oferta de empréstimos deve criar e ampliar a necessidade de empréstimos".[3]

Assim, o crédito é o mecanismo que propicia acesso ao consumo, consumo que é vendido como felicidade. Logo, só poderão ser felizes na sociedade de consumidores aqueles que conseguem se inserir no mercado, mesmo que a condição para tanto seja o endividamento.

Entretanto, não podemos responsabilizar apenas um dos atores do mercado de consumo, no caso, os consumidores dos produtos e serviços, vez que o capitalismo inaugurou novo embate de opostos: o fornecedor *versus* o consumidor. Assim, o consumo em massa e a facilidade para obtenção do crédito produz o que Diógenes Faria de Carvalho chama de "sociedade do endividamento".[4]

Há pouco tempo, era extremamente difícil conseguir crédito no Brasil, entretanto, a partir da estabilidade econômica do país e a presença abundante de capital estrangeiro, emprestar dinheiro tornou-se um negócio interessante aos bancos.[5]

Nesse diapasão, além de campanhas massivas de publicidade, com a utilização da autoridade de pessoas famosas, as instituições financeiras se utilizam de intermediários (financeiras e correspondentes

2 BAUMAN, *op. cit.*, p. 74.

3 BAUMAN, Zygmunt. *Vida a crédito*. Rio de Janeiro: Zahar, 2010. p. 28.

4 CARVALHO, Diógenes Faria de; FERREIRA, Vitor Hugo do Amaral. Consumo(mismo) e (super)endividamento (des)encontros entre a dignidade e a esperança. *In*: MARQUES, Cláudia Lima; CAVALAZZI, Rosangela Lunardelli; LIMA, Clarissa Costa de (org.). *Direitos do consumidor endividado II*: vulnerabilidade e inclusão. São Paulo: Revista dos Tribunais, 2016. p. 172.

5 DOLL, Johannes; CAVALLAZZI, Rosângela. Crédito consignado e o superendividamento dos idosos. *Revista de Direito do Consumidor*, São Paulo, v. 107, ano 25, p. 309-341, 2016.

bancários), que contatam diretamente os consumidores para adquirirem os créditos ofertados.[6]

Para tanto, essas empresas utilizam grandes bancos de dados que contêm dados pessoais dos consumidores brasileiros, tais como número de inscrição no Cadastro Nacional de Pessoas Físicas, endereço, telefone de contato residencial, pessoal e comercial, dentre outras informações pessoais, de obtenção, guarda e tratamento ainda bastante nebulosos.

No caso dos servidores públicos, a utilização destes bancos de dados torna-se ainda mais relevante, porquanto há a divulgação por força de lei, pelo ente público ao qual o servidor está vinculado, de informações pessoais desses servidores. A partir de tais dados, as instituições financeiras obtêm os subsídios para formação de bancos de dados empregados, especialmente por processos automatizados, para o fomento da oferta do crédito.

Ocorre que essa equação de propaganda enganosa, utilização de banco de dados para cooptação de consumidores, juros abusivos e comprometimento de renda além do nível legal, "toma para si o título de uma das piores consequências da atual cultura do consumo que faz do consumidor a sua vítima, o endividamento".[7]

Desse modo, a proteção dos dados dos consumidores erige, hodiernamente, como um direito fundamental e possui grande repercussão no que diz respeito ao endividamento, objeto do presente estudo, vez que potencialmente resultará em um maior controle na obtenção, tratamento e utilização dos dados pessoais do consumidor brasileiro.

Danilo Doneda conclui ser

> "necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais

6 DOLL; CAVALLAZZI, *op. cit.*

7 CARVALHO; FERREIRA, *op. cit.*, p. 173.

é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção humana e como um direito fundamental"[8].

Entretanto, é necessário conformar a proteção de dados pessoais do servidor público com os mandamentos de otimização constitucional da publicidade na administração pública, o que implica dar transparência aos atos praticados pelos entes públicos, bem como demais leis espaçadas, como a conhecida Lei de Acesso à Informação, Lei nº 12.527/2011, editada para garantir o acesso a informações relativas a várias áreas da atuação pública, sendo, inclusive, importante instrumento de combate à corrupção e má alocação de recursos públicos.[9]

Assim, persegue-se no presente estudo realizar, a partir de uma leitura de como a utilização dos bancos de dados e cadastros de consumidores tem contribuído para o endividamento do servidor público, como a nova Lei Geral de Proteção de Dados (LGPD), erigida a direito fundamental, poderá dirimir o emprego dessas informações para concessão irresponsável de crédito, bem como a Administração Pública poderá conformar a aplicação da novel legislação, de forma a cumprir ambos os primados constitucionais.

A utilização dos bancos de dados da Administração Pública pelas empresas privadas

A sociedade brasileira se modificou profundamente nas últimas décadas, de modo que elementos políticos, econômicos e especialmente

8 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*, [Chapecó], v. 12, n. 2, p. 91-108, 2011.

9 RIBEIRO, Giovana Bellini. Compatibilidade entre a proteção de dados pessoais e o dever de transparência pública. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. *LGPD e Administração Pública*. São Paulo: Revista dos Tribunais, 2020. p. 293-310, RB.17.1.

demográficos merecem ser destacados para compreender a relevante situação da utilização dos bancos de dados da Administração Pública pelas instituições financeiras como critério potencializador do endividamento do servidor público.

Conforme citado anteriormente, a concessão de crédito no Brasil somente começou a ser facilitada com a sua estabilização econômica, no início do século XXI. Este equilíbrio das finanças nacionais possibilitou a entrada de investimento e capital estrangeiro, que consequentemente provocou o abastamento de capital disponível para pulverização do crédito.

Imperioso destacar também que, no mesmo período, ocorreram mudanças internas na sociedade brasileira, como o crescimento populacional, e, por consequência, houve maior demanda pela prestação de serviços públicos, o que exigiria, igualmente, mão de obra. Além disso, a instabilidade das relações de trabalho privadas, bem como os salários superiores à média do setor, aumentou a procura pelo trabalho no setor público. Assim, emergiu uma nova classe na sociedade brasileira, a advinda do funcionalismo público.

Necessário destacar também que apesar de uma elite do funcionalismo público perceber valores demasiadamente superiores à média da iniciativa privada, a realidade não é tão discrepante: no holerite médio de um servidor municipal, nível mais à ponta na prestação do serviço público, constam cerca de R$ 2,9 mil reais.[10]

Diante do crescimento do número de servidores públicos no Brasil nas últimas décadas, bem como da disponibilidade de rendas regulares e estáveis, mesmo que somente pouco superiores à média da iniciativa privada, o funcionário público tornou-se um potencial alvo para as instituições financeiras.

10 LUPION, Bruno. Servidor ganha 'demais'? Na verdade, funcionalismo é desigual como o Brasil. *Uol*, Brasília, DF, 3 set. 2020.

Nesse contexto, os bancos e o mercado inauguraram diversos produtos voltados a este público, a exemplo do crédito consignado. Nesta modalidade de empréstimo, o único risco eventualmente imposto à instituição financeira era que o servidor público viesse a falecer. Assim, em contraposição, houve uma promessa de redução de juros devido ao baixo risco.[11]

Por ser um crédito acessível, vendido com a promessa de juros baixos, o crédito consignado alcançou grande relevância econômica, bem como potencial lucrativo, tendo em vista a ausência de inadimplemento, o que estimulou uma campanha agressiva de publicidade pelos bancos, como citado anteriormente.[12]

Igualmente, foram criados os chamados correspondentes bancários e financeiras, que tinham como objetivo principal promover a inclusão financeira, visto que aproximaria os bancos das pessoas físicas consumidoras, intermediando a relação entre o fornecedor de serviços bancários e o destinatário final.

Entretanto, a maneira de proceder com essa intermediação por parte destas empresas, bem como a forma com que obtinham informações dos servidores públicos para lhes ofertar os seus serviços, gerou desconfiança no sentido de que os dados dos membros do funcionalismo público não estavam sendo tratados da maneira mais adequada pela Administração Pública, tendo em vista que o nível das informações obtidas e a forma como elas eram utilizadas auxiliaram na oferta inapropriada do crédito. Consequentemente, houve alarmantes níveis de endividamento dos servidores públicos, sobretudo os menos escolarizados.

É sabido que o poder público repassa dados dos servidores públicos aos bancos, uma vez que são contratados para prestação de serviço de pagamento dos salários de seus funcionários, ou seja, para que o

11 DOLL; CAVALLAZZI, *op. cit.*

12 DOLL; CAVALLAZZI, *op. cit.*

servidor receba sua remuneração, necessariamente precisa se vincular a instituição financeira que possui contrato com o seu empregador, por exemplo.

Entretanto, não são evidenciados quais desses dados pessoais são franqueados, nem qual o alcance desse compartilhamento. Ademais, retornando à questão dos empréstimos consignados, há uma espécie de cooperação técnica entre os órgãos públicos e as instituições financeiras, uma vez que é imprescindível a transmissão de dados dos contratos de créditos celebrados entre o servidor e o banco para garantir a retenção diretamente na fonte pagadora para o adimplemento das parcelas do empréstimo.

Importante destacar também que, devido à imposição constitucional e também de legislação extravagante da transparência administrativa, diversos dados pessoais dos funcionários públicos estão à disposição de todos e, inclusive, com acesso facilitado. Assim, empresas vêm usando essa base de dados para auferir lucros.

Através de sistemas na internet, eles compilam e disponibilizam dados dos servidores públicos como telefones, endereços, CPF, RG, data de nascimento, histórico de consignações e até informações de parentes, de modo que o interessado deve dispender valores mensais para poder ter acesso a este tipo de conteúdo, o que configura prática considerada ilegal.[13]

A repercussão desta facilidade de acesso aos dados pessoais do servidor público está no crescimento do seu nível de endividamento, uma vez que as instituições financeiras, sobretudo os intermediários dessa prestação de serviço, no caso, os correspondentes bancários, utilizam essas informações para ofertar empréstimos dos mais variados e de forma absolutamente irresponsável.

13 PF vai investigar denúncia sobre venda de dados pessoais. *Monitor Mercantil*, Rio de Janeiro, 25 abr. 2019.

Irresponsável porquanto não vigilante às regras do direito consumerista. O consumidor, como vulnerável na relação de consumo relativamente às instituições financeiras, deve ser protegido das práticas abusivas. Para tanto, quando da contratação de um empréstimo, deve ter a ciência prévia do conteúdo do contrato a ser firmado.

Assim, na fase pré-contratual o consumidor deveria receber a informação sobre a modalidade do empréstimo, o seu custo efetivo total, correspondente a todos os encargos e despesas da operação, bem como receber, depois de concluída a contratação, uma cópia do contrato, que deve ser redigido em termos de fácil compreensão, o que costumeiramente não ocorre.[14]

Em outras palavras, sob esta ótica, o contrato somente seria válido caso fosse compreensível por um leigo. Portanto, o contrário coloca o consumidor em estado de incerteza sobre o que estaria acobertado pelo contrato e sobre possíveis consequências. Desse modo, o endividamento ocorre porque o consumidor efetivamente não sabe o que está avençando, ele apenas quer ter acesso ao crédito que lhe possibilitará consumir.

Ainda, há a questão das fraudes, quando terceiro que não é o titular dos dados os utiliza para obter empréstimos em benefício próprio, deixando, entretanto, a responsabilidade pelo pagamento para o titular.

Também as empresas intermediárias, ávidas por fechar novas contratações, vez que trabalham com metas e ganham pelo êxito, aproveitam a posse dos dados, inclusive de assinaturas, para realizar contratações em nome do titular, sem que estas tenham sido

14 Art. 6°, III da Lei n° 8.078/90: "São direitos básicos do consumidor:
[...]
III – a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem."
BRASIL. Lei n° 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, ano 128, n. 176, p. 17271, 12 set. 1990.

solicitadas. Esta situação ocorre, sobretudo, nas operações de crédito consignado, atingindo, portanto, os servidores públicos.[15]

Reportagem de 2018 do jornal *Correio Braziliense* fez uma comparação entre o nível de endividamento dos trabalhadores do setor privado e do setor público e concluiu que os servidores públicos devem quase 10 vezes mais que os empregados assalariados – esses com um saldo de R$ 19 bilhões em empréstimos consignados com instituições financeiras.[16]

Percebe-se, desse modo, que a facilidade de acesso aos dados pessoais dos servidores públicos tem contribuído para o endividamento excessivo da categoria, o que eleva ainda mais a necessidade de implementação da nova LGPD no âmbito também da Administração Pública, como será descortinado a seguir.

A proteção de dados como um direito fundamental e dever do Estado e sua conformação com o interesse público

A forma como os dados pessoais dos servidores públicos hodiernamente vêm sendo tratados merece atenção, sobretudo porque causa repercussões severas na vida deles no que diz respeito ao endividamento, como sustentado anteriormente.

Na medida do possível o Estado deve tutelar as relações entre os privados – no caso aqui objetivado, entre bancos e servidores – que venham a violar os direitos fundamentais de uma das partes.[17]

E a utilização ampla das informações particulares dos funcionários públicos para finalidade de pulverização de crédito no mercado, em

15 RECORDE de fraudes com empréstimo consignado. *Tribuna Online*, [*s. l.*], 17 out. 2020.

16 TEMÓTEO, Antonio. Servidores públicos estão cada vez mais endividados. *Correio Braziliense*, Brasília, DF, 19 jul. 2018.

17 REVERDEL, Carlos Eduardo Dieder. Drittwirkung e ADI dos bancos: a proteção fundamental do consumidor ao não superendividamento. *Revista de Direito do Consumidor*, São Paulo, v. 26, n. 110, p. 17-41, 2017.

particular por processos automatizados, é considerada por Danilo Doneda uma atividade de risco, que se concretiza na "possibilidade de exposição e utilização indevida ou abusiva de dados pessoais", Por esse motivo, conclui que "a proteção de dados é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental".[18]

Inicialmente, a proteção de dados pessoais era tratada como uma espécie de adendo do direito à privacidade, entretanto, presentemente ocorreu uma inversão e, assim, como bem pontua Doneda,[19] "a temática da privacidade passou a se estruturar em torna da informação e, especificamente, dos dados pessoais".

E continua o autor:

> "o ponto fixo de referência neste processo é que, entre os novos prismas para visualizar a questão, mantém-se uma constante referência objetiva a uma disciplina para os dados pessoais, que manteve o nexo de continuidade com a disciplina da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo características próprias."[20]

Portanto, com o volume de dados coletados, tratados e distribuídos ultimamente, a proteção de dados ganha contornos de direito fundamental, inclusive garantido constitucionalmente, vez que deriva do direito à privacidade esculpido na nossa Carta Magna.[21]

Antes do advento da LGPD, o ordenamento jurídico brasileiro não possuía uma legislação específica sobre o tema, tendo o operador

18 DONEDA, 2011.

19 DONEDA, Danilo. *Da privacidade à proteção de dados*. 2. ed. São Paulo: Revista dos Tribunais, 2020. p. 172.

20 DONEDA, 2020, p. 173.

21 Art. 5°: "X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

do direito o múnus de reunir legislações esparsas. Destarte, o nosso arcabouço normativo somente se baseava em "etiquetas, permissões ou proibições para o uso de informações específicas, sem levar na devida conta os riscos objetivos potencializados pelo tratamento informatizado das informações pessoais".[22]

Nesse diapasão, a LGPD surgiu com objetivo precípuo de garantir a instrumentalidade da proteção de dados, que, como dito, deriva da tutela da privacidade, mas não se encerra nela, uma vez que traz e também compila outras relevantes garantias fundamentais antes espaçadas no ordenamento jurídico brasileiro.[23]

Conforme explicitado logo no seu art. 1º,[24] a LGPD é igualmente de observância obrigatória pelas pessoas jurídicas de direito público. Outrossim, pela sua instrumentalidade, a LGPD também normatizou a forma como a Administração Pública deve tratar os dados que se encontram sob seu controle, além dos princípios gerais que balizam toda aplicação da lei e que devem ser observados também pelo ente público. A lei abordou o assunto especialmente no Capítulo IV.

Depreende-se em uma leitura sumária do texto que apesar de um aparente conflito com os princípios basilares da administração pública, especialmente o da publicidade, existe uma conformação deles com a LGPD, e isso resta evidente logo no primeiro artigo do capítulo 23, que versa:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à

22 DONEDA, 2020, p. 261.

23 DONEDA, 2020, p. 265.

24 "Art. 1° Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".
BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n° 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, p. 59, 15 ago. 2018.

> Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público [...]

Como visto, a Lei nº 13.709/2018[25] faz referência expressa à Lei de Acesso à Informação (Lei nº 12.527/2011)[26], bem como conforma a necessidade de atendimento aos pressupostos intrínsecos da administração pública, no caso a finalidade pública e o interesse público.

Com a acomodação da proteção de dados com o privilégio ao interesse público, o legislador está vedando o referido tratamento em atendimento a interesses privados ou particulares.[27]

Deste modo, o tratamento de dados pela Administração Pública deve obedecer aos seguintes requisitos: 1. a previsão legal; 2. a finalidade; 3. os procedimentos e as práticas utilizadas nesse tratamento; 4. indicar um encarregado que passará a responder por essas atividades, devendo essas informações serem claras e estarem presentes em veículos de fácil acesso, de preferência em seu sítio eletrônico.[28]

Cumprindo esses requisitos, a Administração Pública conseguirá não somente atender aos primados da publicidade e transparência no

25 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

26 BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, ano 148 n. 221-A, p. 1-4, 18 nov. 2011. Edição extra.

27 COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados comentada*. 3. ed. São Paulo: Revista dos Tribunais, 2020. p. 145.

28 CANHADAS, Fernando Augusto Martins. A Lei de Acesso à Informação e a Lei Geral de Proteção de Dados: a transparência proibida. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. *LGPD e Administração Pública*. São Paulo: Revista dos Tribunais, 2020. p. 245-444.

trato da coisa pública, mas também proteger os dados pessoais que estão sob sua responsabilidade.

Importante lembrar também que não estão sob a posse do Estado apenas os dados de seus servidores, mas também de boa parte da população: dados dos contribuintes, seus dependentes, dados dos inscritos no Sistema Único de Saúde, INSS, FGTS, DETRAN, órgãos de segurança pública etc.

A posse desses dados inclusive é importante para consecução da sua própria função de execução de políticas públicas, prestação de serviço público, cumprimento do seu poder de polícia, dentre outras atribuições.

Dessa forma, a implementação da LGPD no âmbito da Administração Pública demonstra-se de extrema importância, uma vez que conforme restou evidenciado, esta não vem cumprindo a rigor os preceitos da novel legislação.

Proteção aos dados dos servidores públicos como proteção ao endividamento

Sustentamos que o Estado ainda não consegue dar guarida às determinações da Lei nº 13.709/2018[29], porquanto são flagrantes os casos de utilização dos dados pessoais dos seus servidores públicos por entidade privadas, especialmente instituições financeiras, e que devido a esta falta de implementação da LGPD, a omissão do Estado contribui significativamente para o endividamento excessivo dos integrantes do funcionalismo público, sobretudo nos níveis mais básicos.

Há pouca transparência nos acordos de cooperação firmados pelo Poder Público com entidades privadas, de modo que não se sabe exatamente quais dados estão sendo compartilhados, bem como nos portais de transparência muitas vezes são divulgados dados desnecessários, fragilizando a privacidade do funcionário público.

29 BRASIL. Lei nº 13.709, *op. cit.*

Deve-se destacar também que esta prática não coaduna com a própria prevalência do interesse público sobre o privado, já que o compartilhamento das bases de dados que estão sob a posse do ente público promove um evidente benefício às instituições financeiras, encerrando flagrante afronta ao princípio do interesse público.

A LGPD criou uma série de barreiras e condicionantes ao tratamento e dados e informações pessoais, possuindo o Poder Público exceções, em detrimento aos particulares, quanto à utilização para cumprimento de políticas públicas e o compartilhamento de dados com empresas contratadas para o desenvolvimento de atividades relacionadas às funções administrativas.[30]

Logo, não há impedimentos no sentido do compartilhamento de dados entre o Estado e a instituição financeira que presta o serviço de abertura de contas para pagamento das remunerações dos servidores de determinado órgão, por exemplo. Entretanto, essa partilha deve ocorrer seguindo os demais regramentos da lei.

Guillermo Glassman sintetiza essa necessidade de conformação, quando diz que "a introdução da LGPD no sistema jurídico brasileiro representa a inserção de um novo elemento na equação que balanceia o dever de publicidade a que está submetida à Administração Pública e a proteção da intimidade e vida privada das pessoas".[31]

E conclui:

> o acesso a informações pessoais de terceiros exige uma boa justificativa jurídica e uma destinação específica. Ou seja, deve haver um motivo específico para que haja a divulgação de cada categoria de informações pessoais e a cada uma delas deve corresponder o cumprimento de valores jurídicos bem definidos.[32]

30 GLASSMAN, Guillermo. Interfaces entre o dever de transparência e a proteção dos dados pessoais no âmbito da Administração Pública. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. *LGPD e Administração Pública*. São Paulo: Revista dos Tribunais, 2020. p. 863-878, RB.48.4.

31 GLASSMAN, *op. cit.*, RB.48.5.

32 GLASSMAN, *op. cit.*

Destarte, a própria LGPD aponta soluções possíveis em relação aos dados concernentes aos servidores públicos, objeto do presente trabalho, primeiramente em relação à remuneração deles, que por obrigação legal de transparência na gestão é divulgada de maneira ostensiva, e posteriormente em relação ao compartilhamento de dados com entidades privadas.

Inicialmente, no que diz respeito à remuneração de agentes públicos, alguns cuidados podem ser adotados de forma dirimir a utilização indevida desses dados, a exemplo da retirada do nome ou anonimização do banco de dados, conforme art. 12 da LGPD.[33]

Igualmente, o acesso à informação poderá ser individualizado, de modo que cada pessoa que ali adentrar possa ser identificada, facilitando, portanto, a responsabilização em caso de uso indevido desses dados.

Noutra ponta, em relação ao compartilhamento dos dados com entidades privadas, novamente a solução nos é apresentada pela lei, dessa vez pelo art. 26, que veda a transferência de dados pessoais constantes nos seus bancos de dados, com exceção de quando houver previsão legal ou respaldo em contratos, convênios ou instrumentos congêneres.[34]

E mesmo no caso das exceções é imposto pelo citado dispositivo o respeito aos princípios de proteção de dados pessoais elencados no art. 6º da Lei, de tal modo que essa transferência de dados deve ter uma finalidade, com a explicitação da motivação desse compartilhamento, além do imperativo de se apontar a necessidade.

33 GLASSMAN, *op. cit.*

34 "Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6° desta Lei.
§ 1° É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
[...]
IV – quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres".
BRASIL. Lei n° 13.709, *op. cit.* p. 59.

Também deve ser mantida a transparência, isto é, deve ser ofertado o livre acesso ao titular, para que ele tenha o protagonismo na propriedade dos seus dados e, sobretudo, saiba com quem essas informações foram divididas.

Implementando esses dispositivos o Poder Público contribuirá sobremaneira com a preservação dos dados pessoais dos seus servidores, ao passo que não abrirá mão do seu mister de mirar o interesse público e a transparência pública no exercício de seu múnus.

Nessa direção, ainda poderá contribuir com redução do alarmante índice de endividamento do funcionário público, pois ficou evidenciado que a forma como esses dados vêm sendo manipulados presentemente tem colaborado para a pulverização irresponsável do crédito.

Assim, por esses servidores terem seus dados mais expostos por obrigação legal, bem como pelo fato de o crédito consignado ser uma forma de concessão do crédito mais seguro aos bancos, eles estão mais suscetíveis a essas práticas, sendo, desse modo, papel do Estado garantir essa proteção.

Conclusão

Percebe-se que o crescimento do consumo é um fenômeno social das últimas décadas, de modo que o fomento da cultura do consumismo leva ao desenvolvimento da pulverização do crédito na sociedade e, por consequência, aos altos índices de endividamento.

Como corolário da política de concessão irresponsável do crédito está a manipulação de dados pessoais com formação de grande banco de dados de consumidores para promoção massiva desse tipo de oferta. Nesse viés, os servidores públicos estão mais suscetíveis às más utilizações das suas informações pessoais, uma vez que elas são expostas por determinação legal pelo próprio ente ao qual está vinculado.

O Poder Público hodiernamente não protege a contento os dados que mantém em sua posse, propiciando a coleta e o emprego indevido destas informações pessoais, inclusive para fins ilícitos. Esta situação tem contribuído sobremaneira para o alto índice de endividamento do funcionário público, principalmente os de nível fundamental e médio, pois, conforme sustentado, estão mais expostos.

Neste panorama, restou demonstrado que a LGPD oferta instrumentos adequados para promover a defesa das informações pessoais do funcionalismo público, sem, no entanto, desatentar-se à promoção do interesse público e a transparência governamental, primados constitucionais assim como a privacidade.

A aparente contradição entre os mandamentos de otimização constitucional fora descortinada pela própria legislação, que conseguiu de maneira muito cuidadosa conformar o interesse público com o resguardo do direito à privacidade e, consequentemente, da proteção de dados pessoais.

Entretanto, ainda falta que o Poder Público dê efetividade à LGPD, uma vez que ainda não a implementou da maneira adequada, possibilitando ainda que os dados sob sua tutela tenham destinações indevidas.

A implementação apropriada da LGPD trará, conforme defendido neste trabalho, importante contribuição para diminuição dos índices de endividamento do consumidor brasileiro, sobretudo o servidor público, visto que com a adoção das práticas disciplinadas na novel legislação, será possível identificar quem estará manipulando os dados, com quem estes serão compartilhados, bem como inibirá a utilização ilícita dessas informações, com vista, inclusive, a eventual reparação civil, dentre outros benefícios, fatores esses preponderantes para o cumprimento das balizas trazidas pela lei, especialmente por se tratar de um direito fundamental.

Referências

BAUMAN, Zygmunt. *Vida para consumo*: a transformação das pessoas em mercadorias. Rio de Janeiro: Zahar, 2008.

BAUMAN, Zygmunt. *Vida a crédito*. Rio de Janeiro: Zahar, 2010.

BRASIL. Lei n° 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, ano 148 n. 221-A, p. 1-4, 18 nov. 2011. Edição extra.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

CANHADAS, Fernando Augusto Martins. A Lei de Acesso à Informação e a Lei Geral de Proteção de Dados: a transparência proibida. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. *LGPD e Administração Pública*. São Paulo: Revista dos Tribunais, 2020. p. 245-444.

CARVALHO, Diógenes Faria de; FERREIRA, Vitor Hugo do Amaral. Consumo(mismo) e (super)endividamento (des)encontros entre a dignidade e a esperança. *In*: MARQUES, Cláudia Lima; CAVALAZZI, Rosangela Lunardelli; LIMA, Clarissa Costa de (org.). *Direitos do consumidor endividado II*: vulnerabilidade e inclusão. São Paulo: Revista dos Tribunais, 2016. p. 171-202.

CAVALAZZI, Rosangela Lunardelli; LIMA, Clarissa Costa de (org.). *Direitos do consumidor endividado II*: vulnerabilidade e inclusão. São Paulo: Revista dos Tribunais, 2016.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados comentada*. 3. ed. São Paulo: Revista dos Tribunais, 2020.

DOLL, Johannes; CAVALLAZZI, Rosângela. Crédito consignado e o superendividamento dos idosos. *Revista de Direito do Consumidor*, São Paulo, v. 107, ano 25, p. 309-341, 2016.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*, [Chapecó], v. 12, n. 2, p. 91-108, 2011.

DONEDA, Danilo. *Da privacidade à proteção de dados*. 2. ed. São Paulo: Revista dos Tribunais, 2020.

GLASSMAN, Guillermo. Interfaces entre o dever de transparência e a proteção dos dados pessoais no âmbito da Administração Pública. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. *LGPD e Administração Pública*. São Paulo: Revista dos Tribunais, 2020. p. 863-878.

LUPION, Bruno. Servidor ganha 'demais'? Na verdade, funcionalismo é desigual como o Brasil. *Uol*, Brasília, DF, 3 set. 2020. Disponível em: https://economia.uol.com.br/noticias/deutsche-welle/2020/09/03/servidor-ganha-demais-na-verdade-funcionalismo-e-desigual-como-o-brasil.htm.

PF vai investigar denúncia sobre venda de dados pessoais. *Monitor Mercantil*, Rio de Janeiro, 25 abr. 2019. Disponível em: https://monitormercantil.com.br/pf-vai-investigar-denuncia-sobre-venda-de-dados-pessoais.

RECORDE de fraudes com empréstimo consignado. *Tribuna Online*, [*s. l.*], 17 out. 2020. Disponível em: https://tribunaonline.com.br/recorde-de-fraudes-com-emprestimo-consignado.

REVERDEL, Carlos Eduardo Dieder. Drittwirkung e ADI dos bancos: a proteção fundamental do consumidor ao não superendividamento. *Revista de Direito do Consumidor*, São Paulo, v. 26, n. 110, p. 17-41, 2017.

RIBEIRO, Giovana Bellini. Compatibilidade entre a proteção de dados pessoais e o dever de transparência pública. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. *LGPD e administração pública*. São Paulo: Revista dos Tribunais, 2020. p. 293-310.

TEMÓTEO, Antonio. Servidores públicos estão cada vez mais endividados. *Correio Braziliense*, Brasília, DF, 19 jul. 2018. Disponível em: https://www.correiobraziliense.com.br/app/noticia/economia/2018/07/19/internas_economia,695866/servidores-publicos-estao-cada-vez-mais-endividados.shtml. Acesso em: 26 nov. 2020.

EL SECRETO EMPRESARIAL Y LA PROTECCIÓN DE DATOS: UN BREVE ENFOQUE EN EL ORDENAMIENTO JURÍDICO BRASILERO

Marta Carolina Giménez Pereira
Mayana Barbosa Oliveira

Introducción

¿Qué es lo más valioso que posee una empresa? Tomando el ejemplo de la sociedad "Google", una de las mayores empresas del mundo, es fácil concluir que sus mayores activos no son de índole material. El mayor valor que "Google" ostenta, más allá de su propia marca posicionada como la segunda más valiosa en el mundo con un valor estimado en 167,7 billones de dólares,[1] son los millares de datos que detiene cuyo valor resulta imposible de dimensionarse.

Se trate de una tienda pequeña que mantiene un registro de proveedores o de una empresa tecnológica de mayor porte como la citada en el párrafo anterior que almacena datos, comparte y desarrolla nuevas tecnologías a partir de las informaciones de que dispone, los datos fungen como un capital esencial para el sostenimiento de la empresa en una moderna sociedad que marcha al ritmo de los avances tecnológicos.

1 BADENHAUSEN, Kurt. As 100 marcas mais valiosas do mundo em 2019. *Forbes*, New York, 22 mayo 2019.

En entrevista para la *Wipo Magazine*, en su edición de octubre 2019, el Director General de la Organización Mundial de Propiedad Intelectual (en adelante, OMPI), Francis Gurry, anunciaba que estamos frente a una cuestión fundamental para la Propiedad Industrial.[2]

Sobre la Propiedad Industrial es posible afirmar que la misma es la disciplina del derecho que cuida de los bienes intangibles empresariales ocupándose de los mecanismos jurídicos que se destinan a delimitar, regular y tutelar los más diversos de esos bienes que representan un efectivo valor económico en el ámbito empresarial.

A su vez, los derechos de esa disciplina se encuentran dentro de los derechos de Propiedad Intelectual. Así, éstos engloban dos vertientes bien diferenciadas, a saber: a) Derecho de Autor y Derechos Conexos, rama que se ocupa de las obras artísticas, científicas, literarias y audiovisuales en general; y b) Derecho de Propiedad Industrial, ya mencionado, que comprende por su parte las marcas de fábrica y de comercio, patentes de invención, modelos de utilidad y los dibujos y modelos industriales. También comprende los circuitos integrados, los derechos de obtentores vegetales, los secretos empresariales (industriales y comerciales), el nombre comercial, las indicaciones de procedencia o denominaciones de origen y la competencia desleal.[3]

Ante lo mencionado, el presente trabajo posee el propósito de discutir la relación entre la figura de secreto empresarial y la protección de datos personales, principalmente en lo que se refiere a privacidad, presentando desafíos para una convivencia armónica entre ambos.

Para la construcción del presente estudio se utilizó la técnica de investigación bibliográfica y los métodos deductivo y dialéctico.

El trabajo se divide en cuatro partes. En el primer tópico, se aborda la figura del secreto empresarial. En la segunda parte, se describe la

2 GURRY, Francis. Intellectual property in a data-driven world. *WIPO Magazine*, Ginebra, n. 5, oct. 2019. Entrevista, p. 2 y ss.

3 GIMÉNEZ PEREIRA, Marta Carolina. *Efectos de las patentes farmacéuticas*: un análisis de propiedad intelectual. Ciudad de México: Tirant lo Blanch, 2017. p. 27.

relevancia del fenómeno denominado "*big data*" dentro del marco de la Propiedad Industrial, presentando aspectos a ser contemplados por el derecho, como ser, el respeto al principio constitucional de privacidad y de los principios éticos que deben ser observados en las relaciones comerciales, en especial el que se vincula con la transparencia. Ya en el tercer ítem, se esbozan los desafíos a ser presentados con la llegada de la Ley General de Protección de Datos en Brasil, de reciente incorporación,[4] en la búsqueda de una gestión de éstos que vele por su correcta privacidad y proteja las empresas de aquellos actos que configuran competencia desleal.

Delineamientos del secreto empresarial y la protección de datos

El secreto empresarial, ya sea comercial o industrial, puede ser definido como toda información comercialmente útil que, mantenida en secreto, garantiza a su detentor una posición privilegiada ante sus competidores.[5]

La OMPI indica tres características para que pueda delinearse tal concepto. La primera de ellas consiste en el hecho de que la información no puede ser conocida, ya sea por el público, ya sea por el círculo de probables competidores comerciales. La segunda característica es que tal desconocimiento debe conllevar algún tipo de ventaja económica para su propietario, es decir, que ésta sea el efecto o la consecuencia que surge de la no divulgación. Por último, esta figura debe ser objeto de esfuerzos razonables para mantener su cualidad de secreto,[6] como se explicará en detalle más adelante de conformidad con la normativa internacional.

4 Apenas en 2020 ha entrado en vigor en Brasil.

5 WORLD INTELLECTUAL PROPERTY ORGANIZATION. *Trade secrets*. Ginebra: [*s. n.*], [202-?]. p. 5.

6 Se lee a la letra: "A trade secret is defined as any information that is: (1) Not generally known to the relevant business circles or to the public; (2) confers some sort of economic benefit on its owner. This benefit must derive specifically from the fact that it

Quizás la última de las características mencionadas sea la más significativa y la que justifica que la figura conserve su cualidad. El valor del secreto empresarial proviene de su confidencialidad. Luego, toda información de carácter público o que pueda ser fácilmente accesible por un número no restringido de personas, no puede ser considerada como secreto empresarial.

Cabe resaltar la gran extensión del concepto, que abarca tanto aspectos técnicos como comerciales, incluyendo también los datos personales.[7] Así, cualquier información puede ser considerada como secreto empresarial, sea ella de naturaleza técnica, procedimental, metodológica, científica, financiera o de otra índole. En consecuencia, las fórmulas, las recetas, las informaciones técnicas usadas en un proceso de fabricación, los métodos, las rutinas o procedimientos de gerenciamiento de negocios, los planos o procesos de negocios, las condiciones de pago, los cálculos (de precios, de ofertas a clientes, por citar algunos), las especificaciones del producto, las informaciones sobre materias primas utilizadas, las informaciones sobre el patrimonio de la empresa, los datos de prueba, los diseños o esbozos técnicos, las especificaciones de ingeniería, los análisis o anotaciones, los códigos fuente, los códigos objeto, los datos electrónicos, las compilaciones, las informaciones contractuales, la compilación de informaciones usadas por un intervalo de tiempo, los catálogos de proveedores o los de clientes, los banco de datos e inclusive los datos personales o los datos sensibles, entran dentro del rango de esta figura.

Las informaciones pueden caracterizarse como secreto empresarial de forma aislada o pueden presentarse como un conjunto de datos considerados de forma integrada.

is not generally known, and not just from the value of the information itself; and (3) the subject of reasonable efforts to maintain its secrecy. A trade secret continues for as long as the information is maintained as a trade secret". Ibidem, p. 5.

7 FEKETE, Elizabeth Kasznar. *O regime jurídico do segredo de indústria e comércio no direito brasileiro*. Rio de Janeiro: Forense, 2003. p. 65-66.

Es importante recalcar el sentido finalístico o teleológico de la protección jurídica atribuida a esta figura, buscando su mejor comprensión hermenéutica. En efecto, la protección del secreto empresarial se fundamenta como una especie de protección a los actos que constituyen competencia desleal.

La doctrina sugiere que las reglas de las leyes anticompetitivas tendrían finalmente como objetivo proteger a la empresa.[8] Empero, esta perspectiva es impugnada por Oliveira Ascensão, quien defendió que los delitos de competencia desleal están tipificados como delitos de mera actividad, independientemente de la identificación de un bien jurídico objeto de protección.[9]

Otra perspectiva ve la protección contra la competencia desleal como protección de la propiedad intelectual, por lo que el objeto sería la protección de los derechos sobre bienes inmateriales o de un monopolio, significando una lesión a los derechos de propiedad industrial.[10] Una última postura, representada por Brito Filomeno, sostiene que la protección contra la competencia desleal tiene como objetivo último la protección del consumidor. Al representar al destinatario final de la relación de consumo, éste corre el riesgo de ser engañado por actos de competencia desleal.[11]

De hecho, el patrimonio inmaterial de la empresa, en especial este tipo de secretos que describimos, es objeto inmediato de leyes anticompetitivas, siendo ella misma la destinataria de la norma. No obstante, no se puede perder de vista que un análisis sistémico del asunto nos permite concluir que tanto el consumidor como el propio orden económico son los destinatarios mediatos y teleológicamente esenciales de la protección jurídica atribuida a los secretos empresariales.

8 CORREIA, A. Ferrer. *Lições de Direito Comercial*. Coimbra: Lex, 1973. v. 1, p. 245 y ss.

9 ASCENSÃO, J. Oliveira. *Concorrência desleal*. Lisboa: Coimbra Ed., 1994. p. 21, 54-55.

10 MENÉNDEZ, Aurélio. L*a competencia desleal*. Madrid: Civilitas, 1988. p. 33.

11 FILOMENO, José Geraldo Brito e outros. C*ódigo Brasileiro de Defesa do Consumidor comentado*. Rio de Janeiro: Forense, 2000. p. 86.

El Convenio de París para la Protección de la Propiedad Industrial de 1883 (en adelante CUP), importante texto internacional que marca el inicio de una estructuración global en temas de Propiedad Intelectual, asegura en su artículo 10 bis la protección contra la competencia desleal. En su texto, el CUP conceptúa esta actividad de forma amplia, definiéndola como "cualquier acto de competencia contrario a los usos honestos en materia industrial o comercial".[12]

Sin embargo, es importante resaltar las críticas que se suscitan del Convenio, suscrito en París y reformado luego en numerosas ocasiones. El mismo se origina no en base a un análisis económico de los efectos de un sistema internacional de patentes, sino más bien y principalmente fundamentado en los derechos naturales de los inventores y la intención de cada país de proteger su propia tecnología, sin tener en cuenta los efectos que pudieran darse en el contexto internacional y dejando en un segundo plano a la finalidad de maximización de beneficios que la comunidad recibe de la actividad inventiva. Por otro lado, el Convenio, con sus modificaciones, no es un instrumento adecuado para llevar a la práctica los aspectos económicos que pueden fundamentar un sistema internacional de patentes. Sus normas se originan de muy diversos intereses nacionales, especialmente aquellos provenientes de los países industrializados y sin llevar mucho en cuenta aquellos originados de los países en vías de desarrollo y su particular situación frente al mundo globalizado.[13] Éste arrojaba múltiples inconvenientes en el seno de la comunidad internacional y su sistema de patentes y adolecía de capacidad suficiente para solucionar el inconveniente de que la tecnología pasa a ser un bien público, y es entonces apropiada por los países que no la producían, sin incurrir

12 Véase el texto del Convenio de París, edición en internet: https://www.wipo.int/treaties/es/ip/paris. Consultada el: 27 sep. 2020.

13 Ver: GIMENEZ PEREIRA, *op. cit.*, p. 113.

en los costos que implica del régimen de patentes y su concesión, en ninguna de sus distintas etapas.

Puntualizadas estas críticas, que merecen una consideración aparte,[14] cabe ahora adentrarnos en el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC o TRIPS por sus siglas en inglés), en el que aparece una definición más completa de la figura de la competencia desleal. En efecto, el artículo 39.2 del texto legal hace una expresa remisión al artículo 10 bis de la Convención CUP al destacar la importancia de la protección de las informaciones confidenciales. De acuerdo con el texto legal puede entenderse que:

> las personas físicas y jurídicas tendrán la posibilidad de impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honestos, en la medida en que dicha información: a) sea secreta en el sentido de que no sea, como cuerpo o en la configuración y reunión precisas de sus componentes, generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y b) tenga un valor comercial por ser secreta; y c) haya sido objeto de medidas razonables, en las circunstancias, para mantenerla secreta, tomadas por la persona que legítimamente la controla.[15]

De esta tesitura legal surge que para que la información haga derecho a tal protección, son listados los siguientes requisitos, como se anticipó más arriba: i) que no sea conocida en general ni fácilmente accesible; ii) que alcance un valor comercial en virtud de su secrecía; iii) que se adopten precauciones razonables para mantenerla en secreto.

14 GIMENEZ PEREIRA, *op. cit.*, p. 113. y ss.

15 Véase el texto de ADPIC, edición en internet: https://www.wto.org/spanish/tratop_s/trips_s/ta_docs_s/1_tripsandconventions_s.pdf.

El mismo artículo, en su inciso tercero, impone además impone a los países miembros la obligación de garantizar la protección de los datos confidenciales en situaciones en las que las agencias gubernamentales requieran la presentación de dichos datos como condición para la comercialización de medicamentos o productos químicos, absteniéndose de cualquier divulgación, excepto aquellos esenciales para la protección del público.[16] Sobre este inciso, denominado mayormente *data protection* y que ha sido foco de un amplio debate en distintas rondas negociadoras y que se relaciona con lo que se denomina ADPIC PLUS, la moderna tendencia de países desarrollados en ampliar las medidas proteccionistas para sus mercados innovadores, no ahondaremos en este estudio y lo citamos tan sólo a modo de referencia para ilustrar hasta dónde pudieran llegar los datos protegidos.[17]

A pesar de esta amplia protección que aparece con ADPIC, no existe un requisito de registro para garantizar dicha protección, como se requiere para otros institutos de propiedad industrial, como por ejemplo las marcas y las patentes, otras figuras de Propiedad Industrial. Por tanto, la protección de los secretos no está limitada en el tiempo, teniendo efecto inmediato.

Ocurre sin embargo que la protección asegurada a los secretos de este tipo no impide que los mismos sean descubiertos por medios lícitos y éticos, como por ejemplo una invención independiente o por ingeniería inversa. Así, la protección del secreto apenas protege contra lo que se entiende en doctrina como competencia desleal.

En el ámbito brasilero, la Ley de Propiedad Industrial n° 9.279/96, dispone en su artículo 2 que la protección de los derechos de propiedad

16 Véase el texto de ADPIC, edición en internet: https://www.wto.org/spanish/tratop_s/trips_s/ta_docs_s/1_tripsandconventions_s.pdf.

17 Consultar GIMÉNEZ PEREIRA, Marta Carolina. Protección de datos de prueba y su exclusividad en medicamentos y agroquímicos: la interpretación del articulo 39.3 ADPIC. *Revista Eletrônica do Curso de Direito da UFSM*, Santa Maria, RS, v. 14, n. 1, p. 1-13, 2019.

industrial se efectúa, entre otros, mediante la represión de la competencia desleal (ítem V).[18] Esta ley sanciona en diferentes artículos sobre responsabilidad penal y civil por la práctica de competencia desleal, lo que refuerza el principio de independencia entre los dos ámbitos.

En el ámbito penal, nos ceñiremos únicamente a observar los puntos XI y XII del art. 195 de la misma ley ya que son las que interesan a nuestro objeto de estudio. Dichos incisos conllevan una sanción de tres meses a un año, o una multa a quienes:

> "XI. divulga, explora o utiliza, sin autorización, conocimientos, informaciones o datos confidenciales, utilizables en la industria, comercio o prestación de servicios, excluidos aquellos que sean de conocimiento público o que sean evidentes para un técnico en el asunto, de los que tuvo acceso mediante relación contractual o de empleo, incluso después del término del contrato; XII. divulga, explota o utiliza, sin autorización, conocimientos o informaciones a que se refiere el inciso anterior, obtenidos por medios ilícitos o a los que tuvo acceso mediante fraude".[19]

Ya en el ámbito civil, el artículo 209 prevé el derecho a la indemnización por daños y perjuicios que resultaren de actos de violación de los derechos de propiedad industrial y actos de competencia desleal no previstos en esta Ley.[20]

18 El mencionado artículo 2 dispone textualmente: "La protección de los derechos relativos a la propiedad industrial, considerado su interés social y el desarrollo tecnológico y económico del País, efectúase mediante: I. concesión de patentes de invención y de modelo de utilidad; II. concesión de registro de diseño industrial; III. concesión de registro de marca; IV. represión de las falsas indicaciones geográficas; y V. represión de la competencia desleal". Véase el texto de la ley en edición en internet: http://www.sice.oas.org/int_prop/nat_leg/Brazil/SPA/L9279sA.asp.

19 Véase el texto de la ley en edición en internet: https://www.wipo.int/edocs/lexdocs/laws/es/br/br003es.pdf.

20 *Ibidem*.

Por su parte, la Ley General de Protección de Datos n° 13.709/18 (en adelante LGPD),[21] menciona el término *"secreto comercial e industrial"* trece veces, en nueve artículos diferentes, lo que denota una cifra muy superior a la propia Ley de Propiedad Industrial.

Al respecto, la observación que surge es que en todos estos artículos, el secreto empresarial es visto como una especie de excepción legal, que limita los derechos de los usuarios cuando colisionan y, en ocasiones, como objeto de protección por parte del órgano denominado Autoridad Nacional de Protección de Datos (en adelante ANPD) lo que revela la urgencia de discutir, con base al ordenamiento jurídico vigente, prácticas que armonicen la relación entre protección de datos y la tutela de los secretos en análisis.

Relevancia del *big data* para la protección de datos y la propiedad industrial

Con el advenimiento de lo que hoy la doctrina llama "*big data*", la protección de datos personales se ha convertido en un tema sensible. El término se utilizó por primera vez en un artículo científico publicado en 1997 por Michel Cox y David Ellsworth, investigadores de la Administración Nacional de Aeronáutica y del Espacio (NASA), para describir un gran volumen de datos.[22]

Según Shoshana, nuestra sociedad vive el establecimiento de un nuevo modelo económico marcado por la monetización de los datos, es lo que la autora denomina 'capitalismo de vigilancia'.[23] La autora

21 *Vide* texto de la ley en edición en internet: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

22 COX, Michel; ELLSWORTH, David. Managing big data for scientific visualization. *ACM Siggraph*, [*s. l.*], 1997.

23 ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, Fernanda *et al*. *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018. p. 18.

describe este nuevo modelo económico, en pleno desarrollo, como la "lógica de acumulación actualmente institucionalizada que produce ensamblajes en híperescala de datos objetivos y subjetivos sobre los individuos y sus hábitats con el fin de conocer, controlar y modificar comportamientos".[24]

En una entrevista reciente concedida a la Revista de la OMPI, la Wipo Magazine, el director general de la OMPI destacó la necesidad de un amplio debate entre los países miembros de la Organización sobre la efectividad del sistema actual de Propiedad Intelectual para abordar cuestiones que surgen de tecnologías basadas en datos. La atención de la OMPI a la cuestión se justifica por la creciente recopilación, almacenamiento y transferencia de datos por parte de empresas, ya sean privadas o públicas.[25]

La escasa disposición legal sobre la protección de los secretos empresariales en los acuerdos internacionales, ya abordada en este documento, enfrenta ahora nuevos desafíos ante el gran volumen de datos personales que son tratados por empresas públicas y privadas, lo cual abordaremos a continuación.

24 ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, Fernanda *et al*. *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018. p. 57.

25 Así manifestaba a la letra: "We do have to take note of the fact that advanced data-driven digital technology is clearly the dominant force in economic production and distribution within the digital economy. We also have to ask if the statistics reveal increasing use in relation to the industrial economy or if they also apply to the digital economy. How effective the classical IP system will be in addressing all of the issues arising from the data-driven technologies that dominate in the digital economy remains unclear. Undoubtedly, these will pose significant challenges for IP policymakers... At present, there is broad agreement that making data available is a good thing for the development of useful and beneficial products and services. However, governments cannot reasonably require companies to share their confidential data with competitors". GURRY, *op. cit.*, p. 4-5.

Desafíos a enfrentar

La protección de datos, aunque sea de naturaleza privada en cuanto secreto empresarial, y el respeto de los principios éticos son dos aspectos que, a pesar de a primera vista parecer antagónicos, deben convivir de forma armónica en el entorno empresarial, posibilitando la lucha contra la competencia desleal.

La preocupación de la propiedad intelectual de proteger datos, a través de una legislación anticompetitiva, debe ceñirse al hecho de que gran parte de esta información comercial protegida por secreto empresarial son datos personales.

La defensa de la protección de la base de datos mediante el secreto empresarial no significa en modo alguno que los datos personales de terceros, considerados individualmente, sean considerados propiedad inmaterial de la empresa detentora del secreto. Cabe tener en cuenta que tales datos representan derechos individuales personalísimos que, en los términos del art. 5 inciso X de la Constitución Federal de Brasil son inviolables.[26] Es importante también señalar que la Declaración Universal de Derechos Humanos en su artículo 12 y de forma concordante reconoce la privacidad como un derecho humano fundamental.[27]

Por tanto, a pesar de estar incluidos en el "acervo" inmaterial de la empresa, los datos protegidos por secreto empresarial, en teoría, no podrían ser objeto de uso o cesión sin autorización de los titulares.

No obstante este impedimento, las empresas de alta tecnología han cometido numerosas violaciones en este sentido durante las últimas décadas.

26 Véase el texto de la ley en edición en internet: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

27 Consultar el texto de la ley en edición en internet: https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf.

De hecho, ilustrando la cuestión, mencionamos algunos casos según el informe de fuga y filtración de datos, ocurridos inclusive en el año 2020:[28]

- Una base de datos desprotegida de la aplicación "Peekaboo Moments", donde los padres publican fotos y videos de sus hijos, ha sido difundida. Un número no revelado de direcciones de correo electrónico, datos de ubicación geográfica, datos detallados del dispositivo y enlaces a fotos y videos publicados por los padres se vieron afectados.
- Se ha dejado desprotegida en la web una base de datos de soporte al cliente con más de 280 millones de registros de clientes de la firma "Microsoft". La base de datos expuesta de esta empresa reveló direcciones de correo electrónico, direcciones IP y detalles de casos de soporte.
- "TH Suite", un sistema de punto de venta de dispensarios de marihuana en los Estados Unidos, divulgó información personal perteneciente a más de 85.000 pacientes de marihuana medicinal y usuarios recreativos después de dejar su base de datos desprotegida. La violación de datos afectó nombres, fechas de nacimiento, números de teléfono, correos electrónicos, direcciones, nombres de pacientes y números de identificación médica, así como la variedad de *cannabis* y las cantidades compradas, costos totales de transacción, fecha de recepción y fotografías y escaneados de de documentos gubernamentales y sus empleados.
- Más de 10.6 millones de huéspedes de hoteles que se alojaron en el afamado "MGM Resorts"; tenían su información personal publicada en un foro de piratas informáticos (*hackers*). El conjunto de datos expuestos incluye nombres, domicilios, números

28 BEKKER, Eugene. 2020 Data Breaches: The Most Significant Breaches of the Year. *Identity Force*, [s. *l.*], 3 jan. 2020.

de teléfono, correos electrónicos y fechas de nacimiento de antiguos huéspedes del hotel. Actualizado en fecha 15 de julio de 2020, los investigadores encontraron 142 millones de registros personales de antiguos huéspedes del hotel en mención en venta en la *dark web*, lo que sugiere que la violación original fue mayor de lo anunciado anteriormente.

- La aplicación de fotografía denominada "PhotoSquared", expuso la información personal y las fotos de 100.000 personas que descargaron la aplicación.
- "Whisper", una aplicación anónima para compartir secretos, dejó la información de los miembros expuesta en una base de datos no segura y aunque la aplicación no recopila nombres, la base de datos incluye apodos, edades, etnias, géneros y datos de ubicación de más de 900 millones de usuarios.
- El sitio web de lecciones de guitarra en línea "TrueFire", notificó a sus usuarios que un pirata informático o *hacker* había obtenido acceso a nombres, direcciones, números de cuentas de tarjetas de pago, fechas de vencimiento de tarjetas y códigos de seguridad en los últimos seis meses. El número total de usuarios afectados aún se desconoce, pero lo que sí es sabido es que "TrueFire" tiene millones de usuarios en todo el mundo por lo que es posible dimensionar el daño causado.
- Utilizando las credenciales de inicio de sesión de dos empleados a través de una aplicación de terceros utilizada para brindar servicios a los huéspedes, los hoteles "Marriott International" expusieron la información de 5.2 millones de huéspedes. La información personal de los huéspedes del hotel afectados incluye nombres, direcciones postales, direcciones de correo electrónico, números de teléfono, números de cuentas de lealtad y saldos de puntos, empresa, sexo, fechas de nacimiento, programas y números de fidelidad de las aerolíneas vinculadas, preferencias de habitación y preferencias de idioma. Como

antecedente, ya en una violación de datos anterior, en 2018, los hoteles en mención habían expuesto la información personal de 500 millones de huéspedes.

- Las credenciales de las más de 500.000 cuentas de teleconferencia de la plataforma conocida como "Zoom" se encontraron a la venta en la *dark web* y foros de piratas informáticos o *hackers* por solo 0,02 dólares. Las direcciones de correo electrónico, las contraseñas, las URL de reuniones personales y las claves de host se recopilan mediante un ataque de llenado de credenciales.
- Se han puesto a la venta más de 267 millones de perfiles de la red social "Facebook" en la *dark web* por un total de 600 dólares. Los informes vinculan estos perfiles a la filtración de datos descubierta en diciembre, con información adicional de identificación personal adjunta, incluidas direcciones de correo electrónico. Los investigadores aún no están seguros de cómo se expusieron originalmente estos datos, pero señalaron que 16.8 millones de perfiles de *Facebook* ahora incluyen más información de las que se expusieron originalmente.
- Un ataque de relleno de credenciales, utilizando identificaciones de usuario y contraseñas previamente expuestas de la popular compañía de videojuegos "Nintendo", dio a los *hackers* acceso a más de 160.000 cuentas de jugadores. Con el acceso no autorizado a las cuentas, los estafadores pudieron tener la posibilidad de comprar artículos digitales utilizando tarjetas almacenadas, así como ver información personal, incluido el nombre, fecha de nacimiento, sexo, país o región y dirección de correo electrónico.
- Un fallo de seguridad en "*Twitter*" ha dejado expuesta la información de cuenta de usuarios comerciales de esta empresa de red social. No se reveló la cantidad de cuentas comerciales filtradas, pero las direcciones de correo electrónico, los números de teléfono y los últimos cuatro dígitos del número de la tarjeta de crédito de sus usuarios comerciales se vieron afectados.

- Un servidor desprotegido expuso los datos confidenciales pertenecientes a 60.000 clientes de la empresa de software de investigación de historia familiar denominada "Ancestry.com". Los detalles revelados incluyeron direcciones de correo electrónico, datos de geolocalización, direcciones IP, identificaciones de usuarios del sistema, mensajes de soporte y detalles técnicos.
- La plataforma de creación de videos "Promo.com" confirmó que sus 22 millones de clientes tuvieron su información personal y de cuenta reveladas en una violación de datos de terceros. Los datos comprometidos incluían nombres, direcciones de correo electrónico, direcciones IP, ubicación del usuario, género y contraseñas cifradas.
- Una base de datos inseguro develó la información de identificación personal (PII) de 19 millones de clientes y empleados de la empresa de cosméticos "Avon". La información filtrada incluyó nombres, números de teléfono, fechas de nacimiento, direcciones de correo electrónico y direcciones y coordenadas de geolocalización, así como otras informaciones técnicas.
- Otras denuncias se han hecho respecto a empresas tan conocidas como "*Instagram*", "TikTok", "Youtube" de los perfiles de sus usuarios incluyendo, a más de los datos ya mencionados, la divulgación de si perfil pertenece o no a una empresa o si contiene anuncios.
- De idéntico modo aconteció con la empresa "Freepik", una base de datos de imágenes gratuita, que reconoció la divulgación de datos de 8.3 millones de usuarios ocurrida a través de un *malware* inyectado en su enlace, lo que derivó en la colecta de *emails* de todos estos seguidores e inclusive realizó el cifrado de contraseñas de 3.77 millones de ellos.
- Por último, mencionamos el caso de un fabricante de dispositivos de rehabilitación de movimiento, "Dynasplint Systems, Inc.", empresa que sufrió un ataque de cifrado en sus dispositivos

comerciales que expuso la información personal y médica de 103.000 pacientes. La información a la que se accedió incluyó nombres, direcciones, fechas de nacimiento, números de seguro social e información de índole médica.

Los hechos denunciados aquí devienen, entre otros factores, por el desconocimiento e inexperiencia de los usuarios, así como por la rapidez con la que se crean y difunden las nuevas prácticas de "*data mining*",[29] dejando atrás las leyes y normativas existentes, dada la falta de disposición legal moderna que prevenga efectivamente tales arbitrariedades.

Los usuarios se convierten en rehenes de las tecnologías,[30] como por ejemplo las redes sociales, las aplicaciones, los clubes de fidelización o membresías, entre otros, que son utilizadas por las empresas de vigilancia como "anzuelo"; para la captura de datos y conductas. Sin embargo, en este escenario, no existe una autonomía plena por parte de los usuarios, ya que la propia evolución de la vida en sociedad hace inevitable el suministro de datos.

Al respecto, David Lyon sostiene que la ética relacionada con la acumulación de datos debe promover agendas y acciones políticas, y no ser encarada solamente como abstracta o desconectada. El autor no ignora el papel de las leyes, pero éstas, por regla general, no logran ponerse al día con las nuevas tecnologías y los nuevos contextos sociales que se imponen.[31]

A pesar de las grandes deficiencias y problemáticas apuntadas, no se puede negar que el Reglamento General de Protección de Datos (en adelante RGPD), elaborado por la Unión Europea,[32] representó el

29 Concepto de minería de datos o exploración de datos y el conjunto de sus técnicas y tecnologías a tal efecto.

30 ZUBOFF, *op. cit.*, p. 58.

31 LYON, David. Cultura da vigilância: envolvimento, exposição, e ética na modernidade digital. *In*: BRUNO, Fernanda *et al*. *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018. p. 171.

32 Véase el texto de la ley en edición en internet: https://gdpr-info.eu/.

gran hito en el tratamiento de las cuestiones éticas relacionadas con la protección de datos personales.

La exigencia de un mayor rigor en la protección de datos establecida desde el RGPD ejerció presión en la misma línea sobre otros países, entre ellos Brasil. Así, ante tal presión internacional, Brasil promulgó la reciente y ya mencionada Ley General de Protección de Datos Personales (LGPD),[33] que exige por parte de las empresas una nueva visión sobre cómo vienen almacenando y procesando los datos personales que recopilan. De esta forma, la Ley n° 13.709/2018 impuso la identificación y restricción de acceso a los datos personales, estén o no configurados estratégicamente como secretos empresariales, además de conciliar dicha protección con el respeto a la privacidad y a los principios éticos como la transparencia.

Según el artículo 2, inciso II, de la LGPD, se expone el fundamento de la autodeterminación informativa en la disciplina de protección de datos y, de forma complementaria, su artículo 6, inciso VI, reclama atención al principio de transparencia a través de la *"garantía, a los titulares, de informaciones claras, veraces y de fácil acceso sobre la ejecución del tratamiento (de datos) y los respectivos agentes de tratamiento, observando los secretos comercial e industrial"*.[34]

Si, por un lado, la llegada de la LGPD impone a las empresas la necesidad de establecer prácticas seguras para el tratamiento de los datos desde sus activos intangibles, la implementación de una gestión eficiente y segura de estos datos puede otorgar a estas empresas una mayor protección para datos que puedan clasificarse como secreto empresarial.

La filtración de datos personales contenidos en bases de datos corporativas, tales como los casos ya enumerados, además de causar daños graves al usuario, genera perjuicios económicas directos e

33 Véase el texto de la ley en edición en internet: https://gdpr-info.eu/.

34 Ver: texto de la ley en edición en internet: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

indirectos a la empresa detentora de la información, posibilitando su uso por parte de sus competidores directos, lo cual no es un mal menor que incide incluso en la propia imagen de la empresa.

Quien quiera mantener cierta información como secreto empresarial debe limitar e identificar a las personas que tendrán acceso a ella, no solo a través de contratos de confidencialidad, por ejemplo, sino también utilizando recursos tecnológicos, a saber: contraseñas de acceso, cifrado, entre otros. Esto se debe al hecho de que, al volverse pública o accesible, la información deja de ser clasificada como secreto empresarial, perdiendo, por ende, la posible protección legal que le pueda ser atribuida.

Conclusión

El presente trabajo abordó la protección jurídica que otorga la Propiedad Industrial a los datos de naturaleza privada que aparecen dentro de la particular figura del secreto empresarial. A partir del análisis bibliográfico, hemos presentado conceptos esenciales sobre los institutos jurídicos relacionados con el tema.

A pesar de que la legislación a nivel nacional y supranacional sobre este secreto es escasa, y el mismo instituto bastante *sui generis* dentro de la propia materia de Propiedad Intelectual, la finalidad de la protección anticompetitiva se justifica por la protección inmediata de los bienes inmateriales de toda empresa, pero la protección mediata y teleológica del consumidor y el orden económico se imponen, ante todo, como se ha propuesto asentar y priorizar el presente estudio.

En este sentido, destacamos la atención de la OMPI dada al tema, especialmente con respecto al escenario actual existente en lo que se refiere al almacenamiento, procesamiento y transferencia de datos personales en todo el mundo, cuyo cuidado se maximiza considerando la rapidez con que se transmite la información tecnológica, así como los constantes avances en esta materia.

La preocupación por el respeto a cuestiones de privacidad es fundamental y prioritaria cuando del usuario, como ser humano que es, se trata. Por otro lado, con la llegada de la LGPD, se ha vuelto aún más esencial para la supervivencia de las empresas, en un mercado altamente competitivo, identificar y restringir el acceso a los datos que quieren proteger a través del secreto empresarial.

A partir de este análisis, destacamos la importancia del tema para que las empresas nacionales puedan defenderse simultáneamente en un entorno comercial mayúsculamente tecnológico y competitivo, así como seguir los lineamientos y directrices que presenta la nueva legislación de protección de datos, implementando una política de transparencia y respeto a los consumidores, quienes representan, en definitiva, los destinatarios finales y principales de la legislación anticompetitiva.

Referencias

ASCENSÃO, J. Oliveira. *Concorrência desleal*. Lisboa: Coimbra Ed., 1994.

BADENHAUSEN, Kurt. As 100 marcas mais valiosas do mundo em 2019. *Forbes*, New York, 22 mayo 2019. Disponible en: https://forbes.com.br/listas/2019/05/as-100-marcas-mais-valiosas-do-mundo-em-2019. Consultado el: 27 set. 2020.

BEKKER, Eugene. 2020 Data Breaches: The Most Significant Breaches of the Year. *Identity Force*, [*S. l.*], 3 jan. 2020. Disponible en: https://www.identityforce.com/blog/2020-data-breaches. Acceso en: 23 sep. 2020.

BRASIL. Acuerdo sobre Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio (ADPIC). *Diário Oficial da União*: seção 1, Brasília, DF, n. 248-A, 31 dic. 1994.

BRASIL. Constitución (1988). *Constitución de la República Federativa de Brasil*. Brasília, DF .Presidência da República, 1988. Disponible en: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acceso en: 28 set. 2020.

BRASIL. Convenção de Paris para a Proteção da Propriedade Industrial. Primeira publicação, 1883. Promulgada pelo Decreto-Lei nº 75.572, de 8 de abril de 1975. [*S. l.: s. n.*], 1975. Disponible en: http://www.inpi.gov.br/legislacao-1/cup.pdf. Acceso en: 27 set. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acceso en: 28 set. 2020.

BRASIL. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. *Diário Oficial da União*: seção 1, Brasília, DF, ano134, n. 93, p. 8353-8366, 15 maio 1996. Disponible en: https://www.wipo.int/edocs/lexdocs/laws/es/br/br003es.pdf. Acceso en: 27 set. 2020.

BRASIL. Decreto no 1.355, de 30 de dezembro de 1994. Promulgo a Ata Final que Incorpora os Resultados da Rodada Uruguai de Negociações Comerciais Multilaterais do GATT. *Diário Oficial da União*: seção 1, Brasília, DF, ano 132, n. 248, p. 21394, 30 dez. 1994.

CONSEJO DE LA UNIÓN EUROPEA. *General Data Protection Regulation del 15 de diciembre de 2015. [S. l.: s. n.]*, 2015. Disponible en: https://gdpr-info.eu/. Acceso en: 28 set. 2020.

CORREIA, A. Ferrer. *Lições de Direito Comercial*. Coimbra: Lex, 1973. v. 1.

COX, Michel; ELLSWORTH, David. Managing big data for scientific visualization. *ACM Siggraph*, [*s. l.*], 1997. Disponible en: https://www.researchgate.net/publication/238704525_Managing_big_data_for_scientific_visualization. Acceso en: 23 set. 2020.

FEKETE, Elizabeth Kasznar. *O regime jurídico do segredo de indústria e comércio no direito brasileiro*. Rio de Janeiro: Forense, 2003.

FILOMENO, José Geraldo Brito e outros. *Código Brasileiro de Defesa do Consumidor comentado*. Rio de Janeiro: Forense, 2000.

GIMÉNEZ PEREIRA, Marta Carolina. *Efectos de las patentes farmacéuticas*: un análisis de propiedad intelectual. Ciudad de México: Tirant lo Blanch, 2017.

GIMÉNEZ PEREIRA, Marta Carolina. Protección de datos de prueba y su exclusividad en medicamentos y agroquímicos: la interpretación del articulo 39.3 ADPIC. *Revista Eletrônica do Curso de Direito da UFSM*, Santa Maria, v. 14, n. 1, 2019. Disponible en: https://periodicos.ufsm.br/revistadireito/article/view/32530. Acceso en: 27 set. 2020.

GURRY, Francis. Intellectual property in a data-driven world. *WIPO Magazine*, Geneva, n. 5, p. 2-7, 2019. Entrevista. Disponible en: https://www.wipo.int/export/sites/www/wipo_magazine/en/pdf/2019/wipo_pub_121_2019_05.pdf. Acceso en: 27 set. 2020.

LYON, David. Cultura da vigilância: envolvimento, exposição, e ética na modernidade digital. *In*: BRUNO, Fernanda *et al. Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018.

MENÉNDEZ, Aurélio. *La competencia desleal*. Madrid: Civilitas, 1988.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. *Declaración Universal de los Derechos Humanos*. [*S. l.: s. n.*], 1948. Disponible en: https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf. Acceso en: 28 sep. 2020.

ORGANIZACIÓN MUNDIAL DE COMERCIO. *El Acuerdo sobre los ADPIC y los instrumentos internacionales a los que hace referencia*. [*S. l.: s. n.*], [201-]. Disponible en: https://www.wto.org/spanish/tratop_s/trips_s/ta_docs_s/1_tripsandconventions_s.pdf. Acceso en: 27 sep. 2020.

WORLD INTELLECTUAL PROPERTY ORGANIZATION. *Convenio de París*. Ginebra: [*s. n.*], 2021. Disponible en: https://www.wipo.int/treaties/es/ip/paris. Acceso en: 27 sep. 2020.

WORLD INTELLECTUAL PROPERTY ORGANIZATION. *Trade secrets*. Ginebra: [*s. n.*], [202-?]. Disponible en: https://www.wipo.int/export/sites/www/sme/en/documents/pdf/ip_panorama_4_learning_points.pdf. Acceso en: 27 sep. 2020.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, Fernanda *et al. Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018.

SEGREDOS INDUSTRIAIS E COMERCIAIS: PROTEÇÃO AO AGENTE DE TRATAMENTO DE DADOS PESSOAIS TRAZIDA PELA LEI GERAL DE PROTEÇÃO DE DADOS

Maria Clara Seixas

Do sopesamento dos objetivos e fundamentos da LGPD

O aumento da profundidade e complexidade tecnológicas aplicadas aos dados pessoais ao longo dos últimos anos, combinado com a crescente conscientização e reconhecimento do direito à proteção de dados pessoais como um direito fundamental, fortaleceu a tendência a um tratamento autônomo legislativo sobre o uso dos dados pessoais.

Partindo-se da análise feita por Mayer-Schonberger[1] do cenário europeu, o início deste processo legislativo era caracterizado por regulamentações voltadas para a "concessão de autorizações para a criação desses bancos de dados e do seu controle *a posteriori* por órgãos públicos" e a disciplina do controle do uso de informações pessoais pelos Estados e Administração Públicas. Aos poucos, este processo evoluiu para regulamentações mais preocupadas com as consequências desconhecidas que o uso de determinadas tecnologias poderia trazer.

1 MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a revolution that will transform how we live, work, and think. New York: Houghton Mifflin Harcourt, 2013.

Com o reconhecimento da insuficiência deste tipo de regulamentação, especialmente por conta da dispersão dos centros de bancos de dados (o que dificultava eventuais fiscalizações e controles), surgiu um segundo tipo de regulamentação, já não mais focada no uso de dados por meio de computadores. Neste sentido, Doneda menciona a Lei Francesa de Proteção de Dados Pessoais de 1978 e a *Bundesdatenschutzgesetz*, regulamento alemão.[2]

Estas regulamentações já buscavam dar uma resposta às insatisfações da população, que percebia a utilização dos seus dados pessoais por terceiros sem poder fazer frente a este uso. São legislações, assim, que enxergavam a proteção dos dados pessoais e, consequentemente, da privacidade, como uma liberdade negativa do cidadão. Este passava a ter alguns instrumentos para conseguir se defender do uso indevido dos seus dados.

É com a terceira geração de leis focada no uso dos dados pessoais, surgida na década de 1980, que se começa a entender melhor a origem dos diversos objetivos e fundamentos da Lei nº 13.709/2018[3], a Lei Geral de Proteção de Dados (LGPD) brasileira.

A terceira geração veio com a tarefa de equilibrar os múltiplos interesses em jogo. O uso de determinados dados pessoais da população começou a ser visto como requisito para a participação na vida social. A restrição ao uso de dados pessoais, tanto no âmbito da iniciativa privada quanto do setor público, poderia significar uma exclusão de parte da vida social do indivíduo.

> A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e considera o contexto no qual lhe é solicitado que

2 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law*, Joaçaba, v. 12, n. 2, p. 91-108, 2011. p. 96.

3 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

> revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes – proporcionando o efetivo.[4]

O conceito da autodeterminação informativa começa a ser disseminado e melhor compreendido, no famoso julgado do Tribunal Constitucional alemão sobre o recenseamento geral da população, em 1983. Este conceito significava um direito do cidadão que ia além do controle sobre a coleta ou não do seu dado. Todo uso e tratamento dos seus dados deveria poder ser controlado, devendo os casos de restrição ocorrer apenas quando da existência de interesse público maior.[5]

A prática, contudo, mostrou que o mero reconhecimento do direito sobre o controle do tratamento das suas informações era insuficiente e que a "autodeterminação informativa era, porém, o privilégio de uma minoria que decidia enfrentar os custos econômicos e sociais do exercício dessas prerrogativas".[6]

A quarta geração buscou assim uma regulamentação que oferecesse instrumentos para um controle e exercício destes direitos individuais de forma mais ampla e coletiva. O desequilíbrio entre a posição do titular do dado e as instituições que tratam os seus dados passou a ser questão crítica que merecia atenção e solução.[7] Mas tudo isso não ocorreu sem que existisse forte *lobby* por parte de quem tinha interesse na exploração e uso de dados pessoais.[8]

4 DONEDA, *op. cit.*, p. 97.

5 LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2011. p. 70.

6 DONEDA, *op. cit.*, p. 98.

7 A LGPD é sem dúvidas uma legislação que apresenta as características desta quarta geração, o que inclui a previsão de uma Autoridade Nacional de Proteção de Dados e a opção do legislador por categorias de dados que exigem maior proteção.

8 ATIKCAN, Ece Özlem; CHALMERS, Adam William. Choosing lobbying sides: The General Data Protection Regulation of the European Union. *Journal of Public Policy*, [s. *l.*], v. 39, n. 4, p. 543-564, 2019.

Com toda esta evolução e os constantes jogos de interesses, a LGPD surge com objetivos e fundamentos plurais, não apenas direcionado à proteção dos direitos fundamentais de liberdade e de privacidade, o livre desenvolvimento da personalidade da pessoa natural e a autodeterminação informativa, como também possui como fundamento outros interesses além do individual do titular ou da coletividade dos titulares.

É assim que o seu art. 2º trata também da liberdade de expressão, de informação, de comunicação e de opinião, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa e a livre concorrência.

A lei brasileira apresenta, desta forma, em diversos artigos, possibilidades de ponderação entre os interesses em jogo. Já em outros casos, a LGPD desde já apresenta de forma objetiva opções feitas pelo legislador – que ora privilegiam os direitos e a proteção à privacidade dos titulares, ora privilegiam interesses sociais ou individuais dos agentes[9] de tratamento de dados. O aspecto racional e o rigor técnico destas opções, contudo, não estão isentos de dúvidas, inseguranças jurídicas e questionamentos.

Este é o caso das constantes relativizações de direitos e princípios em razão dos termos "observados", "pela observância" e "respeitados" os "segredos industriais e comerciais", que aparecem em treze diferentes momentos na LGPD.

A título de exemplo, o princípio da transparência, que estabelece a garantia de informações claras, precisas e acessíveis aos titulares, bem como o consequente direito de acesso à informação sobre a forma e duração do tratamento dos seus dados, devem ser vistos com a observância dos segredos comercial e industrial.

De igual maneira, quando da solicitação pela Autoridade Nacional de Proteção de Dados (ANPD), o relatório de impacto à proteção de dados pessoais (documento que contém os processos de tratamento

9 Entende-se por "agente de tratamento de dados" a pessoa natural ou jurídica que desempenha o papel de controlador ou operador nos termos do art. 5° da LGPD.

e as garantias de segurança das informações e mecanismos de mitigação de riscos), também tem como garantia do controlador do dado a observância dos seus segredos comercial e industrial.

Conforme será discutido mais adiante, não se questiona aqui "se" os segredos comerciais e industriais são direitos que mereçam proteção e atenção do legislador, mas sim a opção pelo "como". O que se busca debater são as decisões legislativas sobre a forma *como* deve ser esta proteção e em detrimento do quê.

Parte-se da premissa de que para a efetividade desta lei, os mecanismos de transparência e até mesmo de *accountability* devem ser sempre exigidos dos agentes de tratamento de dados pessoais na máxima medida do possível. O que não parece ter sido o direcionamento do legislador pátrio em muitos momentos.

A data driven economy e os segredos industriais e comerciais

A transformação digital criou um novo tipo de economia que recai sobre os dados agregados. Com uma miríade de rotinas diárias conectadas direta ou indiretamente à máquinas, a coleta de dados pessoais se tornou onipresente – com computadores, *smartphones*, circuitos de vigilância, mecanismos de IoT, com sensores e *chips* em equipamentos inteligentes etc. –, criando um fenômeno de "datificação" de todos os aspectos da vida humana social, política e econômica.

O uso dos dados pessoais como insumo

Esta construção foi em grande parte criada pelas "*big techs*",[10] que atuaram e se desenvolveram em um território sem qualquer tipo de

10 Este termo costuma ser utilizado em referência a grandes empresas de tecnologia como o Google, a Amazon, o Facebook e a Apple.

regulamentação mais efetiva – em grande parte pelas oportunidades trazidas pelo desconhecimento do potencial e consequências deste novo modelo de economia:

> as principais empresas de tecnologia foram respeitadas e tratadas como emissários do futuro; nada na experiência passada havia preparado as pessoas para essas novas práticas, havendo, portanto, escassez de barreiras para que se protegessem; os indivíduos passaram rapidamente a depender das novas ferramentas de informação e comunicação como recursos necessários na luta cada vez mais estressante, competitiva e estratificada para uma vida mais eficaz; as novas ferramentas, redes, aplicativos, plataformas e mídias tornaram-se requisito para a participação social.[11]

Neste cenário, as "*big techs*", como o Google, a Amazon, o Facebook e a Apple, aparecem sempre com destaque pela nova lógica de acumulação de dados pessoais que ajudaram a criar. Mas o fenômeno da economia movida a dados já se tornou muito maior do que algo focado em um pequeno grupo de empresas ou até mesmo focado no setor privado.

O insumo desta nova economia costuma ser processado por meio de algoritmos – uma sequência de instruções que são dadas para resolver um determinado problema – e estes trazem algumas dificuldades quando se trata não apenas da compreensão dos seus comandos, quanto da previsão dos seus resultados.

Desde já, é intuitivo perceber que a opacidade dos algoritmos é antagônica ao princípio da transparência e, consequentemente, da autodeterminação informativa quando se trata de proteção ao uso dos dados pessoais.

A assimetria de conhecimento entre as instituições que desenvolvem tecnologias e estratégias para transformar os dados pessoais em

11 BRUNO, Fernanda *et al*. *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018. p. 58.

informações economicamente úteis é patente. E, individualmente, é impossível que exista um controle do titular dos dados sobre a destinação das suas informações com os poucos recursos atualmente disponíveis.

Pensando nos algoritmos que utilizam como insumo banco de dados pessoais, em diversos contextos, é difícil que a própria instituição que o criou avalie todo o seu potencial danoso, considerando que existem correlações diversas e elementos novos que desviam os resultados. Para terceiros, então, sem a expertise técnica ou a abertura completa sobre a estrutura do algoritmo e da origem do seu insumo, a tarefa se torna quase impossível.

Neste sentido, Frazão traz a percepção de Cathy O'Neil que se refere:

> aos algoritmos como armas matemáticas de destruição, na medida em que, longe de serem neutros e objetivos, embutem em seus códigos uma série de decisões e opiniões que não podem ser contestadas, até porque não são conhecidas. Daí o seu potencial de destruição silenciosa, na medida em que podem basear seus julgamentos em preconceitos e padrões passados que automatizam o status quo e ainda podem ser utilizados para toda sorte de discriminações e violações de direitos.[12]

Analisando este mesmo momento histórico, Pasquale, entende que vive-se em uma "*Black Box Society*" e que diversos algoritmos controlam aspectos cotidianos da população de forma obscura, sem permitir o entendimento e auditorias sobre o seu funcionamento e suas consequências.[13]

Não obstante, a discussão fica ainda mais complexa quando se adiciona na cadeira direitos de proteção ao segredo industrial e comercial

12 FRAZÃO, Ana. Data-driven economy e seus impactos sobre os direitos de personalidade. *Jota*, [*s. l.*], 17 jul. 2018.

13 PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

presentes não apenas nas regulamentações voltadas ao uso dos dados pessoais, mas também em outros instrumentos legais focados na proteção à empresa. Percebe-se com clareza a existência de duas diferentes forças: a da proteção aos segredos dos agentes de tratamento de dados e a proteção ao seu titular ou até mesmo a toda a sociedade em última instância.

Os segredos industriais e comerciais

Pode-se dizer que a proteção ao segredo industrial e comercial nasceu das normas de proteção à propriedade intelectual. Este tipo de preocupação em oferecimento de uma proteção legal tem origem com a Revolução Industrial, por meio da qual a produção artesanal cedeu lugar a uma produção industrial e a sociedade começou a perceber que o "como fazer" tinha valor passível de monetização, valor econômico real. A proteção por meio de leis e regulamentos nacionais passou a ser uma demanda concreta.

Este movimento trouxe também consigo o incremento no comércio internacional e, assim, começaram a surgir convenções internacionais – como a Convenção de Paris de 1883 – tratando da proteção à propriedade industrial principalmente com o foco em uniformizar e eventualmente trazer normas para países nos quais não havia regulamentação sobre o tema.[14] Referida Convenção resultou, posteriormente, juntamente com a Convenção da União de Berna, no *Trade Related Aspects of Intellectual Property Right* (TRIPS).

14 A regulamentação teve por "objeto as patentes de invenção, os modelos de utilidade, os desenhos ou modelos industriais, as marcas de fábrica ou de comércio, as marcas de serviço, o nome comercial e as indicações de proveniência ou denominações de origem, bem como a repressão da concorrência desleal". Ver: http://www.direitoshumanos.usp.br/index.php/WIPO-World-Intellectual-Property-Organization-Organiza%C3%A7%C3%A3o-Mundial-de-Propriedade-Intelectual/convencao-de-paris-para-a-proteccao-da-propriedade-industrial.html.

Os TRIPS tiveram como "escopo garantir às empresas, a recuperação de investimentos na pesquisa e desenvolvimento tecnológico, ao determinar a exclusividade de comercialização de um produto ou serviço".[15]

Também no Brasil as normas sobre concorrência desleal estiveram ligadas desde o início à proteção ao segredo industrial, como o Decreto nº 24.507/1934[16]. Foi assim estabelecido que o ato de "desvendar a terceiros, quando em serviço de outrem segredos de fábrica ou de negócio conhecidos, em razão do officio" constituía ato de concorrência desleal. Na mesma linha segue o Decreto n° 7.903/1945.[17]

Quanto ao conceito do que seria um segredo industrial ou comercial, os referidos regulamentos, bem como a Lei nº 9.279/1996, atualmente em vigor regulando os direitos e obrigações relativos à propriedade industrial, não trazem uma definição. Existe, assim, construção doutrinária que estabelece quais as características deste instituto.

Na mesma linha que o TRIPS, a Lei nº 9.279/1996[18] adotou um conceito mais amplo de "segredo industrial", falando em "informações

15 DEL'OLMO, Florisbal de Souza; ROSADO, Olivério de Vargas; ARAUJO, Thiago Luiz Rigon. Propriedade intelectual no cenário internacional: organismos de proteção e o acordo trips. *Revista Eletrônica do Curso de Direito – UFSM*, Santa Maria, v. 8, p. 129-137, 2013. p. 134.

16 BRASIL. Decreto n° 24.507, de 29 de junho de 1934. Approva o regulamento para a concessão de patentes de desenho ou modelo industrial, para o registro do nome commercial e do titulo de estabelecimentos e para a repressão á concorrencia desleal, e dá outras providencias. *Diário Oficial da União*: seção 1, Brasília, DF, p. 15332, 26 jul. 1934.

17 "Art. 178. Comete crime de concorrência desleal que: XI. divulga ou explora, sem autorização, quando a serviço de outrem, segredo de fábrica, que lhe foi confiado ou de que tece conhecimento em razão do serviço; XII, divulga ou se utiliza, sem autorização, de segredo de negócio, que lhe foi confiado ou de que teve conhecimento em razão do serviço, mesmo depois de havê-lo deixado".
BRASIL. Decreto n° 7.903, de 4 de fevereiro de 2013. Estabelece a aplicação de margem de preferência em licitações realizadas no âmbito da administração pública federal para aquisição de equipamentos de tecnologia da informação e comunicação que menciona. *Diário Oficial da União*: seção 1, Brasília, DF, ano 150, n. 25, p. 7, 5 fev. 2013.

18 BRASIL. Lei n° 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. *Diário Oficial da União*: seção 1, Brasília, DF, ano 134, n. 93, p. 8353-8366, 15 maio 1996.

ou dados confidenciais", incluindo aqui os segredos utilizados na indústria, comércio ou prestação de serviços.

Para que se possa estar diante de um segredo industrial ou comercial, é estabelecido como requisito que se trate de uma informação evidentemente secreta, que não tenha sido, portanto, objeto de divulgação. Tal confidencialidade, contudo, não significa que apenas uma determinada quantidade de pessoas possa ter acesso ou que nenhum terceiro pode ter tido acesso, mas sim que a informação não é de conhecimento público.

Ademais, segundo Fekete, a confidencialidade deve ter sido protegida por meio da adoção de precauções razoáveis, para que seja demonstrada de forma manifesta a intenção de manter determinada informação em segredo.[19]

Soma-se a este rol de características a existência de um valor econômico, implicando em uma vantagem competitiva, a aplicabilidade no negócio, podendo ser suscetíveis de transações comerciais. A relativa novidade (aqui entendida no sentido de uma não obviedade para quem entende tecnicamente do assunto) costuma também ser elemento de análise casuística a respeito da caracterização ou não de um segredo industrial ou comercial.[20]

Neste sentido, observa-se que estes segredos não são passíveis de patenteamento ou registro – o que resultaria em uma publicização deles. Ademais, a doutrina considera que a análise da proteção ao segredo industrial e comercial deve pressupor um contexto concorrencial,[21] o que confere ao tema inclusive relevo constitucional. Os seus direitos são protegidos por prazo indeterminados, diferentemente

19 FEKETE, Elizabeth. Segredo de empresa. *Enciclopédia Jurídica da PUC-SP*, São Paulo, Edição 1, jul. 2018.

20 FEKETE, *op. cit.*

21 BARONE, Daniela. *Proteção internacional do segredo industrial*. 2009. Dissertação (Mestrado em Direito) – Universidade de São Paulo, São Paulo, 2009.
BRASIL. Lei n° 13.709, *op. cit.*

das patentes e inventos. Contudo, caso o segredo seja revelado, o seu titular estará limitado ao recurso da concorrência desleal.

Percebe-se uma amplitude e subjetividade na análise do que pode ser enquadrado como segredo comercial/industrial. Pode-se estar diante do desenvolvimento de uma tecnologia, algum processo de fabricação, o desenho de um algoritmo ou o substrato que o alimenta, um modo de atuação, algum conhecimento específico ou até mesmo uma estratégia negocial (estratégia esta que pode ter como finalidade, por exemplo, influenciar as preferências de determinado indivíduo ou até moldar a sua visão de mundo).

Certamente a inexistência de proteção ao segredo industrial e comercial seria de extrema lesividade para o desenvolvimento econômico e tecnológico do país. Contudo, conforme já mencionado, os segredos industrial e comercial foram inseridos na LGPD e se apresentam como um limite ao direito de acesso à informação e ao princípio da transparência. Isso significa, portanto, que em diversas situações, a exceção trazida aos segredos industrial e comercial pode se tornar uma verdadeira carta branca, carta esta que pode estar legitimando a lesão a um direito fundamental.

O Princípio da Transparência e o direito de acesso à informação

Parece haver uma oposição semântica dos conceitos "segredo" e "transparência". Contudo, quando se trata de uma análise destes termos dentro do universo jurídico, tais conceitos deverão ser entendidos à luz do seu específico contexto e eventuais conceituações legislativas explícitas.

Conceito e as opções do legislador

Quando nos referimos à proteção à privacidade e a proteção dos titulares quanto ao uso dos seus dados por terceiros, a transparência deve ser vista como condição *sine qua non* para a efetividade desta proteção. Conforme já mencionado, a autodeterminação informativa se tornou um instituto central e esta não existirá nos casos em que não há transparência a respeito do que é feito com o dado pessoal por determinada instituição.

O princípio da transparência é entendido pela regulamentação europeia de dados pessoais (GDPR) como a necessidade de que qualquer informação ou comunicação relativa ao processamento de dados pessoais seja acessível, de fácil compreensão e em linguagem clara e simples.

Já a LGPD conceitua no seu art. 6º, inciso VI, o princípio da transparência como a garantia que os titulares possuem de ter "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial"[22]. Percebe-se, portanto, que desde já, no seu próprio conceito, referido princípio já é relativizado pelo legislador.

Por meio de uma interpretação isolada e literal do citado dispositivo, caso um agente de tratamento de dado opte por não revelar alguma informação sobre o tratamento dos dados pessoais de algum titular, argumentando que é uma questão de segredo comercial ou industrial, ele não estaria indo de encontro ao princípio da transparência previsto na lei. Contudo, mais adiante será aprofundado o porquê uma interpretação neste sentido não deve prevalecer.

Vale observar que o *Recital 63* da regulamentação europeia de proteção de dados,[23] ao analisar a ponderação entre os interesses dos

22 BRASIL. Lei nº 13.709, *op. cit.*

23 "A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. [...] Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where

titulares e dos agentes, dispôs que o titular tem o direito de verificar a legalidade do processo de tratamento dos seus dados e de verificar a lógica envolvida no tratamento automatizado dos seus dados e a consequência de tais processamentos.

A orientação segue explicando que este direito dos titulares não deve afetar negativamente os "*trade secrets or intellectual property and in particular the copyright protecting the software*", mas que estes não devem servir como recusa ao acesso à informação.

A LGPD possui ainda diversos artigos cujo objetivo parece ser o de concretizar o mencionado princípio. É assim que de acordo com o art. 9º, é direito do titular ter acesso facilitado às informações sobre o tratamento de seus dados (atendendo ao princípio do livre acesso), o que inclui informações sobre a finalidade, compartilhamento, forma e duração (estes dois últimos relativizados também pela expressão "observador os segredos comercial e industrial")[24]. O art. 9º ainda acrescenta que nos casos em que o consentimento é utilizado como base para o tratamento dos dados, este será nulo caso as informações "não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca"[25].

Ao mesmo tempo em que diversas disposições da LGPD trazem a proteção da transparência e o acesso à informação dos titulares dos dados, bem como criam mecanismos de exercício direto dos seus direitos, quando se trata da proteção aos segredos industriais e comerciais, os direitos dos titulares são deixados de lado, preteridos.

possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject". Ver em: https://www.privacy-regulation.eu/en/recital-63-GDPR.htm.

24 BRASIL. Lei n° 13.709, *op. cit*.

25 *Ibidem*.

Por evidente, considerando todo o sistema legislativo pátrio, e até mesmo as normas internacionais, haveria uma incompatibilidade caso os titulares pudessem exercer de forma direta a sobreposição do seu direito de transparência e autodeterminação informativa em detrimento dos segredos industriais e comerciais dos agentes de tratamento. É inquestionável o impacto negativo dessas situações, pois este poder acabaria por aniquilar legítimos interesses da iniciativa privada. A publicização de um segredo industrial ou comercial descaracterizaria a sua própria natureza.

Mas o que se percebe é que não apenas aos titulares não foi dado referido poder (sendo coerente não obrigar a ampla divulgação do segredo, e sua consequente descaracterização), mas igualmente os órgãos de fiscalização e controle quedaram-se sem ferramentas aptas a verificar nas situações concretas o interesse que deveria prevalecer e a possibilidade de compatibilização entre os diferentes interesses.

Ressalta-se, mais uma vez, que a existência de um segredo industrial ou comercial não significa o seu desconhecimento absoluto por terceiros, na medida em que o compartilhamento pode ocorrer de forma controlada e segura.

Neste sentido, os arts. 10º e 38º da LGPD[26] estabelecem que a ANPD poderá solicitar o relatório de impacto à proteção de dados pessoais, mas que deverão ser observados os segredos comercial e industrial. Diante da ausência de maiores esclarecimentos da própria lei, bem como de pronunciamento da ANPD, será que isso significa que as empresas poderão omitir dos seus relatórios entregues à ANPD informações importantes sobre o tratamento realizado com os dados mas que possam se enquadrar sob a rubrica de "segredos comerciais ou industriais"? A princípio, por uma interpretação literal, é possível que se defenda que sim.

Na mesma linha, o art. 55-J, ao tratar das competências da ANPD, dispõe que cabe a ela "zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das

26 BRASIL. Lei nº 13.709, *op. cit.*

informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º"[27] da LPGD.

Estes segredos (ou a alegação da existência destes segredos) serviriam como um escudo impedindo que o titular e a ANPD tivessem transparência ou conhecimento real sobre o tratamento realizado com os seus dados.

O único dispositivo que parece ter seguido por uma ponderação diferente foi o art. 20º, que trata do direito de revisão de decisões tomadas unicamente a partir de algum tratamento automatizado de dados pessoais. Isso ocorre pois apesar de seu §1º também relativizar o princípio da transparência e o direito de acesso à informação em razão dos segredos industriais e comerciais, o §2º dispõe que:

> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.[28]

Aqui, portanto, resta claro que diante de situações em que se possa estar diante de aspectos discriminatórios e se tratar de um tratamento automatizado, a ANPD poderá intervir e fiscalizar para verificar a conduta do agente. Não obstante, conforme será analisado mais adiante, este dispositivo parece ser insuficiente.

A insuficiência da proteção exclusiva aos aspectos discriminatórios em tratamento automatizado de dados pessoais

Sem dúvidas uma das grandes preocupações atuais relativas ao uso de dados pessoais está centrada nos riscos relativos às decisões

27 BRASIL. Lei nº 13.709, *op. cit.*

28 *Ibidem*.

automatizadas. Sabe-se que as decisões automatizadas, ao contrário do que muitos defendem, não são necessariamente objetivas e imparciais. Tornou-se falaciosa a crença de que as decisões tomadas com base no uso da inteligência artificial são sempre objetivas e "melhores" que as tomadas diretamente pelos seres humanos portadores de subjetividades.

As decisões tomadas por algoritmos – ou seja, sem o julgamento direto do homem – podem conter diversos vieses e desvios realizados por preconceitos – na programação ou na construção do que irá o alimentar. Não apenas os vieses cognitivos humanos são capazes de serem injustos e discriminatórios, mas também os vieses algorítmicos.

Já se tornou uma realidade o uso de algoritmos em processos seletivos de empresas, para a realização de diagnósticos médicos, classificação de pessoas, julgamentos criminais etc. Estes podem ser utilizados com o objetivo de se identificar determinado padrão comportamental, orientação sexual, opinião política, emoções, doenças, entre outros.

Os vieses algoritmos podem, assim, estar presentes em todos estes diferentes processos. Tudo isso cria mais atividades de risco para as liberdades e para os direitos individuais dos titulares objeto destes tratamentos. E os riscos vão muito além da mera e direta violação da privacidade. Muitas destas decisões automatizadas significam o acesso ou não a determinadas oportunidades de serviço, empregos, seguros, crédito etc., impactando na própria experiência e expressão humanas.

Isso sem aprofundarmos na discussão sobre o uso dos dados para fins de manipulação e controle dos indivíduos, inclusive com o foco de influenciar a consciência individual e coletiva.[29]

> Vista a questão por esse ângulo, a tecnologia pode estar sendo utilizada contra aquilo que temos de mais precioso: a nossa individualidade. A partir do momento em que as máquinas conseguem nos conhecer melhor do que nós mesmos, podem utilizar nossas

29 WU, Tim. *The attention merchants*: the epic scramble to get insideour heads. New York: Knopf, 2016.

> fragilidades para manipular nossas emoções, crenças e opiniões para os mais diversos fins, inclusive políticos. Aliás, as eleições de Donald Trump e do Brexit ilustram bem tal preocupação.[30]

É indiscutível, assim, que as decisões automatizadas podem resultar em muitas violações aos direitos e liberdades fundamentais, sendo o tratamento discriminatório apenas uma delas. Nem todo tratamento de dados indevido terá como pano de fundo uma ação ou omissão que dispense de forma direta um tratamento diferenciado/inferiorizado em razão de uma característica do seu titular, resultando em uma discriminação em sentido estrito.

Tudo isso já mostra uma insuficiência da exceção trazida pela LGPD ao permitir à ANPD apenas realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. Ou seja, apenas nestes casos, quando o argumento para a não transparência for o segredo industrial ou comercial e houver suspeita de um tratamento automatizado discriminatório, é que a lei já dispõe sobre a possibilidade de verificação da ocorrência ou não da lesão ao titular do dado pessoal.

Ademais, não são apenas as decisões automatizadas que podem utilizar dados pessoais de forma ilegal e contrária à LGPD. O segredo industrial ou comercial não deveria ser excepcionado e passível de auditoria por parte da ANPD apenas quando diante de decisões automatizadas. Um processo seletivo pode se utilizar de uma estratégia na análise dos dados dos candidatos sem o uso de qualquer tecnologia de decisão feita por algoritmo e o resultado da estratégia ser a lesão a um direito.

Sem a possibilidade de verificação ampla por parte da ANPD dos tratamentos feitos pelos agentes – sejam eles automatizados ou não e havendo ou não a suspeita de uma discriminação –, o argumento de um segredo industrial ou comercial se torna um coringa nas mãos

30 FRAZÃO, *op. cit.*

de quem não quer dar transparência sobre a sua atividade alimentada por dados pessoais.

O legislador pátrio privilegiou, assim, apenas o princípio da não discriminação em detrimento do segredo industrial e comercial e ainda parece ter restringido aos casos de decisão automatizada.

Conclusão

A balança entre os diferentes direitos e interesses dos atores sociais nunca é tarefa fácil para um regulador. Igualmente não se espera de um texto legislativo, mesmo após a edição de regulamentações e consolidação de interpretações, que todas as respostas a inúmeras situações concretas já estejam previstas. Não obstante, não é excessivo nem desarrazoado esperar que ao menos os mecanismos de controle a *accountability* estejam previamente definidos.

A não existência de normas objetivas, disciplinando o princípio da responsabilização e prestação de contas[31] quando se trata de proteção ao segredo industrial ou comercial, e a expressa exceção em apenas uma situação, abrem o risco interpretativo de que é objetivo do legislador priorizar estes em detrimento da comprovação da observância do cumprimento da LGPD em todas as demais hipóteses não contempladas pelo art. 20º.[32]

Este tipo de interpretação poderia pôr em risco em grande medida a efetividade da proteção ao cidadão, titular do dado, bem como criaria uma "ditadura" dos algoritmos com reflexos negativos nos âmbitos concorrencial, econômico e social. Como seria possível verificar o respeito aos direitos e liberdades fundamentais sem que ao menos

31 Art. 6, inciso X da LGPD: "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".
BRASIL. Lei nº 13.709, *op. cit.*

32 *Ibidem*.

se tenha a possibilidade de solicitar a uma autoridade que conheça as correlações e tratamentos feitos com os dados? Como será possível contestar determinado tratamento sem qualquer possibilidade de verificação de que realmente se trata de um segredo industrial e comercial (ou apenas algum segredo, até mesmo ilegal) o motivo pelo qual o agente não está revelando o que é feito com os dados coletados?

É papel da ANPD o de fiscalizar e controlar como é feito o tratamento dos dados pessoais, bem como é dever de quem trata os dados comprovar que as suas ações são feitas dentro dos limites legais estabelecidos pela LGPD. Assim, a interpretação que parece ser a mais coerente com todo o sistema de normas relativas ao tratamento dos dados pessoais é a de que os poderes de fiscalização da ANDP, mesmo diante de possíveis segredos comerciais e industriais, devem ser amplos, e não restritos ao caso de decisões automatizadas com possíveis tratamentos discriminatórios.

Assim, os segredos comerciais e industriais não devem ser vistos como carta branca para a omissão de informações e especificações sobre os tratamentos dos dados, mas tão apenas como fatores que trazem necessidades procedimentais distintas. Ou seja, diante de tratamentos envolvendo segredos comerciais e industriais, os titulares poderão eventualmente não ter o mesmo grau de transparência direta e a verificação da conformidade do tratamento com a lei ficará, em parte, nas mãos de uma autoridade específica, mas de nenhuma maneira a sua proteção deverá ser reduzida ou fragilizada em razão destes institutos.

Referências

ATIKCAN, Ece Özlem; CHALMERS, Adam William. Choosing lobbying sides: The General Data Protection Regulation of the European Union. *Journal of Public Policy*, [*s. l.*], v. 39, n. 4, p. 543-564, 2019.

BARONE, Daniela. *Proteção internacional do segredo industrial*. 2009. Dissertação (Mestrado em Direito) – Universidade de São Paulo, São Paulo, 2009. Disponível em: https://teses.usp.br/teses/disponiveis/2/2135/tde-19112009-133733/pt-br.php. Acesso em: 10 nov. 2020.

BRUNO, Fernanda *et al. Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018.

DEL'OLMO, Florisbal de Souza; ROSADO, Olivério de Vargas; ARAUJO, Thiago Luiz Rigon. Propriedade intelectual no cenário internacional: organismos de proteção e o acordo trips. *Revista Eletrônica do Curso de Direito – UFSM*, Santa Maria, v. 8, p. 129-137, 2013. Disponível em: https://periodicos.ufsm.br/index.php/revistadireito/article/view/8254. Acesso em: 10 nov. 2020.

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

FEKETE, Elizabeth. Segredo de empresa. *Enciclopédia Jurídica da PUC-SP*, São Paulo, 2018. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/248/edicao-1/segredo-de-empresa. Acesso em: 10 nov. 2020.

FRAZÃO, Ana. Data-driven economy e seus impactos sobre os direitos de personalidade. *Jota*, [*s. l.*], 17 jul. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/data-driven-economy-e-seus-impactos-sobre-os-direitos-de-personalidade-18072018. Acesso em: 15 nov. 2020.

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

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a revolution that will transform how we live, work, and think. New York: Houghton Mifflin Harcourt, 2013.

PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

WU, Tim. *The attention merchants*: the epic scramble to get inside our heads. New York: Knopf, 2016.

SEGREDOS DE EMPRESA, PROPRIEDADE INTELECTUAL E A PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

Wendel Machado de Souza

Introdução

A propriedade intelectual, em todas as suas gamas de proteção e alcance, tem se tornado um tema de recorrente interesse, especialmente pela aceleração do desenvolvimento tecnológico e de difusão da informação vivenciadas no contexto da sociedade da informação.

De outro modo não poderia ser, pois desenvolvimento tecnológico, inovação e propriedade intelectual guardam entre si uma verdadeira dinâmica de impulsionamento mútuo. A propriedade intelectual cumpre, então, dentre outros aspectos, com a função de ao mesmo tempo garantir os direitos, mas também, do ponto de vista econômico, fomentar as criações do intelecto humano que podem gerar valor para a sociedade.

No contexto da sociedade da informação, vivenciamos a interconexão através das redes, possibilitada pelo desenvolvimento das tecnologias da informação e comunicação, mormente por meio da internet. Também em tais circunstâncias é que novos negócios surgiram e foram impulsionados, voltando-se para o campo dos modelos baseados em dados, utilizando ferramentas como *big data*, *data science* e *analytics*.

Tais transformações nos paradigmas do mercado e da tecnologia, influenciaram no desenvolvimento da área de Proteção de Dados Pessoais, inicialmente como derivativa da privacidade e agora já alçada ao *status* de ramo autônomo do Direito. Este movimento tem gerado nas últimas décadas uma prolífica produção de legislações em mais de 120 países do mundo que versam sobre a Proteção de Dados Pessoais.

A este movimento aderiu o Brasil, que em 2018 publicou a Lei nº 13.709/2018[1], denominada Lei Geral de Proteção de Dados Pessoais (LGPD), a qual teve como forte inspiração o Regulamento Geral de Proteção de Dados (GDPR) publicado em 2016 pelo Parlamento da União Europeia.

Apesar da grande relevância da LGPD como marco regulatório em diversos aspectos, necessário lembrar que tal legislação se insere num complexo ordenamento jurídico e com ele interage de maneira dinâmica, exigindo assim uma visão integradora dos operadores do direito para a sua correta interpretação e aplicação.

Isso se torna ainda mais perceptível quando observamos o texto da LGPD, que é crivado por diversas referências a elementos normativos abertos que necessitam da integração com outras normas e ramos do direito para a sua aplicação plena. Entre esses pontos de interseção encontra-se a disciplina dos segredos comerciais e industriais, que por diversas vezes são referenciados na LGPD. Entretanto, não há definição legal na LGPD do conteúdo da expressão "segredos comerciais e industriais", de modo que se faz necessário recorrer ao estudo da Propriedade Intelectual para a correta conceituação e interpretação.

Deste modo, o presente trabalho busca analisar os institutos dos segredos de empresa, sua relação e posição referente à propriedade

1 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

industrial e ao direito concorrencial, bem como estes se inserem no contexto da Proteção de Dados Pessoais no ordenamento jurídico brasileiro por meio da LGPD.

Segredos de empresa e propriedade intelectual

A propriedade intelectual, em sua conceituação, guarda relação direta com as criações que sejam frutos do intelecto humano e que gozam de características de novidade e inventividade, às quais o Estado oferece proteção por determinado período, de modo que o seu criador neste lapso temporal obtém o monopólio do direito de explorar com exclusividade a sua criação e os seus frutos.[2]

Pode-se compreender a propriedade intelectual como um gênero do qual fazem parte algumas espécies, consideradas de acordo com as categorias dos objetos que se pretende proteger, das quais se extrai os seguintes ramos: 1. direito do autor e conexos; 2. propriedade industrial; e 3. direitos *sui generis*, como as indicações geográficas, as topografias de circuito integrado, base de dados, cultivares e conhecimentos tradicionais.

Por outro lado, temas como a concorrência desleal e os segredos de empresa se encontram também afetos aos debates relacionados à propriedade intelectual, ainda que não haja unanimidade em concebê-los, ou não, como ativos próprios.

A partir[3] do ponto de vista internacional, a propriedade intelectual e a concorrência desleal figuram com forte conexão, especialmente quando considerado que protegem, em suma, os mesmos valores. Contudo, o fazem de maneira autônoma e complementar, haja vista

2 GIMÉNEZ PEREIRA, Marta. *Efectos de la protección de las patentes farmacéuticas*: un análisis de propiedad intelectual. Ciudad de México: Tirant Lo Blanch, 2017.

3 VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual*. 2. ed. São Paulo: Almedina, 2020.

que a proteção contra a concorrência desleal pode oferecer tutela a bens imateriais que não sejam objeto de propriedade intelectual, bem como que a prática de concorrência desleal pode ser motivo para o não reconhecimento da propriedade intelectual, sem que haja identidade entre as disciplinas conquanto a propriedade intelectual atribui direitos de exclusividade aos titulares e a concorrência desleal prescreve determinadas condutas.

Neste mesmo sentido é o entendimento de Amorim, que, em análise a partir da legislação portuguesa, afirma *in verbis*:

> A propriedade industrial abrange os sinais distintivos do comércio e as criações intelectuais de aplicação industrial, atribuindo ao titular um direito de utilização exclusiva, que corresponde a um monopólio de exploração económica. Os direitos privativos configuram-se, por isso, sobretudo como direitos de exclusão com carácter taxativo, ficando dependentes de concessão ou registo junto do INPI. Já a disciplina da concorrência desleal incide sobre os meios utilizados no exercício de uma atividade económica, de acordo com um juízo valorativo realizado à luz da contrariedade às normas e usos honestos [...]. Ou seja, a proteção conferida por ambos os regimes jurídicos é qualitativamente diversa.[4]

Embora essa aparente ser a posição majoritária e uma distinção mais pacífica, há autores que adotam uma postura mais unificadora. Parra Satizábal[5] entende que em vários cenários a propriedade intelectual e a concorrência desleal interagem em relação aos bens intangíveis que protegem, seja de maneira conjunta ou contrária, especialmente

4 AMORIM, Ana Clara Azevedo de. O regime jurídico dos segredos comerciais no novo Código da Propriedade Industrial. *Revista Electrónica de Direito*, Porto, v. 19, n. 2, p. 12-41, 2019. p. 15.

5 PARRA SATIZÁBAL, Carlos Alberto. Relación entre propiedad intelectual y derecho de la competencia: mucho más que asuntos de competencia desleal. *Revista La Propiedad Inmaterial*, Bogotá, n. 5, p. 17-36, 2002.

porque tais bens imateriais são protegidos direta ou indiretamente pela propriedade intelectual e constituem instrumentos para competir.

Em outro caminho menos pacífico, entretanto, é a posição do segredo empresarial, ora considerado autônomo, ora sujeito à propriedade intelectual ou à proteção concorrencial. Isso se dá porque há diversos entendimentos doutrinários acerca dos segredos industriais e por uma ampla abertura interpretativa das normas, tanto de direito internacional quanto das legislações internas de diversos países.

Contudo, antes categorizar os segredos industriais, faz-se necessário entender o seu conteúdo conceitual e seu enquadramento normativo no âmbito internacional e na legislação brasileira.

Segundo Rossi, "segredos empresariais incluem qualquer informação protegida — técnica, financeira ou estratégica — que não seja geralmente conhecida e que proporcione uma vantagem competitiva para o proprietário". Tal conceito expressa duas características do segredo de negócio: ser sigiloso e oferecer uma vantagem competitiva.

A definição normativa de segredo industrial, no cenário internacional, deriva da Convenção de Paris de 1967, que foi agregada sob o *Trade-Related Aspects of Intellectual Property Law* – o Acordo TRIPS (ou Acordo ADPIC) – de 1994. Tem-se enfoque sobre o art. 39 do Acordo TRIPS,[6] que lista os seguintes requisitos:

> Pessoas físicas e jurídicas terão a possibilidade de evitar que informação legalmente sob seu controle seja divulgada, adquirida ou usada por terceiros, sem seu consentimento, de maneira contrária a práticas comerciais honestas, desde que tal informação: (a) seja secreta, no sentido de que não seja conhecida em geral nem facilmente acessível a pessoas de círculos que normalmente lidam com o tipo de informação em questão, seja como um todo, seja na configuração e montagem específicas de seus componentes; (b)

6 ORGANIZAÇÃO MUNDIAL DO COMÉRCIO. *Acordo sobre aspectos dos direitos de propriedade intelectual relacionados ao comércio*. Marrakech: OMC, 1994.

> tenha valor comercial por ser secreta; e (c) tenha sido objeto de precauções razoáveis, nas circunstâncias, pela pessoa legalmente em controle da informação, para mantê-la secreta.[7]

De tal regulamento podemos derivar o entendimento de que para que se considere como segredo empresarial, três requisitos devem ser satisfeitos, quais sejam: 1. sigilo, de modo que a informação não faça parte do estado da arte ou da técnica ou que não seja facilmente identificável por pessoa com conhecimentos técnicos; 2. o caráter econômico vinculado ao segredo, haja vista que essa é a principal razão para a existência de um segredo comercial; 3. que haja um controle de acesso, pois, até por consectário lógico, não se trata de segredo aquilo que não se encontra guardado de maneira cuidadosa para que não se revele a público.

O art. 39 do TRIPS marca um importante lugar do segredo industrial, dando maior relevância à sua proteção. Contudo, o texto do acordo em relação a este tema tem caráter mais diretivo do que pragmático, haja vista indicar a necessidade de os países membros realizarem a proteção do segredo de negócio, porém, não traz em seu bojo determinações sobre a instrumentalização dessa proteção, diferentemente do que faz com outras figuras da propriedade intelectual, como as patentes.

Gize-se que o texto do referido artigo faz referência direta à ideia de concorrência desleal, podendo-se inferir a relação entre a proteção ao segredo de negócio também como uma proteção contra a concorrência desleal. De outra via, entretanto, a referência à concorrência desleal e ao segredo industrial está situada na Parte II do Acordo, que trata sobre "normas relativas à existência, abrangência e exercício dos direitos de propriedade intelectual", listada em conjunto com os direitos autorais e conexos, desenhos industriais, patentes etc. Deste modo se torna também

7 ROSSI, Juliano Scherner. Elementos de gestão de segredos empresariais para a inovação. *Revista Thesis Juris*, São Paulo, v. 7, n. 1, p. 25-50, 2018. p. 27.

possível a inteligência de que, ao menos no tocante à sistemática advinda do TRIPS, o segredo de negócio tangencia a Propriedade Intelectual.

Sob a perspectiva do direito dos Estados Unidos, os segredos de negócio, denominados como *Trade Secrets*, encontram principal regulação no *Defend Trade Secrets Act* (DTSA) de 2016, que possibilitou a jurisdição federal para apreciar os atos de apropriação e uso irregular dos segredos empresariais. Observando a partir do direito americano, fica claro que os segredos de negócio fazem parte do conteúdo de propriedade intelectual, que goza de proteção contra apropriação.

O entendimento de segredos de negócio como propriedade intelectual, embora tenha sido reforçado recentemente, já anteriormente encontrava amparo no direito americano, haja vista o *Uniform Trade Secret Act* (UTSA) de 1985, que influenciou a Rodada do Uruguai no Acordo TRIPS. Assim, no direito americano,[8] os segredos empresariais fazem parte da propriedade intelectual, se acercando ao direito do autor e das patentes, porém apresentando alguns aspectos problemáticos, pois, apesar de específico, a sua oponibilidade pública – seja no reconhecimento dos limites ou até a sua defesa em procedimento judicial – pode deslindar por revelar, mesmo que parcialmente, o seu conteúdo. Fica claro, então, que, mesmo que por definição o segredo de negócio esteja incluído no conteúdo de propriedade intelectual, as suas peculiaridades e ligação com a defesa contra a concorrência desleal persistem.

No cenário brasileiro, os segredos empresariais não encontram muita matéria legislada de maneira específica que deem uma definição clara e própria, mas se infere a partir da disposição criminal inserida na Lei nº 9.279/1996, que em seu art. 195, X, define ser crime a divulgação, utilização ou exploração, sem autorização de:

8 DAVID, Paul A. Intellectual Property Institutions and the Panda's Thumb: patents, copyrights, and trade secrets in economic theory and history. *In*: WALLERSTEIN, Mitchel B.; MOGEE, Mary Ellen; SCHOEN, Robin A. (ed.). *Global dimensions of intellectual property rights in science and technology*. Washington, DC: National Academy Press, 1993. p. 19-62.

> [...] conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato.[9]

Deste modo, é possível apreender a existência de proteção cível e criminal contra a violação do segredo empresarial no ordenamento jurídico brasileiro, não obstante a ausência explícita de uma definição legal de segredo empresarial na legislação brasileira.

Necessário ainda delimitar acerca de terminologia, isso porque as expressões "segredo empresarial", "segredo de empresa" e "segredo de negócio", equivalentes à expressão "*trade secrets*" da língua inglesa, indicam um gênero de segredos que estão relacionados com a realização das atividades de empresa, ou seja, com a atividade organizada para produção e circulação de bens e serviços. De outro modo, há uma separação entre o que venha a ser segredo industrial e segredo comercial, bem como outros segredos concernentes à empresa. Neste sentido afirma Payán Rodríguez que:

> a) En primer término [segredo industrial, grifo nosso], los atinentes al sector técnico-industrial de la empresa (procedimientos de fabricación, reparación o montaje, practicas manuales para la puesta a punto de un producto, etc.) [...] b) En segundo lugar, los secretos comerciales son los que se relacionan con el sector puramente comercial de la empresa (venta, publicidad, relaciones con los consumidores y proveedores, etc.) [...] c) Por último, secretos concernientes a otros aspectos de la organización interna de la empresa y relaciones de la misma cuyo conocimiento sería valioso para los competidores, pero que en

9 BRASIL. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. *Diário Oficial da União*: seção 1, Brasília, DF, ano 134, n. 93, p. 8353-8366, 15 maio 1996.

> ningún caso representan un bien en sí mismos. Por ejemplo, relaciones con el personal de la empresa, situación financiera de la empresa, el proyecto de celebrar un contrato etc.[10]

Destarte, observa-se que existe uma diferença entre a natureza industrial e comercial, embora algumas vezes a doutrina na propriedade intelectual costume aplicar o termo segredo industrial como sinônimo de segredo de negócio. Destaque-se, ainda, que em uma mesma organização pode haver a incidência tanto de segredos industriais, quanto de segredos comerciais, dada a possível complexidade das atividades desenvolvidas em uma empresa.

Sobre os segredos de negócio, necessário, ainda, ressaltar que não se confunde com o *know-how*, pois neste pode haver informações que não sejam gravadas com o caráter de confidencialidade, de modo que o segredo empresarial não é aplicável ao *know-how* que não esteja gravado de sigilo, bem como que a ausência de sigilo, por si só, não invalida nem desvaloriza o *know-how*.[11]

Retomando, por fim, a posição do segredo empresarial como um ativo de propriedade intelectual, considerando o quanto já exposto sobre o tema, entendemos que os segredos de negócio constituem categoria *sui generis* dos direitos de propriedade intelectual, gozando de características próprias e estando afeto ao tratamento do direito concorrencial. Deste modo, aderimos ao entendimento[12] de que o segredo de empresa é uma forma de propriedade intelectual de natureza industrial e, por isso, goza de um regime análogo de proteção.

10 PAYÁN RODRÍGUEZ, Carlos Filipe. Secreto empresarial, vigencia como mecanismo de protección en la propiedad intelectual. *Revista La Propiedad Inmaterial*, Bogotá, n. 15, p. 207-224, 2011, p. 211-212.

11 DIAS, José Carlos Vaz e; SANT'ANNA, Leonardo; SANTOS, Bernardo. The legal treatment of know-how in Brazil: peculiarities and controversies of a new intangible form. *Quaestio Iuris*, Rio de Janeiro, v. 9, n. 4, p. 2312-2334, 2016.

12 VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual*. 2. ed. São Paulo: Almedina, 2020.

A Lei Geral de Proteção de Dados Pessoais e os segredos empresariais

Como evidenciam os dados da Pesquisa Nacional por Amostra de Domicílios (PNAD), realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), em 2015, 57% do total da população de 10 anos ou mais de idade tinham acessado a internet nos três meses anteriores à pesquisa e que, neste mesmo ano, 78,3% da população possuía telefone móvel para uso pessoal.[13]

Esses números corroboram com o entendimento de que a tecnologia se tornou mais habitual à população e que este acontecimento representa um ponto de transformação das relações sociais e na vivência de uma denominada "Cibercultura", que é constituída por princípios de interconexão, interação de inteligência coletiva e comunidades virtuais estabelecidas, segundo Pierre Lévy,[14] sobre uma universalidade existente "não porque de fato está em toda parte, e sim porque sua forma ou ideia implicam de direito o conjunto dos seres humanos".

Tal conceito dialoga com os estudos do que Manuel Castells[15] denomina como "Sociedade em Rede", que surge de uma organização social que fornece novas capacidades a uma velha forma de organização social, difundindo-se através do poder integrado nas redes globais de capital, bens, serviços, comunicação, informação, ciência e tecnologia.

Assim, tem-se por definição que a Sociedade em Rede consiste em:

> [...] uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microe-

13 IBGE. *Pesquisa Nacional de Amostra por Domicílios 2015*: acesso à internet e posse de telefone móvel para uso pessoal. Rio de Janeiro: IBGE, 2016.

14 LÉVY, Pierre. *Cibercultura*. 3. ed. São Paulo: Ed. 34, 2010. p. 122.

15 CASTELLS, Manuel. A sociedade em rede: do conhecimento à acção política. *In*: CASTELLS, Manuel; CARDOSO, Gustavo (org.). *A sociedade em rede*: do conhecimento à acção política. Lisboa: Imprensa Nacional; Casa da Moeda (Portugal), 2005. p. 17-30.

> lectrónica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes.[16]

Igualmente, a conjuntura de uso social das tecnologias da informação apresenta a mutação dos próprios elementos estruturais da sociedade, não porque a tecnologia assim o faça de *per si*, sobretudo porque a apropriação desta é que age como elemento de transformação.

Como cediço, o Direito à Privacidade tem caráter fundamental, estando insculpido na Carta Magna em seu art. 5°, X e XII, bem como no Código Civil de 2012 no art. 21, de modo que tal direito também deve também ser debatido considerando as mudanças sociais advindas da revolução tecnológica.

Já nos idos do século XIX, a revolução industrial, o desenvolvimento dos aparelhos fonográficos, fotográficos e a popularização da imprensa, engendraram a necessidade de o Direito oferecer respostas aos conflitos sociais daí nascentes, de modo que se tornou inevitável o desenvolvimento do direito, de modo a proteger a privacidade que poderia ser definida como "o direito de ser deixado sozinho".[17]

Por outro lado, entretanto, no contexto da cibercultura ou da sociedade da informação, para além da privacidade, os dados pessoais se tornam de fundamental relevância, conquanto passem a ser utilizados para as mais diferentes tarefas do dia a dia, mediando muitas relações que influenciam na autonomia e na liberdade, podendo, inclusive, tais dados substituir a presença física de uma pessoa em várias situações.[18]

16 CASTELLS, Manuel. A sociedade em rede: do conhecimento à acção política. *In*: CASTELLS, Manuel; CARDOSO, Gustavo (org.). *A sociedade em rede*: do conhecimento à acção política. Lisboa: Imprensa Nacional; Casa da Moeda (Portugal), 2005. p. 20.

17 WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, p. 193-220, 15 dez. 1890.

18 DONEDA, Danilo. A proteção dos dados pessoais como um Direito Fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, 2011.

Com efeito, a proteção de dados tem sido pensada num contexto de controle do indivíduo sobre seus dados pessoais e seu fluxo, através de uma autodeterminação sobre estes dados, expressa por meio do consentimento e das autorizações que permitam ao cidadão tal controle não apenas no sentido de *notice-and-consent*, mas de maneiras mais profundas.[19]

Deste modo, a proteção de dados exerce uma funcionalidade para além da privacidade simplesmente considerada individualmente e de forte índole patrimonialista, passando a ser uma continuidade da esfera de privacidade, mas que goza de características próprias principalmente pelas formas de atuação em relação ao objeto de sua proteção, de modo a proporcionar novos mecanismos de tutela dos interesses da pessoa humana.[20]

Deste movimento de proteção de dados, podemos apreender a evolução de modelos teóricos, que atualmente se encontram mais centrados na regulação do risco, conforme leciona Zanata, *in verbis*:

> O modelo teórico da regulação do risco, aplicável à proteção de dados pessoais, está relacionado a autores que analisam a "reformatação" da proteção de dados pessoais por um prisma mais complexo do direito regulatório, envolvendo mecanismos de contenção de abusividade e técnicas de prevenção e mitigação a riscos a direitos e liberdades em uma perspectiva coletiva.[21]

Esse modelo teórico, no Brasil se desenvolveu, também a partir do Código de Defesa do Consumidor, do Marco Civil da Internet (Lei

19 BIONI, Bruno. *Proteção de dados pessoais*: função e os limites do consentimento. São Paulo: Forense, 2018.

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

21 ZANATTA, Rafael A. F. *Proteção de dados pessoais como regulação de risco*: uma nova moldura teórica?. *In*: ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1., 2017, Rio de Janeiro. *Anais* [...]. Rio de Janeiro: REDE, 2017. p. 181.

nº 12.965/2014)[22], a recente Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)[23] e, na Europa, o Regulamento Geral de Proteção de Dados, pelos quais os destinatários das normas ali insculpidas devem observar uma série de obrigações relacionadas ao risco da proteção de dados.

Importante salientar que a LGPD versa apenas sobre os dados pessoais, compreendidos, na forma do seu art. 5º, I, como a informação que, relacionada a uma pessoa física, a identifica direta ou indiretamente. Por consequência, estão excluídos do regime e da proteção da LGPD os dados e informações relacionadas às pessoas jurídicas em todas as suas espécies, que, contudo, podem estar tuteladas por outras legislações que versam sobre bens imateriais, como a propriedade intelectual, a lei de informação e transparência pública etc.[24]

O desenvolvimento do sistema brasileiro de proteção de dados a partir da LGPD, que visa a proteção da pessoa e da sua personalidade, deve conviver de maneira harmônica com o desenvolvimento econômico e tecnológico e a inovação, bem como a livre iniciativa, a livre concorrência e a defesa do consumidor, que também são fundamentos do sistema.

Neste sentido, é que se encontram dispostos na LGPD os seguintes princípios, conforme descreve o seu art. 6º: 1. finalidade; 2. adequação; 3. necessidade; 4. livre acesso; 5. qualidade dos dados; 6. transparência; 7. segurança; 8. prevenção; 9. não discriminação; 10. responsabilização e prestação de contas[25]. Cada um desses princípios informa condutas positivas ou negativas, no sentido de incrementar e dirigir a satisfação dos seus fundamentos.

22 BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: seção 1, Brasília, DF, ano 151, n. 77, p. 1-3, 24 abr. 2014

23 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

24 BRASIL. Lei nº 13.709, *op. cit.*

25 *Ibidem*.

Um dos pontos de visível interseção entre os princípios e os fundamentos são as relações dinâmicas que os direitos dos titulares encontram pela interação entre os diversos campos do direito, eis que o conflito de normas se dá por aparência, pois no que é pertinente às normas regras aplica-se a subsunção e, em relação aos princípios, resolve-se por meio da ponderação.

Com efeito, o direito de proteção de dados pessoais não é absoluto e encontra, também, limites que podem ser delineados a partir da interação com outras normas jurídicas. Neste sentido é que se tem a importância destas outras normas e doutrinas como auxiliares no processo de delimitação das fronteiras e dos caminhos interpretativos de um novo ramo do direito que ainda se encontra em fase inicial de desenvolvimento. Entre estas interações, um ponto de singular atenção se dá em relação à propriedade intelectual, mais precisamente em relação aos segredos de empresa.

O texto da LGPD faz menção em 13 diferentes dispositivos acerca do que denomina "segredo comercial e industrial", o que podemos entender como uma variação de terminologia, conforme já explicado anteriormente, para fazer referência ao conjunto dos segredos de negócio ou segredos empresariais. Entretanto, a própria LGPD não traz qualquer definição do que venha a se considerar, para os fins desta lei, o que seria tal categoria de segredos. Deste modo, tais expressões são verdadeiros elementos normativos do tipo, que exigem para a correta aplicação e interpretação da Lei a sua integração com outras normas e fontes do direito.

Contudo, como já visto alhures, a nossa legislação não traz qualquer referência normativa direta sobre o conteúdo e definição do que venha a ser "segredos de empresa", apenas tratando da criminalização da sua violação, o que torna ainda mais dificultosa a compreensão dos limites que são impostos pelo segredo de empresa.

Como modo alternativo, então, devemos fazer referência ao já citado art. 39 do Acordo TRIPS, que traz os elementos básicos para

a caracterização dos segredos de negócio. Necessário comentar sobre o status do TRIPS em nosso ordenamento: este não foi derrogado pela produção da norma específica de Propriedade Industrial (Lei nº 9.279/1994), haja vista que não há propriamente uma disposição específica no direito interno sobre os segredos de negócio. Assim, para que se caracterize o segredo empresarial, devem ser atendidos os requisitos do art. 39 do referido acordo.[26]

Deste modo, a informação, segundo o art. 39 do TRIPS, deve: ser secreta; ter valor comercial por ser secreta; e ser revestida de precauções para a manutenção do segredo. Ressalte-se a natureza cumulativa, de modo que cada um dos requisitos deve ser satisfeito individualmente e em conjunto para a correta configuração do segredo de negócio.

Esta definição correta do conteúdo gravado sob os segredos empresariais se mostra importante no contexto do sistema brasileiro de proteção de dados pessoais. Conforme descreveremos em sequência, considerando apenas para fins didáticos e argumentativos, os segredos empresariais cumprem, na LGPD, as seguintes funções: 1. balizadores dos princípios e direitos dos titulares, 2. limitadores para as obrigações dos agentes de tratamento e 3. Norteadores da atuação da Autoridade Nacional de Proteção de Dados (ANPD).

Em relação à função de balizar os princípios e direitos dos titulares, podemos citar as referências do inciso VI, do art. 6º que trata sobre o princípio da transparência, sendo indicado que o segredo empresarial deve ser observado ao prestar informações aos titulares, *in verbis*:

> [...] VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, *observados os segredos comercial e industrial*.[27]

26 ROSSI, *op. cit.*

27 BRASIL. Lei nº 13.709, *op. cit.*, p. 59, grifo nosso. grifo nosso.

Neste mesmo sentido seguem as disposições dos art. 9º, II; art. 17, V e art. 17, §3º, todos estes tratando sobre direitos dos titulares que, na sua aplicação, precisam ter em observância aos segredos comercial e industrial.

Em relação à função de limitador das obrigações dos agentes de tratamento de dados, em algumas circunstâncias específicas os controladores e operadores podem deixar de fazer ou fazer de maneira diferenciada algumas obrigações se o cumprimento estrito destas incorrer em risco de violação aos segredos de negócios. Nesta função, podemos verificar as disposições do art. 19, II; art. 20, §2º; art. 38; art. 48, §1º, III.

Importante destacar que o art. 20, §2º traz à ANPD a possibilidade de avaliar as circunstâncias específicas para o não oferecimento de informações com base nos segredos comercial e industrial, a saber:

> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.[28]

Podemos ainda observar que os segredos de negócio são importantes também em relação à atuação da ANPD, pois, conforme preconiza a lei, faz parte da competência da ANPD, a saber:

> II – zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei.[29]

28 BRASIL. Lei nº 13.709, *op. cit.*, p. 59, grifo nosso.

29 *Ibidem*.

Neste mesmo sentido também seguem as disposições dos art. 10, §3º, art. 55-J, incisos II, X e art. 20, §5º. Contudo, como a ANPD fora recentemente criada pelo Decreto nº 10.474/2020 e, ainda, não tem atuação ativa até o presente momento, não se encontram delineados quais os critérios que serão adotados pela Autoridade na sua atuação em relação aos segredos empresariais e proteção de dados pessoais.

Conclusão

Conforme foi demonstrado ao longo do trabalho, a propriedade intelectual disciplina as criações do intelecto humano, relacionando-as com o monopólio temporal da exclusividade do direito de exploração destas criações por determinadas pessoas. Comumente o Direito da Propriedade intelectual é dividido em alguns ramos, considerando os direitos do autor e seus conexos, a propriedade industrial e os direitos *sui generis*.

Dentre as várias modalidades destes direitos *sui generis*, existe uma forte discussão sobre a posição da concorrência desleal e dos segredos de empresa dentre os ativos de propriedade intelectual, havendo autores que consideram os segredos de negócio como figuras autônomas, outros como parte da propriedade intelectual ou, ainda, como integrante do direito concorrencial.

Um importante argumento acerca dos segredos industriais fazerem parte do conteúdo da Propriedade Intelectual se dá por detração lógica da presença destes direitos como associados a ela em várias normas de direito internacional ou internas de diversos países, o que é forte indicativo, pois, ainda que não se considere como ativo de propriedade intelectual, os segredos de negócio guardam com ela uma estrita relação de tangenciamento.

Inobstante o amplo debate sobre os segredos negociais no contexto da propriedade intelectual, em nosso ordenamento jurídico pátrio não há norma interna explícita sobre o conteúdo e definições de segredos

de negócio, o que faz incidir, então, a aplicação do art. 39 do Acordo TRIPS, por ser o país também signatário de tal acordo.

O estudo dos segredos negociais também mostra importante relevância quando se fala da proteção de dados pessoais no contexto da legislação brasileira, conquanto o texto da norma faz diversas referências aos segredos industriais e comerciais.

Observa-se que nesta legislação os segredos de negócio cumprem três principais funções ou finalidades, tanto em relação aos princípios e direitos dos titulares, quanto às obrigações dos agentes de tratamento e, ainda, em relação à atuação da ANPD. Deste modo, entender os segredos de negócio se torna essencial para a mais apropriada proteção de dados pessoais, mormente quando na legislação brasileira há poucas referências.

Referências

AMORIM, Ana Clara Azevedo de. O regime jurídico dos segredos comerciais no novo Código da Propriedade Industrial. *Revista Electrónica de Direito*, Porto, v. 19, n. 2, p. 12-41, 2019.

BIONI, Bruno. *Proteção de dados pessoais*: função e os limites do consentimento. São Paulo: Forense, 2018.

BRASIL. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. *Diário Oficial da União*: seção 1, Brasília, DF, ano 134, n. 93, p. 8353-8366, 15 maio 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.html. Acesso em: 10 nov. 2020

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 10 nov. 2020.

CASTELLS, Manuel. A sociedade em rede: do conhecimento à acção política. *In*: CASTELLS, Manuel; CARDOSO, Gustavo (org.). *A sociedade em rede*: do conhecimento à acção política. Lisboa: Imprensa Nacional: Casa da Moeda 2005. p. 17-30.

DAVID, Paul A. Intellectual Property Institutions and the Panda's Thumb: patents, copyrights, and trade secrets in economic theory and history. *In*: WALLERSTEIN, Mitchel B.; MOGEE, Mary Ellen; SCHOEN, Robin A. (ed.). *Global dimensions of intellectual property rights in science and technology*. Washington, DC: National Academy Press, 1993. p. 19-62.

DIAS, José Carlos Vaz e; SANT'ANNA, Leonardo; SANTOS, Bernardo. The legal treatment of know-how in Brazil: peculiarities and controversies of a new intangible form. *Quaestio Iuris*, Rio de Janeiro, v. 9, n. 4, p. 2312-2334, 2016.

DONEDA, Danilo. A proteção dos dados pessoais como um Direito Fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, 2011. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 1 nov. 2020.

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

GIMÉNEZ PEREIRA, Marta. *Efectos de la protección de las patentes farmacéuticas*: un análisis de propiedad intelectual. Ciudad de México: Tirant Lo Blanch, 2017.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *Pesquisa Nacional de Amostra por Domicílios 2015*: acesso à internet e posse de telefone móvel para uso pessoal. Rio de Janeiro: IBGE, 2016. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv99054.pdf. Acesso em: 15 nov. 2020.

LÉVY, Pierre. *Cibercultura*. 3. ed. São Paulo: Ed. 34, 2010.

PARRA SATIZÁBAL, Carlos Alberto. Relación entre propiedad intelectual y derecho de la competencia: mucho más que asuntos de competencia desleal. *Revista La Propiedad Inmaterial*, Bogotá, n. 5, p. 17-36, 2002.

PAYÁN RODRÍGUEZ, Carlos Filipe. Secreto empresarial, vigencia como mecanismo de protección en la propiedad intelectual. *Revista La Propiedad Inmaterial*, Bogotá, n. 15, p. 207-224, 2011. Disponível em: https://revistas.uexternado.edu.co/index.php/propin/article/view/3006. Acesso em: 10 out. 2020.

ROSSI, Juliano Scherner. Elementos de gestão de segredos empresariais para a inovação. *Revista Thesis Juris*, São Paulo, v. 7, n. 1, p. 25-50, 2018.

VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual*. 2. ed. São Paulo: Almedina, 2020.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5., p. 193-220, 1890. Disponível em: http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C. Acesso: 28 out. 2020.

ORGANIZAÇÃO MUNDIAL DO COMÉRCIO. *Acordo sobre aspectos dos direitos de propriedade intelectual relacionados ao comércio*. Marrakech: OMC, 1994. Disponível em: http://www.mdic.gov.br/arquivos/dwnl_1196686160.doc. Acesso em: 8 nov. 2020.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?. *In*: ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 2017, Rio de Janeiro. *Anais* [...]. Rio de Janeiro: REDE, p. 175-193. 2017. Disponível em: http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf. Acesso em: 28 out. 2020.

RESPONSABILIDADE CIVIL NO DESCUMPRIMENTO DA NOVA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI Nº 13.709/2018)

Bárbara Veiga Góes
Teila Rocha Lins D'Albuquerque

Introdução

Com o avanço da internet, dados começaram a ser disponibilizados sem autorização dos seus titulares. O desenvolvimento acelerado deste sistema global acarretou a falta de controle de dados gerados pela disponibilização que o próprio consumidor faz sem percebê-lo. Com isso, aplicativos e empresas passaram a ter acesso a informações pessoais relacionadas a uma pessoa natural identificada ou identificável, como RG e CPF, bem como informações de dados sensíveis (searas de manifestação da personalidade do indivíduo).

A abordagem deste tema se propagou de tal forma que um documentário intitulado *Privacidade Hackeada*[1] teve como foco a criação da Cambridge Analytica nos EUA e sua influência nas decisões políticas, como na campanha de Donald Trump. Essa empresa, em parceria com a plataforma *Facebook*, estudou os cidadãos de cada região do país e escolheu os considerados "passíveis" de influência. Estes seriam os

1 PRIVACIDADE Hackeada. Direção: Jehane Noujam e Karin Amer. New York: The Othrs, 2019. 1 vídeo (139 min).

que se encontravam "em cima do muro", tinham personalidades que se alteravam com o tempo e não costumavam ser extremistas. Eles foram selecionados por meio de suas próprias postagens e através de perguntas feitas pelo Facebook aos usuários.

A partir dessa identificação, segundo o filme, o *site* de relacionamentos começou soltar nas plataformas desses usuários anúncios que estavam relacionados à política de Trump, persuadindo-os a votar nele sem que notassem. A Cambridge Analytica criava perfis de eleitores para finalidades bastante específicas e, junto ao Facebook, responde atualmente a um processo nos EUA por violar dados dos seus usuários.

Com a crescente preocupação mundial acerca da circulação de dados pessoais, os escândalos envolvendo o Facebook e o Google, além da entrada em vigor da Lei Geral de Proteção dos Dados Pessoais Europeia, as pautas brasileiras voltaram-se para o já declarado tema. Diante da ineficiência da legislação nacional até então vigente para a proteção dos direitos da personalidade no uso das novas tecnologias, surge um novo marco legal com o objetivo de suprir esta lacuna, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, para regulamentar e fiscalizar as relações estabelecidas entre os titulares, controladores e operadores dos dados.[2]

Entende-se que, em virtude da falta de conhecimentos técnicos e jurídicos, os usuários são considerados hipervulneráveis, na medida em que aceitam tudo aquilo que lhes é imposto nas contratações, o que permite o aumento considerável de práticas abusivas, especialmente quanto aos dados pessoais. A LGPD foi proposta, portanto, com intuito de evitar a mercantilização não consentida de dados pessoais no Brasil, ou seja, sem o conhecimento dos seus titulares.

2 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

A nova lei, que entrou em vigor em setembro de 2020, ostenta preocupação com esses sujeitos, que sempre estiveram presentes nas relações de consumo, bem como com os impactos que essa vulnerabilidade poderá causar em sua própria eficácia. Em consonância com suas diretrizes, emerge a inquietação dos titulares de dados acerca da responsabilidade aplicada em caso de danos decorrentes do uso indevido de informações.

Sendo assim, surge o seguinte problema a respeito do tema aqui tratado: de que maneira a LGPD aborda a responsabilidade civil dos agentes de tratamento de dados em caso de seu descumprimento? Tal questão justifica a elaboração do presente estudo, evidenciando a busca por corroborar a produção de elementos que contribuam para o desenvolvimento de pesquisas na esfera jurídica, em especial para a nova legislação e suas diretrizes quanto ao dever de reparar.

Compete destacar que o objetivo geral deste trabalho é analisar como o ordenamento jurídico brasileiro atual responsabiliza os agentes de tratamento de dados que descumprem a LGPD. Destarte, a pesquisa apresenta como objetivos específicos: identificar o tipo de responsabilidade civil dos agentes de tratamento de dados; avaliar a pertinência da LGPD nas relações de consumo; e verificar a vulnerabilidade do titular de dados diante da LGPD.

Proteção de dados pessoais como um direito fundamental autônomo à privacidade

Para alguns doutrinadores, a proteção de dados pessoais está inserida na esfera de intimidade do titular, tratando-se de uma dimensão do direito à privacidade. Vejamos:

> [...] (c) o direito fundamental à intimidade e à vida privada, previsto no art. 5.º, X, da CF/1988 (LGL\1988\3), protege a esfera privada do indivíduo em diversas dimensões, inclusive

> na dimensão da privacidade dos seus dados pessoais e da autodeterminação de suas informações.[3]
> O direito à proteção de dados não se limita à proteção da personalidade humana, sua intimidade e vida privada. A proteção de dados visa permitir gama muito maior de relações, ou, de outra parte, evitar que se criem barreiras para a fruição de todos os direitos e garantias. É fonte de fomento para igualdade social.[4]

Nesse sentido, tais autores defendem que a proteção de dados pessoais é um direito à personalidade derivado da tutela da privacidade, que faz jus a um leque de garantias fundamentais que se encontram no ordenamento brasileiro.[5]

Outros autores já pontuam que, apesar de ser um direito fundamental, o direito à proteção de dados é um direito autônomo ao da privacidade por ter certas distinções, uma das quais está relacionada à tutela do direito à proteção de dados, que abrange as esferas privadas e públicas, o que é diferente da privacidade, que se limita à esfera do âmbito privado. Destarte, o direito à proteção de dados pessoais abrange mais liberdades individuais do que as abarcadas pelo direito à privacidade. Como exemplo, existem os cadastros de banco de dados pessoais: mesmo que não envolvam a vida privada da pessoa, eles serão amparados pelo direito à proteção de dados pessoais, o que não ocorreria na esfera do direito à privacidade.[6]

Outra diferença fundamental está nos bens jurídicos tutelados pela privacidade e pelo direito à proteção dos dados pessoais, que não

3 MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. Volume único. São Paulo: Saraiva, 2014. p. 23.

4 ROTUNDO, Rafael Pinheiro. Proteção de dados. *Revista de Direito Privado*, São Paulo, v. 18, n. 74, p. 133–158, 2017, p. 10.

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

6 SHIMABUKURO, Rafael. *Responsabilidade civil na Nova Lei de Proteção de Dados Pessoais*. 2019. Dissertação (Mestrado em Direito) – Centro Universitário Antônio Eufrásio de Toledo, Presidente Prudente, sp, 2019.

coincidem. A proteção dos dados pessoais tem como bem jurídico tutelado as pessoas e seus dados, objetivando proteger suas informações para evitar que sejam discriminadas em razão delas. Já na privacidade, tutela-se a integridade psíquica do indivíduo (a necessidade humana de ter para si uma esfera de reserva).[7]

Na mesma linha desses doutrinadores citados por último, o Senado Federal adotou o entendimento de que há uma necessidade de separar o direito à proteção de dados pessoais do direito à privacidade. Para tanto, propôs um Projeto de Emenda Constitucional que dispõe a proteção de dados como um direito fundamental autônomo:

> Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.[8]

Desse modo, observa-se que apesar de alguns doutrinadores acreditarem que o direito à proteção de dados é derivado da privacidade, outros acreditam que pode ser considerado um direito fundamental autônomo à privacidade, por se tratar de um direito personalíssimo, que difere do direito à privacidade. Inclusive, essa autonomia já vem sendo reconhecida pelo próprio Senado Federal.

Vulnerabilidade do titular de dados

Sabe-se que o Código de Defesa do Consumidor (CDC) e a LGPD visam proteger o consumidor e o titular dos dados, devido à vulnerabilidade de cada um, o que justifica a semelhança entre os dispositivos. Essa similitude permite que se analise analogamente as situações

7 ZANON, João Carlos. *Direito à proteção dos dados pessoais*. 2012. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2012.

8 BRASIL. *Proposta de Emenda à Constituição nº 17, de 2019*. Brasília, DF: Senado Federal, 2019.

de vulnerabilidade às quais os titulares de dados e os consumidores são expostos.[9]

A vulnerabilidade do consumidor é perceptível diante da sua fragilidade nas relações de consumo, por isso, o CDC adotou o princípio da vulnerabilidade no inciso I do artigo 4º, que norteia as relações consumeristas.[10] O princípio da vulnerabilidade define o consumidor como parte mais fraca da relação e foi instaurado com o intuito de equilibrar as relações de consumo, já que o desequilíbrio na relação consumerista é nítido, em razão de o usuário não dispor de conhecimentos técnicos e jurídicos necessários para avaliar de forma correta a qualidade e complexidade dos produtos e serviços que venha a adquirir. No meio virtual, a situação de vulnerabilidade é ainda mais agravada, por inexistirem normas no comércio eletrônico que regulem a vulnerabilidade do usuário.[11]

Por carecerem de conhecimentos técnicos e jurídicos, os consumidores não têm voz ativa no cenário digital, o que permite o aumento considerável de práticas abusivas, especialmente no tocante aos dados pessoais. Os dados pessoais são, em maioria, intangíveis, de forma que não permitem ao titular certeza jurídica de seu tratamento, reiterando o local de fragilidade que esse indivíduo ocupa como sujeito de direitos.[12;13]

A ignorância do usuário fica nítida no ato de achar que tudo se trata de uma mera coincidência no cenário virtual, quando, em verdade, ele está diariamente perante obstáculos à total compreensão da utilização

9 SHIMABUKURO, *op. cit.*

10 BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, ano 128, n. 176, p. 17271, 12 set. 1990.

11 NOVAES E SOUSA ADVOGADOS ASSOCIADOS. A vulnerabilidade do consumidor no e-commerce. *Jusbrasil*, [*s. l.*], 2016.

12 SOBRINHO, Nayara. *A Proteção de Dados Pessoais no E-commerce*: análise da aplicação da LGPD diante da vulnerabilidade do consumidor. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Centro Universitário Unifacig, Manhuaçu, MG, 2019.

13 COÊLHO, Amanda Carmen Bezerra. *A Lei Geral de Proteção de Dados Pessoais brasileira como meio de efetivação dos direitos da personalidade*. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal da Paraíba, João Pessoa, 2019.

de seus dados.[14] Seguindo essa linha de raciocínio, pode-se considerar o titular dos dados pessoais como sujeito hipervulnerável. Isso porque esse cidadão, em muitos casos, não sabe sequer da coleta de seus dados pessoais, tampouco do poder para impedir tal coleta. E, ainda que tenha ciência desta coleta, não tem noção de sua importância, casos em que acaba "trocando" tais dados por vantagens irrisórias.[15]

Sobre este último equívoco, Bioni destaca:

> O ser humano tem a tendência de focar nos benefícios imediatos, o que, de acordo com o arranjo e os modelos de negócios da economia informacional, é representado pelo acesso a um produto ou serviço on-line. Por tal razão, deixa de sopesar os possíveis prejuízos à privacidade, que são temporariamente distantes. De fato, os possíveis danos com relação à perda do controle sobre as informações pessoais só podem ser experimentados no futuro.[16]

Essa vulnerabilidade dos titulares quanto aos dados pessoais também foi reconhecida pela LGPD, que, para tornar mais eficaz a sua aplicação, implementou um método de política de autorização e consentimento dos dados com vistas a proteger o indivíduo que possui uma vulnerabilidade própria. Faz-se necessária ainda, a renovação do consentimento, quando houver mudanças no modo do tratamento ou quando se tratar de dados sensíveis.[17]

A coleta e o compartilhamento de dados devem ocorrer de maneira gratuita e prévia. Mas, segundo Leme,[18] 91% da população confirmam os termos de privacidade sem sequer lê-los, em um desinteresse

14 SHIMABUKURO, *op. cit.*

15 *Idem*.

16 BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e o limite do consentimento. Rio de Janeiro: Forense, 2019. p. 147.

17 COTS, Marcio. A Lei Geral de Proteção de Dados no e-commerce. *E-commerce Brasil*, [*s. l.*], 2018.

18 LEME, Carolina da Silva. Proteção e tratamento de dados sob o prisma da legislação vigente. *Revista Fronteiras Interdisciplinares do Direito*, [*s. l.*], v. 1, n. 1, p. 178-197, 2019.

proporcionado principalmente pelo tamanho dos termos e pela complexidade com que se encontram estruturados. Diante deste cenário, não basta somente o consentimento do consumidor, é crucial que se informe com clareza a razão pela qual os dados serão tratados, de maneira que a Política de Privacidade de muitas empresas seja alterada para uma linguagem menos formal e de fácil compreensão aos usuários.[19] [20]

Lei Geral de Proteção de Dados Pessoais

Para melhor compreensão da LGPD e da necessidade de sua criação, é necessário o estudo da sua evolução histórica, conceitos, sujeitos e aplicações.

Evolução histórica

Com o avanço tecnológico acelerado, nas décadas de 1960 e 1970, vieram as primeiras preocupações sobre o armazenamento e a utilização de dados pessoais. O uso de computadores por indivíduos em todo o mundo resultou no aumento da capacidade de armazenamento fácil, rápido e amplo de informações.[21]

No dia 25 de março de 2018, surgiu na União Europeia a *General Data Protection Regulation* (GDPR), primeira lei acerca do tema, que já vinha sendo planejada e elaborada antes mesmo da querela da Cambridge Analytica. Trata-se de um diploma legal que passou a exercer o controle regulamentar sobre as empresas da União Europeia, assim como de

19 LEME, *op. cit.*

20 SOBRINHO, Nayara. *A Proteção de Dados Pessoais no E-commerce*: análise da aplicação da LGPD diante da vulnerabilidade do consumidor. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Centro Universitário Unifacig, Manhuaçu, 2019.

21 SAUAIA, Hugo Moreira Lima. *A proteção de dados pessoais no Brasil*. Rio de Janeiro: Lumen Juris, 2018.

todas aquelas empresas que mantêm qualquer tipo de relação comercial envolvendo dados pessoais vinculados à territorialidade europeia ou que lhe preste serviço.[22]

A aprovação do Regulamento Geral sobre a Proteção de Dados da União Europeia também pressionou o Brasil, ocasionando a edição de uma lei mais específica sobre o tema, visando nortear a coleta, uso, armazenamento e processamento de dados entre entes públicos e privados, além de se enquadrar no padrão internacionalmente exigido. Em agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados no Brasil (Lei Federal nº 13.709/2018).[23]

A LGPD estabeleceu a *vacatio legis* de dois anos após sua sanção para que as empresas pudessem se adequar, logo, entraria em vigor em 14 de agosto de 2020. Ocorre que esse prazo foi alterado pela publicação, no dia 29 de abril de 2020, da Medida Provisória nº 959/2020, que ampliou em seu artigo 4º a *vacatio legis* da LGPD para 3 de maio de 2021, em razão da pandemia da covid-19.[24] Contudo, tal fato foi novamente alterado com a conversão da medida provisória na Lei nº 14.058/2020, que não recepcionou a ampliação do prazo, ensejando a vigência em setembro de 2020.[25]

Dados pessoais

Os dados pessoais foram definidos no artigo 4º do Regulamento 2016/679 da União Europeia, o GDPR:

22 COÊLHO, *op. cit.*

23 LEME, *op. cit.*

24 MECABÔ, Alex. Postergação da vigência da LGPD: um remédio necessário?. *Conjur*, [*s. l.*], 1 maio 2020.

25 BRASIL. Lei nº 14.058, de 17 de setembro de 2020. Dispõe sobre a conversão da Medida Provisória nº 959 de 2020. *Diário Oficial da União*: seção 1, Brasília, DF, ano 158, n. 180, p. 1, 18 set. 2020.

> "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 eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.[26]

Basicamente, os dados são informações primitivas e fragmentadas, como uma espécie de "pré-informação", ou seja, são atos que necessitam de interpretação antes de adquirirem algum sentido específico. É importante ressaltar as redes sociais, especialmente *Instagram* e *Facebook*, plataformas coletoras de dados por meio da conta do usuário, que dá acesso livre a diversas informações que são inseridas no banco de dados.[27,28,29]

Os dados pessoais podem ser classificados de diversas formas, com destaque para a divisão feita pela LGPD: dados identificados (são os que determinam quem é o titular, como nome, identidade, CPF, entre outros); dados identificáveis (aqueles dos quais não se consegue diretamente determinar o titular, mas é possível sabê-lo com uso de outras informações, como número do cartão de crédito, IP do

26 UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, Luxembourg, 2016.

27 DONEDA, *op. cit.*

28 MENDONÇA, Renata. Como os testes de Facebook usam seus dados pessoais – e como empresas ganham dinheiro com isso. *BBC Brasil*, São Paulo, 22 fev. 2018.

29 BRUNO, Giovana Pizzato. *A proteção de dados pessoais na internet no Brasil*: regime jurídico e responsabilidade dos agentes sob a ótica da Lei nº 13.709 de 14 de agosto de 2018. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Antônio Eufrásio de Toledo, Presidente Prudente, 2019.

computador, nome da empresa onde a pessoa trabalha, entre outros); dados sensíveis (estão relacionados a origem étnica ou racial, crenças religiosas, filiação sindical, direcionamento político, orientação sexual e, especificamente, informações relativas a saúde, genética ou biométrica); por fim, tem-se os dados anonimizados (aqueles em que não se é possível identificar a pessoa, como, por exemplo, dados de uma pesquisa do IBGE).[30]

Os dados pessoais podem formar um banco de dados quando agrupados e organizados. Esses bancos funcionam como um extenso arquivo que traz informações de cada indivíduo, informações que podem ser agrupadas por assunto, com objetivo de facilitar a consulta do "proprietário". O banco de dados pode ser público ou privado. Nele, os dados são processados pelas respectivas organizações que visam ordenar, tratar e classificá-los, formando assim um perfil do usuário. Ele será público quando gerido pela administração pública e será privado quando gerido por pessoas físicas ou jurídicas, para acesso próprio, sem controle de terceiros.[31]

No decorrer dos últimos anos, os dados pessoais tornaram-se indispensáveis à movimentação econômica e à troca das mais diversas informações sobre os consumidores. O distanciamento pessoal, uma realidade contemporânea, passou a ser a regra também nas relações consumeristas. Assim, o manuseio dos dados acaba por servir como meio para inúmeras atividades, em especial, a formulação de perfis de consumidores e o conhecimento da capacidade econômica deles.[32]

30 MIRANDA, Marcelo. *Lei Geral de Proteção de Dados* – LGPD. 2019. [*S. l.*: *s. n.*], 2019.

31 OLIVEIRA, Tassyara Onofre de. *Gestão de dados pessoais*: uma análise de casos concretos a partir do ordenamento jurídico brasileiro. 2017. Dissertação (Mestrado em Gestão nas Organizações Aprendentes) – Universidade Federal da Paraíba, João Pessoa, 2017.

32 ALVES, Victor Hugo Pérez. *Direitos da Personalidade e a proteção de dados pessoais nos contratos de consumo*. 2008. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2008.

Dados sensíveis

Os dados sensíveis são aqueles relacionados à origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical ou associativa, bem como os relativos à saúde ou sexualidade. Além de identificarem o indivíduo, eles revelam os elementos mais profundos da sua personalidade. Por isso, situações que os envolvem apresentam um risco maior de ofensa aos direitos fundamentais, motivo também pelo qual necessitam de maior proteção.[33,34,35]

Os dados sensíveis, também chamados de dados especiais, representam uma espécie de dados pessoais. A GDPR lhes faz esta referência:

> Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo "origem racial" no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas.[36]

A razão para a criação dessa categoria autônoma de dados pessoais se deu, portanto, a partir da constatação de que o armazenamento, o processamento e a circulação de certos tipos de dados ocasionariam um risco maior de práticas discriminatórias. Entre diversos dados associáveis à pessoa, alguns são especialmente aptos a favorecer processos sociais de exclusão e segregação, o que se mostra como

33 LIMBERGER, Têmis. O Direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais. *Revista Brasileira de Direitos Fundamentais*, Porto Alegre, v. 4, n. 11, 2010.

34 OLIVEIRA, Tassyara Onofre de, *op. cit.*

35 SOBRINHO, *op. cit.*

36 UNIÃO EUROPEIA. Regulamento 2016/679, *op. cit.*

a chave de qualificação de determinados dados como sensíveis. É com fundamento nessa discriminação, tanto por parte do mercado quanto do Estado, que os dados sensíveis se associam a conjunturas em que podem estar presentes potenciais violações de direitos fundamentais, de forma que devem ser protegidos para efetivarem diversos direitos como à saúde, liberdade comunicativa, religiosa, de associação, entre outros.[37;38;39]

Agentes de tratamento de dados pessoais

Os agentes de tratamento de dados pessoais são os controladores e operadores de dados, como a própria Lei nº 13.709/2018 prevê. A Lei ainda conceitua tais agentes em seu artigo 5º, incisos VI e VII: o controlador é a "[...] pessoa natural ou jurídica, de direito público ou privado, a quem competem às decisões referentes ao tratamento de dados pessoais"; e o operador, a "[...] pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".[40]

A definição de tratamento de dados pessoais, na LGPD, é extremamente abrangente, estando prevista em prevista no artigo 5º, inciso X:

> Art. 5º Para fins desta Lei considera-se: [...] X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento,

37 MENDES, *op. cit.*

38 MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, p. 159-180, 2018.

39 KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 445-463.

40 BRASIL. Lei n° 13.709, *op. cit.*, p. 59.

> arquivamento, armazenamento, eliminação, avaliação ou controle de informação, modificação, comunicação, transferência, difusão ou extração [...].[41]

Dentre as obrigações dos agentes, está o registro das operações de tratamento de dados que realizarem. A regra está estabelecida no artigo 37 da LGPD, que tem o intuito de assegurar proteção ao titular, assim como possibilitar a fiscalização do procedimento e a defesa em possível suspeita em relação aos agentes.[42]

Os controladores e operadores estão encarregados de informar violações de dados à Autoridade Nacional de Proteção de Dados, além de adotar e registrar as medidas de seguranças técnicas e administrativas para proteger os dados pessoais de acessos que não estejam autorizados e de situações acidentais ou ilícitas, como destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.[43]

Aplicação da lei

Antes da criação da LGPD, o tratamento de dados pessoais não era levado a sério, mesmo estando previsto de forma genérica em leis e normas como a Constituição Federal, o CDC, a Lei de Acesso à Informação, a Lei do Cadastro Positivo e o Marco Civil da Internet. Isso ocorria devido à quantidade de regimes legais para disciplinar um mesmo tema, o que gerava muitos conflitos de aplicação de leis e contradições na prática jurídica, acarretando também a

41 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

42 OLIVEIRA, José Eduardo. *Responsabilidade civil dos agentes de proteção de dados no Brasil*. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal da Paraíba, Santa Rita, 2019.

43 MIRANDA, *op. cit.*

insegurança de empreendedores que precisam lidar com os dados de seus usuários.[44]

A nova lei busca definir quais informações pessoais podem ser coletadas, acessadas, mantidas e abordadas, em meio digital ou físico, além de prever punições em caso de descumprimento das normas estabelecidas. Esta nova legislação é resultado de um grande avanço no trato dos dados e uma convergência com a tendência do que está sendo aplicado mundialmente.[45]

Segundo o artigo 3º da LGPD, a aplicabilidade da lei é para todos aqueles que realizam o tratamento de dados pessoais, sejam órgãos públicos ou privados, pessoas jurídicas ou físicas, independentemente do meio. É válido ressaltar, de acordo com o parágrafo primeiro do artigo supracitado, que serão considerados todos os dados coletados em território nacional dos titulares que se encontrarem nele durante a coleta.[46]

É conferido poder ao titular dos dados, pois o artigo 18 da referida lei prevê que ele tem direito, a qualquer momento, de exigir do controlador uma "prestação de contas" sobre o que está sendo feito com seus dados, ter acesso imediato e poder realizar correções destes, assim como pedir a eliminação dos seus dados tratados, salvo no caso das hipóteses do artigo 16, que determina:

> Art. 16: Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I – cumprimento de obrigação legal ou regulatória pelo controlador; II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III – transferência a terceiro,

44 MIRANDA, *op. cit.*

45 *Idem.*

46 BRUNO, *op. cit.*

> desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.[47]

O consentimento, de início, é utilizado como argumento para justificar as maiores arbitrariedades no tratamento de dados. Acontece que isso não é suficiente, tendo em vista que o titular se encontra em situação de vulnerabilidade singular e, nesta conjuntura, não há como atribuir apenas a ele o papel de abonador do processo de tratamento.[48]

Devem ser analisados, ainda, os requisitos estabelecidos no artigo 8º da LGPD para que o consentimento seja dado de maneira válida e regular. Dentre eles, está o de consentir por escrito ou por outro meio assemelhado que demonstre a manifestação de vontade do titular. Caso haja vício de consentimento, o controlador é impossibilitado de realizar o tratamento, cabendo-lhe provar que esse consentimento foi obtido de maneira válida. Pode, além disso, ser considerado nulo o consentimento que se mostre genérico e inseguro, devendo este ter uma finalidade determinada. Por fim, é importante salientar que, a qualquer momento, o titular pode revogar tal autorização.[49]

Embora os dados pessoais sejam um novo "ativo econômico" e um novo direito da personalidade, o consentimento não exprime, necessariamente, a efetivação da autodeterminação informacional, pois a "(hiper) vulnerabilidade" faz com que o titular não tenha condições de conhecer efetivamente todas as consequências do tratamento para poder se contrapor de modo a conseguir barganhar melhores condições. Outros autores, no entanto, atribuem

47 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

48 BIONI, *op. cit.*

49 OLIVEIRA, José Eduardo, *op. cit.*

ao consentimento e ao contrato força de solucionar a questão da liberdade e da privacidade.[50;51]

Além do consentimento, é necessária a utilização de transparência como demonstração de boa-fé por parte do controlador. O artigo 9º, com o objetivo efetivar o princípio da transparência, determina quais informações devem ser previamente fornecidas aos titulares sobre todo o ciclo de tratamento de dados. Portanto, a consulta a essas informações tem de estar disponível conforme princípio do livre acesso, devendo o controlador esclarecer qual a finalidade do tratamento, no mesmo sentido do artigo 6º, inciso I.[52;53]

Responsabilidade civil da LGPD

É importante observar que o objetivo geral do trabalho é analisar como o ordenamento jurídico brasileiro responsabiliza os agentes de tratamento de dados que descumprem a Lei Geral de Proteção de Dados. Diante disso, é necessário o estudo da responsabilidade civil de modo mais direcionado à esfera da proteção de dados.

Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais

O termo responsabilidade surgiu do termo latino *respondere*, de *spondeo*, pelo qual o devedor se vinculava ao credor nos contratos verbais, nascendo assim uma obrigação primitiva de natureza contratual. Trata-se de um dever jurídico de responder por ação ou omissão

50 PINHEIRO, Patrícia Peck. *Proteção de dados pessoais*: comentários à Lei nº 13.709/2018. São Paulo: Saraiva, 2018.

51 BIONI, *op. cit.*

52 OLIVEIRA, José Eduardo, *op. cit.*

53 MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019.

imputável que indique lesão ao direito de outrem, protegido por lei e imposto a todos. Por fim, a responsabilidade civil pode ser definida como uma obrigação patrimonial de reparar o dano moral ou material causado ao ofendido pela inobservância do ofensor de um dever jurídico legal ou convencional.[54;55;56]

Ao analisar o Código Civil, especificamente seus artigos 927, 932, 936 e 937, pode-se concluir que a responsabilidade civil é um instituto que visa à reparação de danos causados por ato cometido pela mesma pessoa ou por terceiros, podendo ainda ser cometido pela coisa ou pessoa por quem se responde.[57]

A responsabilidade civil ainda pode ser subdividida em responsabilidade civil subjetiva e objetiva. A subjetiva, prevista nos artigos 186 e 187 do Código Civil, leva em consideração a culpa ou o dolo do agente causador do dano. Já a objetiva é aquela prevista no dispositivo 927 do Código Civil, segundo a qual, a despeito da culpa ou dolo do agente, ele será responsabilizado. Um exemplo da utilização da responsabilidade objetiva está prevista no artigo 14 do CDC, que exclui a necessidade da caracterização de culpa do agente nas relações consumeristas devido aos riscos a que os consumidores são expostos por serem vulneráveis ou hipossuficientes. O CDC adotou a teoria do risco-proveito, que gera a responsabilidade independentemente de culpa, na medida em que se expõe ao risco outras pessoas, determinadas ou não, e que delas se tira um

54 MELO, Marco Aurélio Bezerra. *Curso de Direito Civil*: responsabilidade civil. São Paulo: Atlas, 2015. v. 4.

55 GUIMARÃES, Deocleciano Torrieri. *Dicionário técnico jurídico*. 19. ed. Volume único. São Paulo: Rideel, 2016.

56 TARTUCE, Flávio. *Manual de responsabilidade civil*: volume único. Rio de Janeiro: Forense; São Paulo: Método, 2018. Versão digital.

57 DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro*: responsabilidade Civil. 32. ed. São Paulo: Saraiva, 2018. v. 7.

benefício, direto ou indireto, devendo-se arcar com as consequências da situação de agravamento.[58;59]

No que tange à LGPD, o legislador foi omisso ao não estabelecer a responsabilidade dos agentes de tratamento de dados como subjetiva ou objetiva. Todavia, nota-se na referida lei a vulnerabilidade e os riscos aos quais o consumidor é exposto, além da superioridade apresentada pelos produtores e prestadores de serviços, o que faz optar-se por dar maior proteção ao titular de dados, tornando a responsabilidade objetiva em regra, enquanto a subjetiva seria uma exceção.[60]

O artigo 45 da LGPD estabelece que, em caso de violação à legislação de proteção de dados no âmbito das relações de consumo, serão aplicadas as regras de responsabilidade previstas na legislação pertinente. Assim, quando se trata de relações de consumo, aplica-se a responsabilidade prevista no CDC, que adota a responsabilidade objetiva.[61]

O usuário (titular dos dados), por sua vez, precisa de uma maior proteção legislativa, em razão de sua inocência e ignorância sobre o tratamento de seus dados pessoais. Nesse sentido, pode-se definir que o cidadão é (hiper)vulnerável, já que, na maioria das vezes, não sabe sequer da coleta de seus dados pessoais, muito menos do poder de impedir tal coleta, o que torna outra vez necessária a aplicação da responsabilidade objetiva como regra.[62]

Também é válido destacar que os controladores exercem uma atividade que expõe os titulares a determinados riscos, pela grande importância dos dados pessoais. Deste modo, a Lei nº 12.414/2011 determina a regra da responsabilidade objetiva para atividades consideradas de risco:

.....

58 TARTUCE, *op. cit.*

59 SHIMABUKURO, *op. cit.*

60 *Idem*.

61 SILVA, Bruno Marcos Gomes. Dos agentes de tratamento de dados pessoais. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *LGPD*: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p. 324-325.

62 SHIMABUKURO, *op. cit.*

> Art. 16. O banco de dados, a fonte e o consulente são responsáveis, objetiva e solidariamente, pelos danos materiais e morais que causarem ao cadastrado, nos termos da Lei nº 8.078, de 11 de setembro de 1990 (Código de Proteção e Defesa do Consumidor).[63]

Então, quando houver reparação de danos materiais e morais advindos de danos causados pela violação à proteção de dados pessoais, será preciso estabelecer a responsabilidade objetiva como regra na LGPD. O artigo 42 da referida lei estabelece que, ao vincular a obrigação de reparação dos danos com o exercício do tratamento de dados pessoais, o legislador opta pela objetividade da responsabilidade.[64]

Da responsabilidade e do ressarcimento de danos

A LGPD estabelece, em seu artigo 22, a possibilidade de ajuizamento de ação perante o Poder Judiciário para defesa dos interesses e dos direitos dos titulares de dados:

> Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.[65]

Já em seu dispositivo 42, a mesma lei impõe ao controlador e ao operador a obrigação de reparação de danos decorrentes da violação à legislação de proteção de dados pessoais:

63 BRASIL. Lei n° 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. *Diário Oficial da União*: seção 1, Brasília, DF, ano 148, n. 111, p. 2-3, 10 jun. 2011. p. 3.

64 BRASIL. Lei n° 13.709, *op. cit.*, p. 59.

65 *Ibidem*, p. 59.

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.[66]

A fim de assegurar a efetiva indenização aos titulares de dados, a legislação determina, no §1º do artigo 42, a responsabilização solidária do operador e controlador ou de controladores que estiverem envolvidos no tratamento gerador do dano. Ademais, a LGPD prevê, no §2º deste mesmo artigo, a inversão do ônus da prova em favor do titular dos dados, quando houver verossimilhança das alegações, hipossuficiência para fins de produção da prova ou for excessivamente onerosa a sua produção. Por fim, a lei permite, no §3º do referido dispositivo, o ajuizamento de ação de reparação de danos coletivos.[67]

A LGPD também aborda, no seu artigo 44, que a irregularidade no tratamento de dados será constatada quando houver inobservância da legislação ou não se fornecer a segurança que o titular de dados espera, sendo tidas como circunstâncias relevantes o modo de realização, os resultados e riscos razoavelmente esperados e as técnicas de tratamento de dados pessoais disponíveis à época.[68]

Em alguns casos de responsabilização civil das empresas, pode-se aplicar o CDC, quando se constatar uma relação consumerista, em que o titular dos dados é considerado consumidor direto ou indireto e a empresa é considerada fornecedora de produtos ou serviços. A jurisprudência deve tomar a teoria do risco da atividade para concluir pela responsabilidade objetiva do fornecedor, de acordo com o CDC. Com

66 BRASIL. Lei nº 13.709, *op. cit.*, p. 59.

67 *Ibidem*, p. 59.

68 MONTEIRO, Yasmin Sousa. A efetividade dos mecanismos de proteção de dados pessoais na Lei 13.709/2018. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, DF, 2019.

isso, o Poder Judiciário será acionado para efetivar as reparações civis previstas na LGPD e para eventuais casos de judicialização de medidas administrativas da Autoridade Nacional de Proteção de Dados (ANPD).[69]

Responsabilidade dos agentes de tratamento de dados

Pode-se observar que a responsabilidade dos agentes é o ponto central da proteção de dados quando se trata da LGPD. O mercado de dados, em virtude do desenvolvimento tecnológico, está cada vez mais presente em nossos dias e tem grande importância em nosso cotidiano. Assim, a possibilidade de dano ao titular é consequência direta do tamanho da sua importância econômica e da sua abrangência.[70]

O tratamento de dados feito pelo controlador e pelo operador dos dados será considerado irregular quando houver inobservância da lei, sendo consequência para os responsáveis a reparação dos danos causados, como prevê o *caput* do artigo 44. Esses agentes de tratamento responderão pelos danos que causarem, sejam materiais ou morais, individuais ou coletivos, por violação à LGPD. Sendo assim, cada um responde pelos seus atos praticados e por eventuais prejuízos causados.[71;72]

Para que esses agentes sejam responsabilizados civilmente, deve existir nexo de causalidade entre a conduta ilícita prevista na LGPD e o dano. Nexo causal é conceituado como elemento referencial entre a conduta e o resultado, por meio do qual pode-se concluir quem foi o causador do dano.[73;74]

69 SÁ JUNIOR, Sergio Ricardo C. *A regulação jurídica da proteção de dados pessoais no Brasil*. 2019. Trabalho de Conclusão de Curso (Especialização em Direito) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2019.

70 OLIVEIRA, José Eduardo, *op. cit.*

71 COTS, *op. cit.*

72 OLIVEIRA, José Eduardo, *op. cit.*

73 CAVALIERI FILHO, Sergio. *Programa de Responsabilidade Civil*. 14. ed. São Paulo: Atlas, 2020.

74 BRUNO, *op. cit.*

Em exceção à regra do artigo 42 da LGPD, tem-se o §1º, que determina quando a responsabilidade pelo ressarcimento será considerada solidária, com a finalidade de assegurar a efetiva indenização ao titular dos dados. A responsabilidade solidária é mais uma das formas de responsabilidade, com a qual se visa que a vítima não seja prejudicada. Portanto, o titular dos dados pessoais, que será o credor da indenização, poderá cobrar a dívida total tanto do controlador como do operador, dentre qualquer uma das duas hipóteses, pois, nestes casos, ambos seriam responsáveis solidários.[75]

O controlador e o operador possuem responsabilidade solidária quanto a incidentes de segurança de informação, uso indevido ou não autorizado dos dados ou se agirem em desconformidade com a referida lei. No entanto, a responsabilidade do operador será limitada às suas obrigações contratuais.[76]

A Lei estabeleceu expressamente três exceções à responsabilização descritas nos incisos do dispositivo 43, isto é, situações em que os agentes de tratamento poderão afastar o dever de indenizar. Estas ocorrerão quando os agentes provarem: 1. que não realizaram o tratamento dos dados; 2. embora efetuado o tratamento, não violaram a LGPD; por fim, 3. o dano decorreu de culpa exclusiva do titular dos dados ou de terceiros. Este último inciso acaba isentando o agente causador do dano quando existe culpa exclusiva da vítima, o que pode acarretar em interpretações incoerentes, especialmente quando se tratar de vítimas vulneráveis (mulheres, adolescentes, idosos etc.).[77;78]

Por fim, o artigo 44 da LGPD estabelece quais atos praticados pelos agentes de tratamento serão considerados irregulares. Será irregular e, portanto, uma ilicitude, o tratamento dos dados pessoais quando

75 BRUNO, *op. cit.*

76 MONTEIRO, *op. cit.*

77 COTS, *op. cit.*

78 LONGHI, João Victor Rozatti; MARTINS, Guilherme Magalhães. Impactos positivos da nova lei brasileira de proteção de dados. *Jota*, [*s. l.*], 27 ago. 2018.

os agentes de tratamento violarem qualquer disposição da LGPD ou, tendo o dever quanto ao fornecimento de segurança dos dados do titular, deixarem de observá-lo.[79]

Responsabilidade civil do vazamento de dados pessoais por ataques de *crackers*

Para melhor abordagem do tema, é necessário analisarmos também a responsabilidade civil dos agentes de tratamento de dados pessoais que não atuam de maneira lícita com os dados, também conhecidos como *crackers*. Inicialmente, é importante distinguir o que é um *hacker* e o que é um cracker. O termo *crackers* foi criado, em 1985, por *hackers* que discordavam da utilização do termo *hacker* pela imprensa para definir técnicos ou usuários de computadores que incorressem em ações ilegais ou que causassem transtornos para outras pessoas. Entende-se que cracker é apenas uma espécie do gênero *hacker*: apesar de serem semelhantes, eles se diferenciam pela finalidade de suas práticas, já que a atividade dos *hackers* é positiva e legal, enquanto a motivação dos *crackers* é criminosa em sua essência, pois agem normalmente com premeditação e com objetivo criminoso de obter vantagens ilícitas.[80]

O *hacker* pode ser definido como um *expert* na área da informática que modifica *softwares* e *hardwares*. Contudo, utiliza sua expertise para desenvolver defesas contra invasores. Assim, diferem-se dos *crackers* por terem uma finalidade oposta à dos *hackers*, já que utilizam sua expertise para invadir sistemas, com o intuito de tirar proveito de brechas.[81]

No ordenamento jurídico brasileiro, a invasão de um dispositivo informático está prevista no artigo 154-A do Código Penal, que foi

79 BRUNO, *op. cit.*

80 CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. *Âmbito Jurídico*, Rio Grande, v. 15, n. 99, 2012.

81 SHIMABUKURO, *op. cit.*

incluído recentemente pela Lei Carolina Dieckmann. Segundo tal dispositivo, incorre no crime aquele que:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita [...] § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*.[82]

Além do artigo supracitado, há de ressaltar que, para outros crimes cometidos no meio cibernético, é possível a aplicação de outros dispositivos do Código Penal, como é o caso da injúria no meio informático:

> No Código Penal, diversos tipos legais são pertinentes à criminalidade no mundo da informática. Para ofensas à honra alheia, tais como imputações de crimes, a calúnia (art. 138); na difusão de boatos humilhantes, a difamação (art. 139); e nos ataques pessoais, menosprezando as características da vítima, especialmente com apelidos grosseiros, a injúria (art. 140). Nas intimidações em geral, desponta o crime de ameaça (art. 147). Na invasão de conta bancária para desvio ou saque de valores, é de se reconhecer o furto (art. 155). Por sua vez, o envio de vírus para inutilizar equipamento ou seu conteúdo caracteriza o dano (art. 163)[83].

Nesse sentido, nota-se que a internet não é isenta de proteção e que vários dispositivos penais podem ser aplicados no âmbito informático.

82 BRASIL. Lei nº 2.848, de 7 de dezembro de 1940. Institui o Código Penal. *Diário Oficial da União*: seção 1, Brasília, DF, dez. 1940.

83 MASSON, Cleber. *Direito penal esquematizado*: vol. 3: parte especial. 6. ed. Rio de Janeiro: Forense; São Paulo: Método, 2016. v. 3, p. 330.

Porém, deve-se discutir a responsabilidade civil dos agentes quando ocorrerem esses tipos de ataques cibernéticos a bancos de dados, com os quais os *crackers* objetivam vantagens indevidas.[84]

A LGPD define em seu artigo 46 que a segurança dos dados pessoais é obrigação do controlador e operador, e que a falha da segurança dos bancos de dados será da responsabilidade de ambos. Não é possível, nessa situação, a aplicação do excludente de ilicitude também prevista na referida lei, no inciso III do dispositivo 43, porque a própria lei já imputa responsabilidade pela falta de segurança em seu artigo 44. Logo, a única forma de aplicar o excludente por fato de terceiro seria se houvesse prova de ausência de falha e de que o operador e o controlador adotaram as medidas técnicas e administrativas de segurança necessárias.[85]

Considerações finais

Na pesquisa realizada para elaboração do presente capítulo, foram aplicadas estratégias metodológicas que permitiram, através da revisão sistemática da literatura de estudos históricos, legais, doutrinários, artigos científicos e revistas eletrônicas, analisar nosso ordenamento jurídico e seu conteúdo. Possibilitou-se a detecção dos impactos da LGPD nas relações consumeristas e a definição da responsabilidade civil dos agentes de tratamento de dados na seara do Código Civil e do CDC. O desenvolvimento deste trabalho também proporcionou apontar como o ordenamento jurídico brasileiro atual responsabiliza os agentes de tratamento de dados que descumprem a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Na análise da pertinência da LGPD nas relações de consumo, notou-se que se faz necessária a referida lei. Afinal, antes dela, não

84 SHIMABUKURO, *op. cit.*

85 *Idem*.

existia diploma específico que regulamentasse de modo minucioso os regimes de gestão de dados pessoais que são frequentemente violados. Identificou-se, ainda, a vulnerabilidade do titular de dados frente à LGPD, haja vista que este agente não possui conhecimentos técnicos e jurídicos significativos que lhe oportunizem ter voz ativa no cenário digital. Assim, aumentam consideravelmente as incidências de práticas abusivas, sobretudo no que concerne aos dados pessoais. Diante disso, a LGPD implementou um método de política de autorização e consentimento dos dados que visa reduzir esse grau de vulnerabilidade do titular de dados.

O trabalho concluiu que a lei foi omissa ao não estabelecer se a responsabilidade civil dos agentes de tratamento de dados pessoais é subjetiva ou objetiva. Com a finalidade de preencher essa lacuna, o estudo observou que, devido à condição de vulnerabilidade e riscos a que o titular de dados é exposto, além da superioridade dos produtores e prestadores de serviços, deve-se aplicar a responsabilidade objetiva, em regra, e a subjetiva como exceção.

Recomenda-se que a pesquisa se amplie, de maneira a promover ações no cumprimento da legislação de proteção de dados, tornando-a cada vez mais efetiva. Para que isso ocorra, requisitam-se algumas ações, tais como o preenchimento de lacunas acerca do tipo de responsabilidade civil dos controladores e operadores de dados pessoais na nova LGPD e a alteração na Política de Privacidade das empresas para uma linguagem menos formal e de fácil compreensão por parte dos consumidores, com o objetivo de reduzir a sua vulnerabilidade.

Por fim, urge que mais estudos sejam realizados no sentido de aprofundar os conhecimentos a respeito dos impactos da Lei Geral de Proteção de Dados após a sua vigência.

Referências

ALVES, Victor Hugo Pérez. *Direitos da Personalidade e a proteção de dados pessoais nos contratos de consumo*. 2008. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2008.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e o limite do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. Lei nº 2.848, de 7 de dezembro de 1940. Institui o Código Penal. *Diário Oficial da União*: seção 1, Brasília, DF, dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 14 abr. 2020.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, ano 128, n. 176, p. 17271, 12 set. 1990. Disponível em: http://www.planalto.gov.br/Ccivil_03/leis/L8078. Acesso em: 1 maio 2020.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. *Diário Oficial da União*: seção 1, Brasília, DF, ano 148, n. 111, p. 2-3, 10 jun. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.
Acesso em: 15 abr. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 7 abr. 2020.

BRASIL. Lei nº 14.058, de 17 de setembro de 2020. Dispõe sobre a conversão da Medida Provisória nº 959 de 2020. *Diário Oficial da União*: seção 1, Brasília, DF, ano 158, n. 180, p. 1, 18 set. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L14058. Acesso em: 19 dez. 2020.

BRASIL. *Proposta de Emenda à Constituição nº 17, de 2019*. Brasília, DF: Senado Federal, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 10 abr. 2020.

BRUNO, Giovana Pizzato. *A proteção de dados pessoais na internet no Brasil*: regime jurídico e responsabilidade dos agentes sob a ótica da Lei nº 13.709 de 14 de agosto de 2018. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Antônio Eufrásio de Toledo, Presidente Prudente, 2019.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. *Âmbito Jurídico*, Rio Grande, v. 15, n. 99, 2012.

CAVALIERI FILHO, Sergio. *Programa de responsabilidade civil*. 14. ed. São Paulo: Atlas, 2020.

COÊLHO, Amanda Carmen Bezerra. *A Lei Geral de Proteção de Dados Pessoais brasileira como meio de efetivação dos direitos da personalidade*. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal da Paraíba, João Pessoa, 2019.

COTS, Marcio. A Lei Geral de Proteção de Dados no e-commerce. *E-commerce Brasil*, [*s. l.*], 2018. Disponível em: https://www.ecommercebrasil.com.br/artigos/lei-geral-de-protecao-de-dados-e-commerce-2/. Acesso em: 25 mar. 2020.

DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro*: responsabilidade civil. 32. ed. São Paulo: Saraiva, 2018. v. 7.

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

GUIMARÃES, Deocleciano Torrieri. *Dicionário técnico jurídico*. 19. ed. Volume único. São Paulo: Rideel, 2016.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 445-463.

LEME, Carolina da Silva. Proteção e tratamento de dados sob o prisma da legislação vigente. *Revista Fronteiras Interdisciplinares do Direito*, [*s. l.*], v. 1, n. 1, p. 178-197, 2019.

LIMBERGER, Têmis. O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais. *Revista Brasileira de Direitos Fundamentais*, Porto Alegre, v. 4, n. 11, 2010.

LONGHI, João Victor Rozatti; MARTINS, Guilherme Magalhães. Impactos positivos da nova lei brasileira de proteção de dados. *Jota*, [*s. l.*], 27 ago. 2018. Disponível em: www.jota.info/opiniao-e-analise/artigos/protecao-dados-impactos-27082018. Acesso em: 6 maio 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019.

MASSON, Cleber. *Direito penal esquematizado*: vol. 3: parte especial. 6. ed. Rio de Janeiro: Forense; São Paulo: Método, 2016, v. 3.

MECABÔ, Alex. Postergação da vigência da LGPD: um remédio necessário?. *Conjur*, [*s. l.*], 1 maio 2020. Disponível em: https://www.conjur.com.br/2020-mai-01/direito-civil-atual-postergacao-vigencia-lei-geral-protecao-dados-remedio-necessario. Acesso em: 25 maio 2020.

MELO, Marco Aurélio Bezerra. *Curso de Direito Civil*: responsabilidade civil. São Paulo: Atlas, 2015. v. 4.

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

MENDONÇA, Renata. Como os testes de Facebook usam seus dados pessoais – e como empresas ganham dinheiro com isso. *BBC Brasil*, São Paulo, 22 fev. 2018. Disponível em: http://www.bbc.com/portuguese/salasocial-43106323. Acesso em: 27 mar. 2020.

MIRANDA, Marcelo. *Lei Geral de Proteção de Dados* – LGPD. 2019. [*S. l.: s. n.*], 2019. Disponível em: https://www.academia.edu/40367651/Lei_Geral_de_Prote%C3%A7%C3%A3o_de_Dados_-LGPD. Acesso em: 25 mar. 2020.

MONTEIRO, Yasmin Sousa. *A efetividade dos mecanismos de proteção de dados pessoais na Lei 13.709/2018*. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, DF, 2019.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, p. 159-180, 2018.

NOVAES E SOUSA ADVOGADOS ASSOCIADOS. A vulnerabilidade do consumidor no e-commerce. *Jusbrasil*, [*s. l.*], 2016. Disponível em: https://novaesesousa.jusbrasil.com.br/artigos/418476350/a-vulnerabilidade-do-consumidor-no-e-commerce. Acesso em: 24 mar. 2020.

OLIVEIRA, José Eduardo. *Responsabilidade civil dos agentes de proteção de dados no Brasil*. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal da Paraíba, Santa Rita, 2019.

OLIVEIRA, Tassyara Onofre de. *Gestão de dados pessoais*: uma análise de casos concretos a partir do ordenamento jurídico brasileiro. 2017. Dissertação (Mestrado em Gestão nas Organizações Aprendentes) – Universidade Federal da Paraíba, João Pessoa, 2017.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais*: Comentários à Lei nº 13.709/2018. São Paulo: Saraiva, 2018.

PRIVACIDADE Hackeada. Direção: Jehane Noujam e Karin Amer. New York: The Othrs, 2019. 1 vídeo (139 min).

ROTUNDO, Rafael Pinheiro. Proteção de dados. *Revista de Direito Privado*, São Paulo, v. 18, n. 74, p. 133–158, 2017.

SÁ JUNIOR, Sergio Ricardo C. *A regulação jurídica da proteção de dados pessoais no Brasil*. 2019. Trabalho de Conclusão de Curso (Especialização em Direito) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2019.

SAUAIA, Hugo Moreira Lima. *A proteção de dados pessoais no Brasil*. Rio de Janeiro: Lumen Juris, 2018.

SHIMABUKURO, Rafael. *Responsabilidade civil na Nova Lei de Proteção de Dados Pessoais*. 2019. Dissertação (Mestrado em Direito) – Centro Universitário Antônio Eufrásio de Toledo, Presidente Prudente, 2019.

SILVA, Bruno Marcos Gomes. Dos agentes de tratamento de dados pessoais. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *LGPD*: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p. 324-325.

SOBRINHO, Nayara. *A proteção de dados pessoais no E-commerce*: análise da aplicação da LGPD diante da vulnerabilidade do consumidor. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Centro Universitário Unifacig, Manhuaçu, 2019.

TARTUCE, Flávio. *Manual de responsabilidade civil*: volume único. Rio de Janeiro: Forense; São Paulo: Método, 2018. Versão digital.

UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, Luxembourg, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 21 fev. 2020.

ZANON, João Carlos. *Direito à proteção dos dados pessoais*. 2012. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2012.

SOBRE OS AUTORES

Bárbara Veiga Góes
Advogada. Pós-Graduanda em Direito Digital pela Universidade Salvador. Graduada em Direito pela Universidade Católica do Salvador. E-mail: barbaragoes1903@gmail.com

Daniel de Araújo Paranhos
Mestrando em Direitos Fundamentais, Cultura e Relações Sociais pela Universidade Federal da Bahia. Membro do grupo de pesquisa Autonomia e Direito Civil contemporâneo. *E-mail:* daniel.paranhos1@gmail.com

Diego Carneiro Costa
Mestre em Direito pela Universidade Federal da Bahia. Pesquisador do Grupo de Pesquisa Direito e Sexualidade. Membro do Grupo de Pesquisa Autonomia e Direito Civil contemporâneo. Analista Judiciário no Tribunal Regional do Trabalho da 5ª Região. *E-mail:* diegcost@gmail.com.

Edilton Meireles
Possui Pós-Doutorado pela Faculdade de Direito da Universidade de Lisboa. Doutor em Direito pela Pontifícia Universidade Católica de São Paulo. Desembargador do Trabalho no Tribunal Regional do Trabalho da 5ª Região. Professor adjunto da Universidade Católica do Salvador e professor associado da Faculdade de Direito da Universidade Federal da Bahia. *E-mail:* edilton_meireles@uol.com.br

Fernanda Rêgo Oliveira Dias
Mestranda em Direito pela Universidade Federal da Bahia, na linha de pesquisa "Direitos fundamentais, cultura e relações sociais". Membro

do grupo de pesquisa "Autonomia e Direito Civil contemporâneo". LLM em Direito empresarial pela Fundação Getulio Vargas. Graduada pela UFBA. Advogada. *E-mail:* rego@regosampaioandrade.com.br

Fernando Araújo dos Santos
Graduando em Direito pela Universidade Federal da Bahia. Membro do grupo de pesquisa "Autonomia Privada e Direito Civil Contemporâneo". *E-mail:* araujonando.santos@gmail.com

Jéssica Andrade Modesto
Mestranda em Direito Público pela Universidade Federal de Alagoas. Graduada em Direito pela Universidade Federal de Alagoas. Advogada. Servidora Pública Federal. *E-mail:* jessicaandrademodesto@hotmail.com

Laércio Martins
Doutorando em Direito pela Faculdade Nacional de Direito da Universidade Federal do Rio de Janeiro. Advogado e Professor de Direito do Centro Universitário de Goiatuba. *E-mail:* lalorj@gmail.com

Laura Lucia da Silva Amorim
Doutoranda em Direito pelo Doutorado Interinstitucional da Universidade Federal da Bahia, linha de pesquisa "Direitos fundamentais, cultura e relações sociais". Pesquisadora no projeto de pesquisa "Proteção de dados pessoais", coordenado pelo Prof. Dr. Maurício Requião. Doutora em Ciências Jurídicas e Sociais pela Universidad del Museo Social Argentino. Mestre em direito pela Universidade de Caxias do Sul. Especialista em Mediação e Arbitragem. Professora de Direito da Faculdade Pio Décimo em Aracaju(SE). E-mail: llsamorim@hotmail.com

Lorena Esquivel de Brito
Advogada. Graduada em Direito pelo Centro Universitário Jorge Amado. Pós-Graduada em Contratos e Direito do Consumidor pelo Centro de Direito do Consumo da Universidade de Coimbra. Mestre em Ciências

Jurídico-Forenses pela Universidade de Coimbra. Doutoranda no Programa de Pós-graduação em Direito da Universidade Federal da Bahia, linha de pesquisa "Direitos Fundamentais, cultura e relações sociais". Membro do Grupo de Pesquisa "Autonomia e Direito Civil contemporâneo" do Programa de Pós-Graduação em Direito da UFBA. *E-mail:* lorenabritoadv@gmail.com

Marcos Ehrhardt Jr.
Doutor em Direito pela Universidade Federal de Pernambuco. Professor de Direito Civil da Universidade Federal de Alagoas e do Centro Universitário CESMAC. *E-mail:* contato@marcosehrhardt.com.br

Maria Clara Seixas
Advogada. Mestranda na linha de pesquisa "Direitos Fundamentais, cultura e relações sociais" e membra do grupo de pesquisa "Autonomia e Direito Civil contemporâneo" da Faculdade de Direito da Universidade Federal da Bahia. Pós-graduada pela Fundação Getúlio Vargas de São Paulo. Especialista Executiva pelo Insper. Diretora e Professora da ONG Projeto Constituição nas Escolas. Professora de *Compliance*, Riscos e Governança da Pós-graduação da Faculdade Baiana de Direito. *E-mail:* mariaclara@4s.adv.br

Marta Carolina Giménez Pereira
Doutora em Direito pela Universidade Autônoma do México. Possui pós-doutorado em Direito pela Faculdade Meridional. Professora visitante no Programa de Pós-graduação em Direito na Universidade Federal da Bahia (UFBA). Líder do Grupo de Pesquisa em Propriedade Intelectual e Novas Tecnologias da UFBA. *E-mail*: magipe@hotmail.com

Maurício Requião
Doutor em Direito. Professor de Direito Civil na Faculdade de Direito da Universidade Federal da Bahia e na Faculdade Baiana de Direito. Líder do grupo de pesquisa "Autonomia e Direito Civil contemporâneo". Advogado. *E-mail:* maurequiao@gmail.com

Mayana Barbosa Oliveira
Mestranda do Programa de Pós-Graduação em Propriedade Intelectual e Transferência e Tecnologia para a Inovação Mediadora e árbitra credenciada perante o Ministério da Cultura para atuação na resolução de conflitos relativos a Direitos Autorais. Membro do Grupo de Pesquisa Propriedade Intelectual e Novas Tecnologias. *E-mail:* mayanabarbosaoliveira@gmail.com

Rafael da Silva Santana
Advogado. Pós-Graduado, *lato sensu*, em Direito Processual Civil pela Faculdade Baiana de Direito. Mestre e doutorando pela Universidade Federal da Bahia. Membro do grupo de pesquisa Autonomia e Direito Civil Contemporâneo. *E-mail:* rssantana.adv@gmail.com

Rafaela Lamêgo e Aquino Rodrigues de Freitas
Graduanda em Direito pela Universidade Federal da Bahia. Bolsista de iniciação científica Programa Institucional de Bolsas de Iniciação Científica (Pibic)/Fundação de Amparo à Pesquisa do Estado da Bahia (Fapesb), orientada pelo Prof. Dr. Maurício Requião. Membro do grupo de pesquisa Autonomia e Direito Civil Contemporâneo. *E-mail:* rafafreitas2509@gmail.com

Rodrigo Castro Nascimento
Aluno do programa de Doutorado da Universidade Federal da Bahia, na linha de pesquisa "Direitos fundamentais, cultura e relações sociais". Membro do grupo de pesquisa "Autonomia e Direito Civil contemporâneo" da Universidade Federal da Bahia. *E-mail:* rodrigocnster@gmail.com

Salvador Morales Ferrer
Doctor en Derecho por el programa de Estudios Jurídicos, Ciencia Política y Criminología de la Universidad de Valencia, con la calificación Apto Cum Laude. Doctor Honoris Causa por el Claustro Nacional de Doctores de México (Unam). Certificado-Diploma de Estudios

Avanzados TERCER CICLO – DOCTORADO por la Universidad Cardenal Herrera CEU de Valencia. Certificado de Aptitud Profesional realizado en la Escuela de Práctica Jurídica del Ilustre Colegio de abogados de Alzira. Máster Propio en Mediación y Gestión Eficiente de Conflictos por la Universidad Cardenal Herrera-Ceu (Valencia). Certificado de Aptitud Pedagógica por la Universidad de Valencia. Miembro Investigador del ILUSTRE COLEGIO DE ABOGADOS DE ALZIRA. Profesor Colaborador de la Universidad Federal de Bahía UFBA. *E-mail*: salvadormorales@icaalzira.com.

Teila Rocha Lins D'Albuquerque
Professora de Direito Civil e Direito do Consumidor da Universidade Católica do Salvador. Mestre em Relações Sociais e Novos Direitos pela Universidade Federal da Bahia. Doutoranda em Direito pela UFBA. Mestre em Políticas Sociais e Cidadania pela Universidade Católica do Salvador. Especialista em Direito do Trabalho e Processo do Trabalho pela UFBA. Membro dos grupos de pesquisa "Autonomia e Direito Civil contemporâneo" e "Privacidade e Proteção de dados na era digital", da Universidade Federal da Bahia. Advogada e parecerista. *E-mail*: teilarocha.adv@gmail.com; teilarocha.adv@gmail.com

Wendel Machado de Souza
Advogado e consultor jurídico. Mestrando pelo Programa de Pós-graduação em Direito da Universidade Federal da Bahia. Integrante do grupo de pesquisa "Autonomia e Direito Civil contemporâneo". *E-mail:* wendel@mmladvocacia.com

Formato: 17 x 24 cm
Fontes: Aribau Grotesk, Merriweather
Extensão digital: PDF

Maurício Requião.

Doutor em Direito. Professor em Direito Civil na Faculdade de Direito da Universidade Federal da Bahia e na Faculdade Baiana de Direito. Líder do grupo de pesquisa "Autonomia e Direito Civil contemporâneo". Advogado.

ISBN 978-65-5630-363-5

CAPES

A **Série Professor Edvaldo Brito** é composta por obras organizadas por professores do Programa de Pós-Graduação stricto sensu em Direito da Universidade Federal da Bahia (PPGD/UFBA) e conta com a contribuição de artigos de seus docentes, discentes e egressos. Egresso do PPGD, integrante do seu corpo docente há mais de 40 anos e seu ex-coordenador, Edvaldo Brito foi professor de boa parte dos organizadores dos volumes da coleção. A história do PPGD/UFBA está tão entrelaçada com a trajetória acadêmica do professor Edvaldo Brito que uma amostra representativa da produção intelectual deste programa não poderia deixar de portar o nome de tamanha referência no desenvolvimento de altos estudos nos âmbitos do Direito Tributário, do Direito Constitucional e do Direito Civil.

Ricardo Maurício Freire Soares
Coordenador PPGD/UFBA 2021

Daniel Oitaven Pearce Pamponet Miguel
Coordenador PPGD/UFBA 2021-2023