UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE DIREITO
MARIA REGINA DETONI CAVALCANTI RIGOLON KORKMAZ

DADOS SENSÍVEIS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS:
mecanismos de tutela para o livre desenvolvimento da personalidade

Juiz de Fora
2019

MARIA REGINA DETONI CAVALCANTI RIGOLON KORKMAZ

DADOS SENSÍVEIS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS:
mecanismos de tutela para o livre desenvolvimento da personalidade

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Mestra no Mestrado em Direito e Inovação, sob orientação do Prof. Dr. Sergio Marcos Carvalho de Ávila Negri.

Juiz de Fora
2019

Ficha catalográfica elaborada através do programa de geração
automática da Biblioteca Universitária da UFJF,
com os dados fornecidos pelo(a) autor(a)

Rigolon Korkmaz, Maria Regina Detoni Cavalcanti.
Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais : mecanismos de tutela para o livre desenvolvimento da personalidade / Maria Regina Detoni Cavalcanti Rigolon Korkmaz. -- 2019.
118 p.

Orientador: Sergio Marcos Carvalho de Ávila Negri
Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Faculdade de Direito. Programa de Pós-Graduação em Direito, 2019.

1. Proteção de dados. 2. Privacidade. 3. Dados Sensíveis. 4. Dignidade. I. Negri, Sergio Marcos Carvalho de Ávila, orient. II. Título.

FOLHA DE APROVAÇÃO

MARIA REGINA DETONI CAVALCANTI RIGOLON KORKMAZ

DADOS SENSÍVEIS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: mecanismos de tutela para o livre desenvolvimento da personalidade

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Mestra no Mestrado em Direito e Inovação, submetida à Banca Examinadora composta pelos membros:

Orientador: Prof. Dr. Sergio Marcos Carvalho de Ávila Negri
Universidade Federal de Juiz de Fora

Prof. Dr. Danilo Cesar Maganhoto Doneda
Instituto Brasiliense de Direito Público

Prof. Dr. Marcos Vinício Chein Feres
Universidade Federal de Juiz de Fora

PARECER DA BANCA

( ) APROVADA

( ) REPROVADA

Juiz de Fora, 22 de novembro de 2019

AGRADECIMENTOS

Nada realizamos sozinhos. Durante a nossa trajetória são diversas as pessoas, próximas ou não, que colaboram para o nosso desenvolvimento, seja através da ajuda ou mesmo das dificuldades a nos avaliarem. Acima de tudo, em mais uma etapa concluída, meu coração se enche de alegria e gratidão a Deus e a Jesus pelo tanto que recebi, pelas oportunidades de buscar sempre a minha superação e de fazer mais felizes aqueles que me cercam. Sem essa compreensão, a vida seria pequena, quando tenho certeza da sua grandeza diante da eternidade.

Agradeço aos meus pais, Vicente e Isabel, por todo o amor que sempre me cercaram e por serem verdadeiros entusiastas desde que eu era pequena. Ao meu irmão, Antônio Netto, pela amizade que sempre se esforçou por estar presente. À minha irmã e filha do coração, Maria Fernanda, por ser uma grande companheira e por trazer as sutilezas de uma criança para o meu dia. Aos meus queridos avós, por toda a dedicação.

Agradeço ao meu marido, Tharek, pelo apoio incondicional e por compartilhar comigo os ideais mais sublimes.

Agradeço ao meu orientador, Sergio Negri, por todo o aprendizado e orientação que foram fundamentais para a minha trajetória acadêmica.

Agradeço à Universidade Federal de Juiz de Fora (UFJF), à Faculdade de Direito da UFJF e ao Programa de Pós-graduação *Stricto Sensu* em Direito e Inovação da UFJF pela oportunidade do desenvolvimento acadêmico.

Por fim, agradeço a todos os educadores que estiveram presentes na minha vida, particularmente àqueles que me inspiram no propósito da educação como libertação da ignorância. O conhecimento liberta e, no fundo, todos nós buscamos a verdade.

"Ótimo homem, tu que és cidadão de Atenas, da cidade maior e mais famosa pelo saber e pelo poder, não te envergonhas de fazer caso das riquezas, para guardares quanto mais puderes e da glória e das honrarias, e, depois, não fazer caso e nada te importares da sabedoria, da verdade e da alma, para tê-la cada vez melhor?"

Sócrates

RESUMO

O livre desenvolvimento da personalidade se relaciona cada vez mais com os avanços tecnológicos que são associados a um processo de fragmentação da pessoa em dados pessoais. Enquanto representação da personalidade, os dados pessoais ganham progressiva importância para diversas estruturas na sociedade, na medida em que cresce a capacidade de extração de valor dos dados. A proteção dos dados pessoais passa a ser um conceito central para a privacidade, embora a ela não se limite por também assumir um paradigma objetivo e coletivo, como forma de tutelar valores compartilhados socialmente. Como referência teórica, parte-se da percepção de Stefano Rodotà de que entre os dados pessoais ganha relevo os dados sensíveis, caracterizados pela potencialidade discriminatória e por se associarem ao princípio da igualdade material. Em vista da centralidade da pessoa humana no ordenamento jurídico do Brasil, o presente estudo teve por fim compreender, a partir de uma análise predominantemente qualitativa, os mecanismos de tutela estabelecidos para os dados sensíveis na Lei Geral de Proteção de Dados Pessoais – n.º 13.709 de 2018. Para tanto, foi desenvolvida uma abordagem comparativa com o regime jurídico geral dos dados pessoais com o propósito de verificar se a tutela oferecida aos dados sensíveis é significativamente mais protetiva. O Regulamento Europeu de Proteção de Dados Pessoais foi utilizado em caráter complementar para a investigação. Apesar do reconhecimento de limitações na categorização dos dados sensíveis, foram identificados seis mecanismos de tutela específicos, a saber, o consentimento mais qualificado, hipóteses autorizativas restritas para o tratamento dos dados, a extensão do regime jurídico dos dados sensíveis para o tratamento sensível de dados pessoais, a possibilidade de limitação do uso compartilhado de dados sensíveis para fins econômicos pela Autoridade Nacional de Proteção de Dados, limitações adicionais ao tratamento de dados sensíveis referentes à saúde e a referência a padrões técnicos especiais de segurança e sigilo para os dados sensíveis. Conclui-se a presente investigação ao se corroborar a hipótese inicial de que a Lei Geral de Proteção de Dados Pessoais estabelece um regime jurídico significativamente mais protetivo que o regime geral dos dados pessoais, a se erigir como um vetor importante para a concretização da tutela da pessoa a partir dos seus dados no cenário brasileiro.

Palavras-chave: Proteção de dados. Privacidade. Dados Sensíveis. Dignidade.

ABSTRACT

The free development of the personality is increasingly related to technological advances that are associated to a fragmentation process of the person in personal data. Whereas represent personality, personal data gains progressive importance for various structures in the society, as the capacity for extracting value from data increases. The protection of personal data becomes a central concept to privacy, although not limited to it, considered its objectivity and collective paradigm as a protection form of socially shared values. As theoretical reference, we start from Stefano Rodotà's perception that among personal data are highlighted the sensitive data, characterized by the discrimination potential and for being associated with the principle of material equality. Given the centrality of the person in the Brazil's legal framework, the purpose of this research was to understand, based on a predominantly qualitative analysis, the safeguard mechanisms for sensitive data provided by the Brazilian General Law on Data Protection – law n. º 13.709 of 2018. Therefore, we developed a comparative approach to the general framework of personal data in order to verify if the protection offered to sensitive data is significantly more protective. The European General Data Protection Regulation has been used complementarily to the research. Despite the recognition of limitations in the sensitive data categorization, six specific safeguards mechanisms were identified, which are a more qualified consent, restricted legal authorizations for processing sensitive data, the extension of the sensitive data framework for the processing of personal data that can reveal sensitive data, the possibility of limitations at shared use of sensitive data for economic purposes by the Data Protection Authority, additional limitations for processing sensitive data related to health and special technical standards of security and confidentiality for sensitive data. The investigation is concluded by corroborating the initial hypothesis that the Brazilian General Law on Data Protection establishes a sensitive data framework significantly more protective than the general framework, contributing as an important vector for the fullfilment of the protection of the person in relation to its data in the Brazilian scenario.

Keywords: *Data protection. Privacy. Sensitive data. Dignity.*

LISTA DE ABREVIATURAS E SIGLAS

AI	*Artificial intelligence*
Art.	Artigo
ANPD	Autoridade Nacional de Proteção de Dados
CDC	Código de Defesa do Consumidor
COPPA	*Children's Online Privacy Protection Act*
CRFB	Constituição da República Federativa do Brasil
EUA	Estados Unidos da América
GDPR	*General Data Protection Regulation*
HIV	*Human Immunodeficiency Virus*
IBM	*International Business Machines*
IA	Inteligência artificial
IoT	*Internet of things*
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
n.º	Número
NIC.BR	Núcleo de Informação e Coordenação do Ponto BR
p.	Página (s)
PET	*Privacy Enhancing Technologies*
TI	Tecnologia da Informação
TIC	Tecnologias da Informação e Comunicação

LISTA DE SÍMBOLOS

§	Parágrafo
%	Porcentagem

SUMÁRIO

1 INTRODUÇÃO

O desenvolvimento da personalidade humana se relaciona cada vez mais com a evolução da tecnologia. A ideia de progresso promove uma inserção crescente das Tecnologias da Informação e Comunicação (TIC) na realidade social, modificando-a. Inúmeras são as transformações verificadas: a internet passa a se caracterizar pela ubiquidade, as interações sociais são redefinidas, as distâncias são diminuídas, a memória individual e coletiva são ressignificadas e o corpo da pessoa deixa de se restringir à materialidade.

A personalidade, enquanto valor da pessoa que caracteriza o ordenamento jurídico e garante a sua unidade, como define Perlingieri (2005), depara-se com desafios para alcançar a sua plena realização no cenário em que os avanços tecnológicos, que ostentam uma imprevisibilidade intrínseca e desprezam limites extrínsecos (DONEDA, 2006), se associam a um processo de fragmentação da pessoa que passa a ser reduzida a dados, com contradições diante da possibilidade de ampliar ou reduzir o conceito de pessoa (RODOTÀ, 2004, 2012). As múltiplas potencialidades geradas com base nos dados pessoais tornam, no mínimo, obsoleta a defesa da transparência de quem não tem nada a temer.

Segundo Rodotà (2005, p. 25), "as tecnologias da informação não apenas tomam conta de nossas vidas, mas constroem um corpo eletrônico, o conjunto de nossas informações pessoais armazenadas em bancos de dados sem fim, que vive ao lado do corpo físico".[1] Enquanto representação direta da personalidade, os dados pessoais devem ser compreendidos como sua extensão (DONEDA, 2006), constitutivos do corpo eletrônico da pessoa.[2]

Se a alegação de que "nós somos os nossos dados" pode parecer reducionista e perigosa, o nexo que se estabelece entre o corpo da pessoa, as suas informações e o controle social pode tomar contornos dramáticos, com o imperativo de recorrer à dignidade humana (RODOTÀ, 2004). Vale dizer, a unidade da pessoa somente pode ser reconstituída com a ampliação ao corpo eletrônico das garantias elaboradas para o corpo físico (RODOTÀ, 2004).

No paradigma da Quarta Revolução Industrial, a tecnologia passa a promover a fusão das esferas física, digital e biológica, e a informação ganha cada vez mais valor (SCHWAB,

---

[1] Tradução livre de: "Le tecnologie dell'informazione non solo si impadroniscono della nostra vita, ma costruiscono un corpo elettronico, l'insieme delle nostre informazioni personali custodite in infinite banche dati, che vive accanto al corpo fisico".

[2] Não se deve considerar apenas o corpo que se constitui em uma perspectiva física e em outra eletrônica que se entretecem continuamente: percebe-se um corpo multiplicado e distribuído, que primeiro perdeu sua unidade, a qual foi decomposta em órgãos, células, gametas, depois perdeu sua materialidade, tornando-se uma senha, com as impressões digitais, DNA, geometria do corpo, entre outros, pela sua acepção eletrônica (RODOTÀ, 2004).

2016). São diversas as implicações econômicas, políticas e sociais. A hiperconectividade[3] redimensiona expressão da personalidade a partir dos dados e o conceito *data driven economy* é significativo da atual fase do capitalismo baseado na extração de dados pessoais (FRAZÃO, 2019a).[4]

Apontados como o novo petróleo (THE ECONOMIST, 2017),[5] os dados são o insumo para várias tecnologias e na lógica do mercado a fragmentação em dados potencializa uma nova versão de abstração da pessoa, que passa a constituir matéria prima, na forma de dados, produto, porque comercializável, e destinatária da cadeia de consumo, diante da paradoxal "hiperpessoalização" do serviço com base nos dados pessoais (SCHULMAN, 2016).[6] A disponibilização da Calculadora do *Financial Times* para atribuir um preço aos dados pessoais é ilustrativa dessa conjuntura (STEEL, 2013).

Nesse cenário, os dados emergem como um forte ativo dos novos tempos, também apontados como o novo ouro, que igualmente demanda um novo tipo de mineração, a partir da qual empresas se especializam em processos de obtenção, análise e comercialização dos dados (SCHULMAN, 2016). Na síntese de Rodotà (2004, p. 93), o corpo se revela como "verdadeira mina a céu aberto". Os dados pessoais apresentaram-se como meio para o desenvolvimento de estratégias de longo prazo voltadas a revelar causalidades, determinar medidas e corrigir ou direcionar comportamentos, o que se aplica a questões de segurança, saúde, seguros, *marketing*, entre outros (SIMITIS, 2010). Em outra perspectiva, aspectos existenciais da pessoa representam um forte eixo de interesses patrimoniais.

No âmbito político, a vigilância a partir dos dados tem exemplo emblemático no *Social Credit Score* e na conjectura da utilização dos dados pessoais para substituir o debate público na China (LARSON, 2018). No mundo ocidental, a gravidade do uso abusivo de dados pessoais

---

[3] O termo hiperconectidade tem desdobramentos importantes como o estado de conexão e acesso constante das pessoas, a multiplicidade de informações, a interatividade e o armazenamento ininterrupto de dados, o que pode se dar nas comunicações entre indivíduos (*person-to-person*, P2P), indivíduos e máquina (*human-to-machine*, H2M) e entre máquinas (*machine-to-machine*, M2M) (MAGRANI, 2018).

[4] "By collecting more data, a firm has more scope to improve its products, which attracts more users, generating even more data, and so on. The more data Tesla gathers from its self-driving cars, the better it can make them at driving themselves—part of the reason the firm, which sold only 25,000 cars in the first quarter, is now worth more than GM, which sold 2.3m. The giants' surveillance systems span the entire economy: Google can see what people search for, Facebook what they share, Amazon what they buy" (THE ECONOMIST, 2017, sem paginação).

[5] As empresas apontadas como as mais valiosas do mundo exploram a informação, ainda que de formas distintas. Como noticia o The Economist (2017, sem paginação): "These titans—Alphabet (Google's parent company), Amazon, Apple, Facebook and Microsoft—look unstoppable. They are the five most valuable listed firms in the world. Their profits are surging: they collectively racked up over $25bn in net profit in the first quarter of 2017. Amazon captures half of all dollars spent online in America. Google and Facebook accounted for almost all the revenue growth in digital advertising in America last year".

[6] Clavell (2015) reporta a atividade de algumas empresas no sentido de explorar a possibilidade de se tornarem *data brokers* dos cidadãos, uma espécie de corretores de dados.

é exemplificada com o conhecido escândalo da *Cambridge Analytica*, revelado em março de 2018 pelo *The Guardian*.[7] Para além da proteção da pessoa individualmente considerada, a proteção de dados assume um paradigma coletivo, como medida de proteção de diversos valores compartilhados socialmente, a exemplo da própria democracia.[8]

Entre as implicações sociais, a internet redefiniu as estruturas de comunicação e, na medida em que incorporou no seu âmbito a utilização de estratégias de mercado, trocas de experiências, exposição de hábitos pessoais, entre outros, trouxe cada vez mais para a sua esfera o processamento de dados (SIMITIS, 2010). A ampla utilização das redes sociais e a divulgação de informações da personalidade parecem representar uma nova forma de compreender o conteúdo de esfera privada da pessoa (TEFFÉ; MORAES, 2017).

A tecnologia, na medida em que ajuda a moldar uma esfera privada mais rica, torna essa esfera privada mais frágil (RODOTÀ, 2008). A pessoa progressivamente desloca eixos da sua experiência para rede, consequentemente deixando traços que se convertem em dados pessoais e, em última análise, podem vir a ser instrumentalizados para atender a interesses heterônomos. Esse processo toma contornos ainda mais desafiadores com a *Web* 3.0[9] e a partir da identificação de uma coleta pulverizada de dados no tecido social. Exemplificativa desse processo é a Internet das Coisas (em inglês, *Internet of Things*, sigla IoT).[10]

---

[7] A empresa *Cambridge Analytica* se associou à chamada *Global Science Research*, de Aleksandr Kogan, um pesquisador do departamento de psicologia da Universidade de Cambridge. Aleksandr Kogan havia desenvolvido um aplicativo, chamado "*My Digital Life*", através do *Facebook* para coletar dados e traçar perfis das pessoas que o utilizavam e da sua rede de amigos, sem que esses últimos houvessem consentido com a prática (CADWALLADR; GRAHAM-HARRISON, 2018). A partir de uma coleta ostensiva de dados, além do necessário para a operação do aplicativo em si, foi possível desenvolver perfis psicométricos das pessoas com o fim de enviar propaganda política extremamente personalizada (CADWALLADR; GRAHAM-HARRISON, 2018). O caso foi revelado pelo *The Guardian* a partir da delação de Wylie, que afirmou o objetivo de moldar a opinião pública americana na última eleição presidencial nos Estados Unidos (CADWALLADR; GRAHAM-HARRISON, 2018). A *Federal Trade Comission* nos Estados Unidos aplicou em julho deste ano uma multa de 5 bilhões de dólares ao *Facebook* pela violação da política de privacidade dos seus usuários (POZZI, 2019).

[8] A título de exemplo, no uso de plataformas e redes sociais é possível identificar uma "censura de segunda ordem", com a manipulação da curadoria, do contexto e do fluxo de informações e de atenção para a construção de "bolhas" individualizadas e voltadas a um determinado fim (PARISER, 2012). Os dados pessoais exercem um papel fundamental nessas práticas.

[9] O desenvolvimento da internet é caracterizado por três eras: a *Web* 1.0, a primeira delas, surgida na década de 1980, se definiu pela possibilidade de conexão entre pessoas, mas de forma estática e sem interatividade com os sites, estes criados apenas para a leitura e disponibilização de informações, em sentido amplo; a *Web* 2.0 é marcada pela grande interatividade proporcionada nas suas plataformas, além da colaboratividade; a *Web* 3.0 é sinalizada pelo cruzamento de dados, bem como o estabelecimento de novos pontos de conexão, dela fazendo parte a Internet das Coisas (MAGRANI, 2017). Segundo Magrani (2017), o conceito de *Web* 3.0 ainda está em fase de consolidação, mas é possível afirmar o vetor de maior utilização da inteligência artificial para criar uma *web* "mais potente e eficiente", inclusive com a tendência crescente de personalização.

[10] Apesar de fortes divergências conceituais acerca da Internet das Coisas, pode ser compreendida como "um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia" (MAGRANI, 2018, p. 20).

Paralelamente, as potencialidades tecnológicas progressivamente avançam na capacidade de extrair valor dos dados. A evolução da tecnologia operou uma mudança qualitativa nas práticas de tratamento de dados com base em novos métodos, técnicas e algoritmos (DONEDA et. al., 2018).[11] Aliado a esses fatores é possível apontar o *Big Data*[12] que é fonte de poder e se define pela capacidade de megaempresas digitais armazenarem e analisarem dados comportamentais cada vez mais íntimos dos usuários para traçarem perfis de grande valor para o mercado, campanhas políticas, governos ou qualquer interessado em controlar, monetizar e antecipar o comportamento humano (PASQUALE, 2017).

Na era digital, o controle a partir dos dados não tem por fim necessariamente impedir ou desencorajar condutas. À vigilância interessa a repetição de comportamentos para a construção da classificação, de modo a inferir que "a sociedade da vigilância revela-se, progressivamente, como sociedade da classificação" (RODOTÀ, 2008, p. 114). Nesse contexto, o princípio da liberdade individual ganha substância em uma perspectiva de privacidade e de livre construção da esfera privada (MORAES, 2006).

Como anuncia Rodotà (2005, p. 27), sem uma tutela forte das informações, as pessoas estarão sempre mais propensas a serem discriminadas pelas suas opiniões, crenças religiosas, condições de saúde: "a privacidade se apresenta, assim, como um elemento fundamental para a sociedade da igualdade".[13] Para além da privacidade e da proteção de dados pessoais, ganha relevância a tutela dos dados pessoais sensíveis como a defesa do princípio da igualdade material, na medida em que está em questão não somente a esfera privada da pessoa, mas a sua posição na organização social, política e econômica (RODOTÀ, 2008).

Os dados pessoais considerados sensíveis são aqueles associados às opções e características fundamentais da pessoa e, portanto, com uma "potencial inclinação para serem utilizados com finalidades discriminatórias" (RODOTÀ, 2008, p. 96). É com fundamento na possibilidade de 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 protegê-los permite a efetivação de diversos direitos como

---

[11] O termo "algoritmo" não é utilizado neste trabalho no conceito restrito de construção matemática, mas como: "implementation and interaction of one or more algorithms in a particular program, software or information system" (MITTELSTADT et. al., 2016, p. 2).

[12] O *Big Data* é usualmente compreendido a partir de quatro dimensões, o que se convencionou chamar de 4 "Vs": 1) o volume de dados produzidos em alta escala; 2) a velocidade de processamento destes dados a partir das tecnologias disponíveis; 3) a variedade dos dados que viabiliza o seu tratamento para diversos fins; 4) a veracidade dos dados, em vista da sua incerteza e da potencialidade de gerar distorções (INTERNATIONAL BUSINESS MACHINES, 2018b). Questiona-se, ainda, a respeito da existência do quinto "V" referente ao valor dos dados através da possibilidade de alcançar melhores resultados (INTERNATIONAL BUSINESS MACHINES, 2018a).

[13] Tradução livre de: "La privacy si presenta così come un elemento fondamentale della società dell'eguaglianza".

saúde, liberdades comunicativas, religiosa, de associação, entre outros (MULHOLLAND, 2018).

A partir de L. M. Friedman e J. Rosen, Rodotà (2008, p. 15) reconhece que a coleta de dados sensíveis e a aptidão de gerar perfis sociais e individuais discriminatórios indicam para a privacidade como "a proteção de escolhas de vida contra qualquer forma de controle público e estigma social", a implicar na indispensável "reivindicação de limites que protegem o indivíduo do direito de não ser simplificado, objetivado e avaliado fora de contexto". É nesse sentido que os dados sensíveis dão ensejo a uma categoria especial de dados pessoais situados no "núcleo duro" da privacidade (RODOTÀ, 2008).

A proteção de dados emerge como o direito fundamental mais expressivo da condição humana contemporânea (RODOTÀ, 2008),[14] com o imperativo de dirigir o fenômeno informacional para a realização da pessoa através da disciplina da informação (DONEDA, 2006). Assim, em vista da conjugação dos avanços tecnológicos e da necessária proteção da pessoa humana, que se torna mais patente no caso dos dados sensíveis pela associação com o princípio da igualdade, o presente trabalho tem por fim examinar o regime jurídico dos dados sensíveis na Lei Geral de Proteção de Dados Pessoais – Lei n.º 13.709 de 2018, ainda em *vacatio legis*.

A partir de uma pesquisa qualitativa, pretende-se proceder a uma análise da Lei Geral de Proteção de Dados Pessoais (LGPD) com o fim de identificar quais os mecanismos de tutela prescritos especificamente para a categoria dos dados sensíveis e, a partir da sua identificação, verificar se a proteção dos dados sensíveis é substancialmente elevada a um padrão protetivo maior se comparada aos dados pessoais não sensíveis. Apesar da existência de limitações inerentes às regulações de dados pessoais, sobretudo diante do fator tecnológico,[15] como hipótese à pergunta de pesquisa apresentada sugere-se que a LGPD estabelece mecanismos substancialmente mais protetivos para os dados sensíveis, em comparação com os demais dados pessoais. O regime jurídico comum de proteção de dados pessoais será abordado em caráter

[14] A proteção de dados está a caminho de expressamente alcançar o *status* de direito fundamental na Constituição da República Federativa do Brasil através da Proposta de Emenda à Constituição n. 17 (BRASIL, 2019c), muito embora já ostentasse esta natureza com base nas garantias constitucionais da igualdade, liberdade, proteção da intimidade, da vida privada e do objetivo da República consistente na promoção da dignidade humana (BRASIL, 1988). Como observa Schreiber (2019), essa alteração não contribui, de fato, para a construção de uma cultura de proteção de dados no Brasil. De acordo com o autor, o fato da proposta igualmente prever a competência legislativa exclusiva da União a respeito da matéria pode gerar impactos negativos com relação à implementação da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), na medida em que restringirá a atuação de outros entes da federação, inclusive em iniciativas já existentes, o papel normativo da Autoridade Nacional de Proteção de Dados, criada pela Lei 13.853/2019, e dificultará a construção de regulações específicas (SCHREIBER, 2019).

[15] A velocidade da circulação das informações estabelece relação inversamente proporcional com a capacidade de controle, retificação e eliminação dos dados (TEFFÉ; MORAES, 2017).

comparativo com as previsões específicas para os dados sensíveis, de forma que os demais eixos de proteção dos dados pessoais, aplicáveis de maneira geral a todos os dados qualificados como pessoais, não integram propriamente a abrangência deste trabalho.

Para tanto, após esta introdução, no capítulo 2 deste estudo serão apresentadas as diretrizes metodológicas que nortearão o desenvolvimento da pesquisa. No capítulo 3, por sua vez, serão introduzidas as bases teóricas adotadas. Com a centralidade na proteção da pessoa humana na era digital, serão discutidas questões que envolvem a evolução da categoria dos direitos da personalidade até a cláusula geral de tutela e promoção da pessoa, com base na dignidade. Por conseguinte, a partir de um panorama dos novos contornos lançados para o livre desenvolvimento da personalidade, serão apresentadas considerações a respeito da evolução da privacidade até a proteção de dados pessoais.

O capítulo 4 tem por fim endereçar especificamente o tema dos dados sensíveis. Para a compreensão da categoria a partir da experiência jurídica internacional, serão apresentadas as linhas teóricas que envolvem o conceito e o fundamento dos dados sensíveis, caracterizados, de acordo com o paradigma teórico de Rodotà (2005, 2008, 2019), pela potencialidade discriminatória e por se associarem ao princípio da igualdade material. Em seguida, será assinalada a relação que os dados sensíveis estabelecem com diversos direitos fundamentais. Posteriormente, para o desenvolvimento consistente da pesquisa, serão apontadas algumas das críticas relativas à categoria dos dados sensíveis, além de limitações da sua técnica jurídica. Com a finalidade de delinear a relevância da proteção desses dados, serão traçados alguns desafios referentes à potencialidade lesiva do seu tratamento na era digital.

O capítulo 5 tem por referência central a LGPD. A partir de uma análise conceitual dos dados sensíveis na normativa brasileira, serão abordados os mecanismos de tutela específicos desses dados, para além regime comum de dados pessoais, com o fim de verificar o seu *standard* regulatório. Por fim, no capítulo 6 é concluído o trabalho com uma retomada de seu conteúdo e com a apresentação das considerações finais.

2 METODOLOGIA

Partindo do pressuposto de que a metodologia é equiparada a uma preocupação instrumental e que tem por objetivo o aperfeiçoamento dos processos e critérios utilizados na pesquisa, embora não existam regras exaustivas e infalíveis para se investigar (MARTINS E TEÓPHILO, 2016), elegeu-se para a realização da presente pesquisa o método dedutivo, com a predominância de uma análise qualitativa. A adoção de uma perspectiva qualitativa se justifica na medida em que o fenômeno específico a ser estudado, qual seja, a LGPD, diz respeito ao funcionamento de uma estrutura social (MARTINS; TEÓPHILO, 2016), que, em caráter normativo, tem por finalidade regular de forma geral a circulação de dados pessoais no Brasil.

Segundo Martins e Teóphilo (2016), ao longo das pesquisas qualitativas, geralmente, são construídas categorias descritivas, cuja base inicial poderá se dar a partir da plataforma teórica adotada na investigação ou, nos casos em que não é adotado um referencial, o pesquisador terá o desafio de definir as categorias que possam sintetizar ou agrupar conceitos e variáveis para a melhor compreensão do fenômeno. A referência teórica que orientará o desenvolvimento da pesquisa está estabelecida em Stefano Rodotà, que orientará, em última análise, o escopo de agrupar os mecanismos de tutela para os dados sensíveis na LGPD.[16]

Considerando que a LGPD é a primeira norma geral de proteção de dados no Brasil, ainda em *vacatio legis*, é razoável a adoção de uma abordagem exploratória. Para além das diversas alterações legislativas realizadas na LGPD, são depositadas expectativas na constituição e na atuação da Autoridade Nacional de Proteção de Dados (ANPD) no sentido de compreender e aplicar os instrumentos jurídicos previstos na norma. Além disso, a LGPD é estruturada a partir de um modelo regulatório construído na experiência europeia, de forma que a sua efetivação dependerá, a rigor, de uma conformação com a realidade brasileira. A definição do estudo como exploratório, portanto, é importante para proporcionar uma visão geral do problema, como uma etapa fundamental para o desenvolvimento de uma investigação mais ampla, gerando futuras perguntas de pesquisa (GIL, 2008).

Como estratégias de pesquisa científica, ou delineamentos, é relevante destacar a pesquisa bibliográfica direcionada à construção de uma plataforma teórica do estudo, através de fontes secundárias (MARTINS E TEÓPHILO, 2016). O delineamento da pesquisa

[16] "Em pesquisa qualitativa a consistência pode ser checada por meio de exame detalhado entre elementos da plataforma teórica e os achados da investigação" (MARTINS; TEÓPHILO, 2016, p. 143). Esse processo norteará o desenvolvimento do capítulo 5 do presente estudo.

documental também foi utilizado a partir de fontes primárias, com a centralidade na LGPD. Com o fim de compor a pesquisa com outras fontes documentais e contribuir para uma melhor compreensão da normativa a respeito dos dados sensíveis, a pesquisa passa por documentos relevantes que constam do processo legislativo da LGPD. Adicionalmente, procedeu-se a um cotejo com diplomas em nível internacional sobre os dados sensíveis, principalmente com o modelo da União Europeia. Nesse sentido, a pesquisa assumirá um caráter eminentemente comparativo.

A propósito, a facilidade da circulação de dados pessoais em um panorama global evidencia a suscetibilidade da sua normatização a influências exógenas, bem como a sua aptidão de influenciar outras normativas, porque escassa seria a eficácia de iniciativas isoladas e desalinhadas com outras regulações (DONEDA, 2006).[17] A experiência europeia na matéria representa a grande influência exógena na regulação brasileira sobre proteção de dados. Para além dos laços históricos e culturais que indicam a influência da União Europeia na América do Sul, de uma maneira geral, em sede da proteção de dados, é possível identificar o fundamento ontológico da tutela na dignidade humana (VIOLA et. al., 2016).

Conhecido como *General Regulation Data Protection* (GDPR) ou Regulamento Europeu de Proteção de Dados, o Regulamento 2016/679 do Parlamento Europeu e do Conselho da União Europeia é a atual normativa geral na União Europeia sobre o tema. Sucedendo a Diretiva Europeia de Proteção de Dados (95/46/CE), em 25 de maio de 2018,[18] a natureza de regulamento implica na desnecessidade de que os comandos normativos dispostos no GDPR sejam replicados no direito interno da União ou de cada Estado-Membro para que tenha força regulatória.[19] Como observam Tepedino e Teffé (2019), o GDPR funciona como

---

[17] A efetiva proteção dos dados pessoais estabelece uma relação de dependência com uma situação internacional favorável, além de uma certa coesão na matéria (DONEDA, 2006).

[18] "Na Europa, cresceu o entendimento de que o RGPD, instrumento que revogou a Diretiva 95/46/CE, de 24 de outubro de 1995, é a base jurídica específica de raiz antropológica que faltava à União Europeia, para proteger integralmente a pessoa. A despeito de compartilhar com esta visão, entende-se que, de fato, ela é fruto de um somatório, resultando de um conjunto de instrumentos jurídicos relevantes que foram sendo criados ao longo do século XX, dos quais se destacam: Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, (1950), consagra no artigo 8.º o direito ao respeito pela vida privada e familiar: «Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pela sua correspondência; Convenção 108 para a Proteção das Pessoas Singulares (1981), do Conselho da Europa, debruçou-se sobre o Tratamento Automatizado de Dados Pessoais" (SARLET; CALDEIRA, 2019, p. 7-8).

[19] Como instrumento jurídico de direito secundário europeu, o propósito do GDPR é o de uniformizar o regime de tratamento de dados na União Europeia, que se apresenta como um requisito essencial para o bom funcionamento do Mercado Único, na condição do primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados (SARLET; CALDEIRA, 2019). Em 2015, a Europa criou a Estratégia para o Mercado Único Digital ratificando o empenho de aproveitar as oportunidades geradas pelas tecnologias digitais, que não conhecem fronteiras e, portanto, quebram barreiras nacionais em sede de proteção de dados, telecomunicações e direitos de autor (SARLET; CALDEIRA, 2019). Como destacam Sarlet e Caldeira (2019), neste âmbito ganha relevância o Regulamento sobre Privacidade e Comunicações Eletrônicas (Regulamento *e-Privacy*), como um novo instrumento jurídico integrado na Estratégia para o Mercado Único Digital.

um modelo de referência para a elaboração, interpretação e aplicação de marcos regulatórios sobre proteção de dados pessoais a serem considerados por países como o Brasil, em vista do almejado fluxo de informações e de convergências derivadas de diplomas em nível internacional.

Nessa direção, é possível identificar um alinhamento intencional por parte do legislador brasileiro entre a LGPD e o GDPR, como um fator positivo no sentido de viabilizar o reconhecimento da adequação do sistema brasileiro de proteção de dados ao sistema europeu e, por conseguinte, promover a realização de transações e cooperações com os países do bloco (TEPEDINO; TEFFÉ, 2019). No contexto da América do Sul, apenas a Argentina e o Uruguai já foram reconhecidos nesse sentido (COMISSÃO EUROPEIA, 2019).[20]

Com relação à forma de análise da plataforma documental através da referência teórica adotada, cabe a advertência de Perlingieri (2019) no sentido de que cada instrumento deve ser sempre estudado em dois perfis: os perfis da estrutura da realidade e da função do instrumento do direito. O pragmatismo, ao se basear na realidade tão somente e a ela se resignando, é a negação do Direito, porque o Direito promove à mudança da realidade e não pode sucumbir aos fatos (PERLINGIERI, 2019). A primazia do Direito seria, portanto, a primazia da decisão política em face da natureza das coisas (PERLINGIERI, 2019).

Além disso, a força normativa Constituição deve ser evidenciada quando da interpretação da LGPD. Com alicerce ontológico na dignidade humana, a privacidade e a proteção de dados devem ser compreendidas de forma não-finalística e os seus planos de aplicação devem se nortear pela dignidade, porque concretamente relacionam-se com múltiplos valores e interesses não raro contraditórios entre si (DONEDA, 2006). A compreensão do fundamento da proteção dos dados sensíveis na dignidade e, mais adiante, no princípio da igualdade substancial apresenta-se como fundamental para traçar o alcance dos mecanismos de tutela na LGPD, que não podem ser vislumbrados de uma forma rígida ou taxativa, mas de acordo com a tutela integral da pessoa com alicerce constitucional. [21]

---

[20] "The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection. Adequacy talks are ongoing with South Korea. These adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the 'Police Directive' (article 36 of Directive (EU) 2016/680)" (COMISSÃO EUROPEIA, 2019, sem paginação).

[21] "A estrutura e a função indicam a natureza dos instrumentos jurídicos. Tal premissa nos consente saber melhor em relação de uma forma, o que é o formalismo jurídico, a saber, a atitude de aplicação do Direito de forma exacerbada, excessiva em relação à estrutura e em relação à função da letra da lei posta, relativa ao espírito e à substância da lei, dos interesses protegidos pelo formalismo da lei" (PERLINGIERI, 2019, p. 2).

Realizadas as presentes considerações, é possível traçar as diretrizes centrais para o enfrentamento do problema lançado neste trabalho. Primeiro, a pessoa humana se erige como epicentro da fundamentação e da axiologia do ordenamento jurídico. Segundo, apesar das dificuldades apresentadas pelos avanços das novas tecnologias e, paralelamente, os interesses do mercado na sua exploração, o direito não deve se render a essa facticidade, na medida em que se erige como fator de condicionamento da realidade social, assim como é por ela condicionado, na lição de Perlingieri (2019).[22]

Por fim, o terceiro fator consiste na compreensão de que a construção de normativas para a proteção da pessoa no cenário tecnológico, como é o caso das normas em sede de proteção de dados, deve atender a um equilíbrio no sentido de não se render à lógica da eficiência do mercado que instrumentaliza a pessoa para os seus fins, embora deva guardar pertinência com a realidade, especialmente diante das possibilidades tecnológicas, sendo suscetível de efetiva aplicação, sob pena de se tornar hermética e não atender ao objetivo ao qual se propõe.

Não obstante, as realidades econômica, social, cultural e política brasileiras devem constituir referência na análise, sobretudo diante da importação de diversos institutos de proteção que foram frutos, principalmente, da construção europeia, como citado. A natureza relativa da ciência jurídica demanda que a consideração dos conceitos e instrumentos jurídicos se façam à luz da sua relatividade e da sua historicidade (PERLINGIERI, 2019).

A compreensão e o governo das transformações determinadas pelos avanços tecnológicos apenas são viáveis se guardarem sintonia com instrumentos prospectivos aptos a redefinirem os princípios fundadores das liberdades individuais e coletivas sob os paradigmas dos novos tempos (RODOTÁ, 2015). A partir do imperativo da constitucionalização da pessoa, parte-se da premissa de que nem tudo que é tecnicamente possível é socialmente desejável, eticamente aceitável e juridicamente admissível (RODOTÁ, 2004).

[22] "A realidade é una, é unitária, e o seu aspecto (o seu perfil) nada mais é que um aspecto de realidade unitária. Por isto o Estado de Direito não pode se limitar ao estado das leis. Os instrumentos da ciência jurídica, as noções, as definições, os conceitos não são fins em si mesmos, mas sim instrumentos para o conhecimento desta realidade. Por isto, devem ser instrumentos adequados à realidade" (PERLINGIERI, 2019, p. 1).

3 A TUTELA DA PERSONALIDADE NA ERA DIGITAL

A partir da experiência jurídica italiana, Perlingieri (2006) evidencia o processo de funcionalização dos interesses patrimoniais aos interesses de ordem existencial. A princípio, diversos institutos jurídicos foram concebidos para a proteção da propriedade, que era compreendida como essencial ao desenvolvimento da pessoa, e transpareciam uma lógica individualista, centrada na vontade do sujeito, como processo característico da propriedade (PERLINGIERI, 2006).

Como fruto de diversas conquistas sociais e transformações históricas, o debate alcança outros patamares com a centralidade da constituição, a partir da qual as normas que tutelam a pessoa passam a prevalecem em face da tutela meramente patrimonial, usurpando, não obstante, a legalidade em sentido estrito quando da concretização do direito.[23] A rigor, a iniciativa econômica privada e a propriedade devem ser endereçadas considerando a sua instrumentalidade para a realização da pessoa, através de uma leitura pautada da constituição (PERLINGIERI, 2006).[24] Como observa Perlingieri (2006), na perspectiva constitucional o "ter" é funcionalizado ao "ser".[25]

O paradigma então proprietário é alterado com a percepção de que a pessoa não deve ser protegida apenas quanto ao que possui, mas com relação àquilo que é, ou seja, nas palavras de Perlingieri (2006, p. 9), "nas faculdades inseparáveis da natureza humana que constituem a razão e o fundamento de sua existência e o desenvolvimento de sua atividade para alcançar os

[23] "O século XX foi profundamente marcado por duas guerras, pelos horrores efetivamente praticados pelo Estado constituído, especialmente durante a vigência da ideologia nazista. Sua política de racismo, destruição e morte, assegurada por lei, consentiu que fossem ultrapassados limites até então intransitados, e provocou, como reação, a necessidade de concreta efetivação dos direitos humanos (...) Se o Estado de Direito, iluminista e racional, mostrou-se insuficiente para a proteção da coletividade frente ao totalitarismo mais abjeto, tornou-se necessário abandonar a legalidade em sentido estrito" (MORAES, 2010, p. 40).

[24] O ato de mercado não se justifica de *per se*, mas nos princípios jurídicos consagrados na Constituição (PERLINGIERI, 2019). Em outra sede, Perlingieri (2006, p. 7) refere que: "Tale mutamento di funzioni – da una concezione semplicemente produttivistica (che poneva come massimo scopo della collettività la creazione del maggior reddito nazionale) ad una concezione che tende a realizzare il miglioramento della situazione dell'individuo e l'attribuizione allo stesso della libertà e della possibilità efetiva di sviluppare la propria personalità – si giustifica perché a base dell'ordinamento ci sono valori d'ordine morale ed umano che trascendono il momento economico".

[25] Reconhecida a força normativa da Constituição, o seu papel político é extravasado para constituir o filtro de legitimidade da ordem jurídica (HESSE, 1991). No cenário brasileiro, a integralidade do tecido normativo infraconstitucional passa a ser permeada pelos imperativos da Constituição da República Federativa do Brasil (CRFB) de 1988, entre os quais despontam a cidadania e a dignidade da pessoa humana (art. 1º, I e III, CRFB), fundamentos da República, o princípio da igualdade substancial (art. 3º, III, CRFB), ao lado da isonomia formal do art. 5º, além da garantia residual estipulada pelo art. 5º, § 2º, CRFB (BRASIL, 1988), condicionando a atuação do intérprete e do legislador ordinário (TEPEDINO, 2004).

fins essenciais da vida".[26] Em realidade, a pessoa é o valor que fundamenta e é tutelado primariamente pelo ordenamento jurídico, com a paralela compreensão de que "a pessoa é inseparável da solidariedade: ter cuidado com o outro faz parte do conceito de pessoa" (PERLINGIERI, 2008, p. 461).

Em decorrência, a divisão entre o privado e o público que se operava em um primeiro momento, como fruto de uma representação de escolha ideológica, é mitigada com a consideração de que a proteção da personalidade é uma questão unitária, de forma que qualquer abordagem setorial do direito se reflete senão como aplicação específica dos princípios constitucionais (PERLINGIERI, 2006).[27] Vale dizer, o valor da pessoa perpassa integralmente o ordenamento jurídico, consolidando uma nova hermenêutica.

O processo de ruptura dos compartimentos do direito público e do direito privado toma contornos mais evidentes em face das grandes transformações tecnológicas que redesenham o papel dos poderes públicos, transformando as relações pessoais e sociais e interferindo sobre toda a antropologia das pessoas, como percebe Rodotà (2005). Em última análise, o anacronismo dessa separação se evidencia nas situações que simultaneamente demandam uma regulação de natureza privada e de ordem pública, como é o caso das novas tecnologias (TEPEDINO, 2009), e, como a seguir será assinalado, da privacidade e da proteção de dados pessoais.

Traçadas as linhas teóricas introdutórias que orientam a abordagem do ordenamento jurídico a partir da centralidade da pessoa, como epicentro dos valores em uma leitura constitucional, inclusive em termos de intersubjetividade,[28] releva destacar determinadas questões atinentes à sua proteção. Para tanto, deve-se voltar cerca de duzentos anos, nas raízes da idade contemporânea e do direito contemporâneo.

3.1 Dos direitos da personalidade à cláusula geral de tutela e promoção da pessoa

[26] Tradução livre de: "Nella facoltà inseparabili della natura umana che costituiscono ragione e fondamento della sua esistenza e dello sviluppo della sua attività per raggiungere i fini essenziali della vita".

[27] O processo de constitucionalização do direito civil trouxe entre os seus predicados a prevalência das situações não patrimoniais, em vista das existenciais protegidas preferencialmente pelo constituinte, o reconhecimento da historicidade das regras jurídicas e a valorização da função dos institutos jurídicos (MORAES, 2010).

[28] Partindo da consideração de que o indivíduo enquanto tal não existe, mas coexiste, sua relação com os seus semelhantes passa a ser constitutiva da sua existência, em dissonância com a proposta liberal-individualista, baseada em Rousseau, que apresenta o homem como uma pequena "totalidade" (MORAES, 2010). A partir desta perspectiva, a estruturação nas sociedades contemporâneas não mais teria como ponto central a "pessoa", mas o espaço comum entre elas, a constituir a noção de intersubjetividade (MORAES, 2010).

O Código de Napoleão se consolidou como "expressão da monumental Revolução Francesa", nas palavras de Moraes (2010), ao reconhecer os direitos subjetivos e ao garantir proteção à então vitoriosa burguesia através da juridicização das trocas e das titularidades. Como consequência desse paradigma, emergiram a qualificação dos sujeitos de direito, a importância do contrato e o fortalecimento da propriedade (MORAES, 2010).[29] Com esse cenário, a partir da exemplaridade da Revolução Industrial, a consagração do liberalismo jurídico chancelou diversas formas de degradação da pessoa a partir do afastamento do Estado das relações privadas e de uma abordagem formalista, em desconsideração à realidade subjacente aos instrumentos jurídicos (SCHREIBER, 2014).

Mais adiante, o colapso econômico do Estado liberal na virada do século XIX e a ascensão do *Welfare State* evidenciaram a igualdade substancial como fundamento para a multiplicação de hipóteses de intervenção jurídica com o fim de reequilibrar as relações privadas (MORAES, 2010). Partiu-se do reconhecimento da insuficiência do paradigma voluntarista da liberdade formal, que, com uma "moldura" jurídica, abriu campo para abusos de variadas ordens, através dos quais contratantes em posição de inferioridade econômica eram levados a firmar contratos nitidamente lesivos (MORAES, 2010).

A categoria dos direitos da personalidade é fruto da construção a partir das elaborações doutrinárias na Alemanha e na França, na segunda metade do século XIX (TEPEDINO, 2004). O imperativo era a criação de uma categoria de direitos imprescindíveis ao ser humano, para além da liberdade formal, protegendo-o, por vezes, da fragilidade da sua vontade (SCHREIBER, 2014).[30] Como resultado de diversas conquistas históricas, a categoria dos direitos da personalidade se desenvolveu com o reconhecimento jurídico de um conjunto dos atributos essenciais da pessoa humana, relacionando-os diretamente com a tutela da dignidade e da integridade da pessoa (TEPEDINO, 2004).

A dogmática orientada pela proteção da pessoa apontava no instituto da personalidade o seu centro de irradiação (DONEDA, 2006). Todavia, o instrumento então existente para a tutela da pessoa era o direito subjetivo, fruto da Revolução Francesa, que se define por uma lógica patrimonial, pressupõe uma dualidade entre sujeito e objeto e atende, portanto, a um

---

[29] "Na época da codificação, o valor originário e fundamental era constituído pelo indivíduo, por sua capacidade individual, por sua liberdade de escolher suas próprias metas, assumindo, sozinho, o risco do sucesso e do fracasso" (MORAES, 2010, p. 41).

[30] "Alguns aspectos da personalidade foram desenvolvidos entre o século XIX e o início do século XX, como o direito moral de autor ou a proteção da imagem, contudo, o marco mais característico desse processo deve ser reconhecido na Constituição de Weimar, em 1919, pela primazia em trazer ao âmbito constitucional os institutos-chave do direito privado" (DONEDA, 2006, p. 74-75). A propósito, a Constituição de Weimar, em 1919, é significativa no aspecto em que a tutela dos interesses econômicos se legitimava apenas quando vinculada aos direitos da pessoa (DONEDA, 2006).

substrato ideológico liberal (DONEDA, 2006).[31] São lançados, assim, outros desafios para a proteção da pessoa. Nas considerações de Rodotà (2013, p. 12):

> A invenção do sujeito de direito, a instituição do homem como sujeito não apenas no mundo jurídico, continua sendo um dos grandes resultados da modernidade, cujas características e função histórica devem ser assinaladas. O que deve ser rejeitado é um uso político que gradualmente esterilizou a força histórica e teórica dessa invenção, reduzindo o sujeito a um esqueleto que isolava o indivíduo, o separava de qualquer contexto, fazia abstração das condições materiais (...). Daí a necessidade de retomar o fio quebrado da igualdade, não para retirá-la dos benefícios da forma que continua a ser um instrumento contra a institucionalização das discriminações, mas a uma indiferença pela realidade de ser, desenhando assim novas hierarquias e novos abandonos fundamentados sobre a forca política e a prepotência do mercado.[32]

Nesse sentido, "sob o pretexto de proteção do sujeito abstrato, usurpam-se, no plano concreto, direitos inerentes ao ser humano", o que permitiu Negri (2016, p. 2) identificar, a partir de Rodotà (2007), um processo de "expropriação da subjetividade". Assim, para além da consideração kelseniana de sujeito como unidade personificada de normas, Rodotà (2012) sustenta a consideração da pessoa humana como um caminho para a recuperação integral da sua individualidade e da sua identificação como valor fundante do sistema jurídico.

Expressa-se uma nova antropologia, passando de uma noção que predicava indiferença e neutralidade para uma que impõe atenção para o modo como o direito ingressa na vida da pessoa (RODOTÀ, 2012). A valorização da abstração e do normativo, em detrimento da realidade da pessoa, obscurece os campos que demandam direta atuação do direito. Em termos de enunciação da promoção da pessoa, a Constituição da República Federativa do Brasil (CRFB) de 1988 é um primado humanista, embora os desafios lançados para o livre desenvolvimento da personalidade se situem no campo da realidade social.

As construções de sujeito e pessoa, no entanto, coexistem na medida em que o "primado da dignidade humana comporta o reconhecimento da pessoa a partir dos dados da realidade, realçando-lhe as diferenças, sempre que tal processo se revelar necessário à sua tutela integral" (TEPEDINO, 2016, p. 18). Em contrapartida, a abstração do sujeito "assume grande relevância

---

[31] A consequente disseminação de instrumento de tutela de natureza proprietária acabou por abordar a proteção da pessoa, assim como demais categorias privatísticas, à categoria do "ter" (DONEDA, 2006).

[32] Tradução livre de: "L'invenzione del soggeto di diritto, l'istituizione dell'uomo come soggetto non solo nel mondo giuridico, rimangono uno dei grandi esiti della modernità, di cui vanno compresi i caratteri e la funzione storica. Quel che va respinto è un uso politico há via via sterilizzato la forza storica e teorica di quell'invenzione, riducendo il soggetto ad um scheletro che isolava l'individuo, lo separava da ogni contesto, faceva astrazione dalla condizioni materiali. (...) Da qui la necessità di riprendere il filo spezzato dell'egualianza, sottraendola non ai benefici di una forma che continua ad essere strumento contro l'istituzionalizzazione delle discriminazioni, ma a una indifferenza per la realtà dell'essere, disegnando così nuove gerarchie e nuovi abbandoni fondati sulla forza politica e la prepotenza del mercato".

nas hipóteses em que a revelação do dado concreto possa gerar restrição à própria dignidade, ferindo a liberdade e a igualdade da pessoa" (TEPEDINO, 2016, p. 18). Nestes termos, é possível mediar a igualdade formal do sujeito, como libertadora de preconceitos, e a igualdade substancial da pessoa, em atenção às suas vulnerabilidades (TEPEDINO, 2016).

Na conjuntura brasileira do século XX, apesar da categoria dos direitos da personalidade não ter sido prevista no Código Civil de 1916, as duas Guerras Mundiais evidenciaram a necessidade de superação da legalidade estrita, então permissiva a desumanidades, para alçar o campo dos valores da democracia, da liberdade e da solidariedade (MORAES, 2010). Vale dizer, a Declaração Universal dos Direitos Humanos de 1948, ao trazer em seu bojo o reconhecimento da dignidade humana como fundamento da liberdade, acabou por repercutir em todas as constituições da segunda metade do século XX. Embora o árduo caminho percorrido na realidade brasileira no período da ditadura militar, os valores compartilhados socialmente foram consagrados na CRFB de 1988, entre eles diversos direitos historicamente apontados como da personalidade (BRASIL, 1988).

A previsão infraconstitucional de um regime jurídico para os direitos da personalidade foi estabelecida no Código Civil brasileiro de 2002 nos artigos 11 ao 21 (BRASIL, 2002), que sendo excessivamente rígidos e estruturais, apresentam-se como anacrônicos, ainda mais diante das novas tecnologias. Apesar de reconhecido o imperativo de proteção da pessoa, a normatização da categoria dos direitos da personalidade no Código Civil prescreve uma tutela fragmentária, entre outros desafios que fogem da abrangência da presente pesquisa.[33]

Nesse âmbito, um fator que deve ser destacado é a difusão da teoria da *fattispecie*. De acordo com a teoria, os fenômenos jurídicos seriam compostos por um elemento material, referente à situação de fato externa, e outro formal, configurado a partir das regras que determinam a qualificação jurídica daquele fato com as implicações correlatas, erigindo-se como verdadeiro filtro, na medida em que seleciona as situações que têm aptidão para ingressar no "sistema dos fenômenos jurídicos" (NEGRI, 2016).

Compreender a personalidade como valor maior do ordenamento jurídico é logicamente incompatível com uma forma de tutela orientada em moldes taxativos e rígidos, o que se acentua diante da complexidade relacional contemporânea. Vale ressaltar, nas palavras de Perlingieri (2005, p. 13), "a personalidade é valor objetivo, interesse, bem juridicamente relevante, que se implementam de uma forma dinâmica do nascimento à morte da pessoa,

[33] É o caso da extensão, no que couber, dos direitos da personalidade para as pessoas jurídicas, sem a problematização da diversidade de ontologias. Ver mais em Negri (2016) e Schreiber (2014).

desenvolvendo-se com uma formação própria, com uma educação própria, com as suas próprias escolhas".[34]

Como define Moraes (2010) a partir de Perlingieri (2002), a personalidade humana não se realiza através de um esquema taxativo de situações jurídicas objetivas, mas sim de uma complexidade de situações jurídicas subjetivas que podem ostentar formas distintas. A recorrente existência de novas instâncias relativas à personalidade, não previstas e nem previsíveis pelo legislador, indica para uma necessária normatização aberta, a ser limitada apenas quando em colisão com outras personalidades (MORAES, 2010). É neste sentido que a categoria de direitos da personalidade, se considerada como legitimadora de proteção, não é suficiente para promover a tutela que a pessoa demanda.

Portanto, com o alicerce axiológico na dignidade da pessoa humana depreende-se a existência de uma cláusula geral de tutela, que deve ser aplicada em todas as situações que tenham a personalidade como elemento objetivo (TEPEDINO, 2004).[35] No ordenamento jurídico brasileiro, a dignidade, enquanto fundamento da República estabelecido em nível constitucional (art. 1º, III) (BRASIL, 1988), erige-se como fundamento da cláusula geral de proteção e promoção da pessoa humana (MORAES, 2010).

A princípio, as diversas formas de conceituação do que seria a dignidade deram ensejo, inclusive, a pesquisas empíricas e experimentais, como a realizada por Struchiner e Hannikainen (2016), que identificaram discrepâncias não apenas intersubjetivas, mas também intrasubjetivas na sua compreensão.[36] A dignidade, apesar de contar com a conceituação incisivamente controvertida e da relatividade das coisas, permanece como o único valor capaz de dar harmonia, equilíbrio e ponderação ao ordenamento jurídico (MORAES, 2010).[37]

---

[34] Tradução livre de: "(...) La personalità è valore obiettivo, interesse, bene giuridicamente rilevante. Valore e bene che si attuano in forma dinamica dalla nascita alla morte della persona, la quale, a sua volta, si sviluppa con una propria formazione, con una propria educazione, con proprie scelte". Ainda, de acordo com Perlingieri (2005, p. 13): "Tutto questo attiene alla dinamica della personalità, alla personalità come valore e non come capacità giuridica o soggettività". Como diferencia Schreiber (2014), a personalidade pode ser considerada em dois aspectos, a saber, subjetivo, entendido como a capacidade de ter direitos e obrigações, e objetivo, compreendido como o conjunto de características e atributos essenciais da pessoa humana.

[35] A centralidade da dignidade reformula a autonomia da vontade, como concebida nas codificações do século XIX, elevando-a à autonomia privada. Na síntese de Tepedino (2009), o paradigma é alterado no aspecto subjetivo, objetivo e formal. Com relação ao aspecto subjetivo, passa-se do sujeito abstrato à pessoa considerada em termos concretos. A sobreposição de novos interesses existenciais aos patrimoniais que caracterizavam os bens jurídicos no passado integra o aspecto objetivo. No aspecto formal, a forma dos atos jurídicos assume a função limitadora da autonomia privada em vista de interesses socialmente relevantes e das situações de vulnerabilidade (TEPEDINO, 2009).

[36] Recomenda-se a leitura da pesquisa em Struchiner e Hannikainen (2016).

[37] Com o propósito de materializar a relevância do instituto, é importante referenciar a apresentação de Machado e Negri (2011) sobre a construção de Habermas a respeito do papel que a experiência acumulada de violações à dignidade cumpriu na construção dos direitos humanos, sintetizada em três funções: inventiva, heurística e sismográfica. De acordo com os autores, "a função inventiva se explica com a circunstância de que, uma vez experimentada a violação da dignidade, caminha-se para o esgotamento (ou dessecamento) do sistema de direitos

De acordo com Rodotà (2011, p. 11), "a dignidade é o reconhecimento da humanidade profunda das pessoas, da sua liberdade de se autodeterminar, protegidas de qualquer forma de imposição externa".[38] Compreendida como valor e princípio na ordem jurídica brasileira, a dignidade humana compõe-se dos princípios da liberdade privada, da integridade psicofísica, da igualdade substancial e da solidariedade social, como define Moraes (2003) a partir do imperativo categórico kantiano.[39]

A cláusula de tutela depreendida da dignidade tem o condão de irradiar o valor da pessoa do alto da hierarquia constitucional com o propósito de unificar a sua proteção (DONEDA, 2006). Com este paradigma, a categoria dos direitos da personalidade pode se traduzir como especificação analítica para a cláusula geral de tutela (TEPEDINO, 2004) ou meio para que dela se extraiam diferentes potencialidades práticas (SCHREIBER, 2014), mas não mais se erige como fundamento e filtro legitimador da proteção da pessoa. Como observa Doneda (2006, p. 99-100):

> É inevitável que, no desenvolvimento de uma tradição hermenêutica que porte às devidas consequências os efeitos da cláusula geral da proteção da personalidade, tal operação tenda a absorver a própria ideia geratriz dos direitos da personalidade. Isto se justifica pelo abandono de um arcabouço teórico identificado com a categoria dos direitos subjetivos, como a subsunção e o sujeito de direito, em favor de instrumentos como a concreção e a própria pessoa humana, cuja ubiquidade como ponto de referência objetivo das relações jurídicas pode ao fim tornar desnecessário o recurso aos próprios direitos da personalidade.

Com efeito, para além da superação de uma ótica "tipificadora" de proteção, a ampliação da tutela da pessoa não deve se restringir a novas hipóteses de ressarcimento, mas alcançar a promoção da personalidade, independente das situações de patologia, para se entender a qualquer situação jurídica da qual a pessoa participe (TEPEDINO, 2004). No imperativo da

---

disponível" (MACHADO; NEGRI, 2011, p. 188). A função heurística, por sua vez, é verificada "na medida em a dignidade integra as categorias de direitos e a sua invocação rapidamente põe em evidência a indivisibilidade desses direitos, como um atalho mental ao dado de que os direitos guardam entre si relação de mútua dependência" (MACHADO; NEGRI, 2011, p. 189). Por fim, a função sismográfica apresenta que a dignidade procede a um registro constante do que é efetivamente constitutivo de uma ordem legal democrática (MACHADO; NEGRI, 2011, p. 189).

[38] Tradução livre de: "La dignità è il riconoscimento dell'umanità profonda delle persone, della loro libertà di determinarsi, al riparo da qualsiasi forma di imposizione esterna".

[39] Ainda com a lição de Moraes (2003, p. 85), "o substrato material da dignidade assim entendida pode ser desdobrado em quatro postulados: i) o sujeito moral (ético) reconhece a existência dos outros como sujeitos iguais a ele, ii) merecedores do mesmo respeito à integridade psicofísica de que é titular; iii) é dotado de vontade livre, de autodeterminação; iv) é parte do grupo social, em relação ao qual tem a garantia de não vir a ser marginalizado. São corolários desta elaboração os princípios jurídicos da igualdade, da integridade física e moral – psicofísica –, da liberdade e da solidariedade". A proposta de compreensão da dignidade humana a partir desses princípios encontra seu fundamento nos riscos de generalização da dignidade, colocando-a como *ratio* jurídica de todo e qualquer direito fundamental, postura hermenêutica que acabaria por atribuir ao princípio tamanho grau de abstração que inviabilizaria a sua aplicação (MORAES, 2003).

constituição, a tutela dos interesses fundados em valores existenciais não se restringe à repressão da lesão, em um tipo negativo clássico, mas abarca uma tutela negativa, preventiva ou inibitória, para evitar situações potencialmente lesivas, assim como uma tutela positiva para proteger o interesse e viabilizar a sua máxima realização (SCHREIBER, 2015).

Nesses termos, personalidade não mais se erige como um reduto de poder do indivíduo, mas "como valor máximo do ordenamento, modelador da autonomia privada, capaz de submeter toda a atividade econômica a novos critérios de validade" (TEPEDINO, 2004). O livre desenvolvimento da personalidade se alia à vedação de qualquer forma de mercantilização da pessoa, demandando a aplicação de instrumentos e procedimentos jurídicos que correspondam à natureza das situações existenciais quando estas estiverem em tela, como é o caso da integridade, da identidade e da privacidade (KONDER, 2015).

Para além desse panorama, é importante apontar as três circunstâncias que caracterizam o paradigma pós-moderno: a impossibilidade de dominar os efeitos da tecnologia em termos autopoiéticos, a monumental disponibilidade de informações forjadas no ambiente virtual e que a acumulação profunda de conhecimentos sobre o mundo não aumentou a sabedoria do mundo, notoriamente na convivência social (MORAES, 2003). É com relação ao primeiro fator que o presente trabalho busca se debruçar.

A ciência, ao se basear no princípio do possível/impossível, é incapaz de limitar a si mesma (MORAES, 2003). Emerge, portanto, o papel do direito de responder aos reflexos da dinâmica tecnológica com a reafirmação do seu valor fundamental, que é a pessoa humana, devendo fornecer segurança e previsibilidade para que as estruturas econômicas se façam viáveis de acordo com a axiologia constitucional (DONEDA, 2006). Enquanto uma das estruturas responsáveis por disciplinar as escolhas relacionadas à técnica, compete ao direito normatizar as decisões ético-político-jurídicas da sociedade (MORAES, 2003).

Na contemporaneidade, a esfera privada ganha cada vez mais relevância porque representa campo para o livre desenvolvimento da personalidade, sem ingerências externas e sem mecanismos de controle social que acabariam por anular a sua individualidade e cercear a sua autonomia privada (DONEDA, 2006). Como anuncia Rodotà (2008), o livre desenvolvimento da personalidade deposita na proteção de dados pessoais a condição de ferramenta essencial na era digital e de um conjunto de direitos que configuram a "cidadania do novo milênio". Com fundamento na dignidade da pessoa, imperativo, portanto, assinalar o desenvolvimento da privacidade à proteção de dados pessoais.

3.2 Privacidade e proteção de dados pessoais

A privacidade é um conceito manipulável pelo próprio ordenamento jurídico para atender algumas de suas necessidades estruturais, dificultando a sua redução a uma definição âncora diante de variações que se expressam em diversas experiências normativas pelo mundo (DONEDA, 2006). Como destaca Doneda (2006, p. 119), essa indeterminação se erige como uma característica ontológica da construção de esfera privada e a busca pelo que hoje referimos como "privacidade" era atendida, em outras épocas, por outras arquiteturas da estrutura social e política, a exemplo da proteção da propriedade.

Como uma noção cultural induzida no tempo e dependente de bases sociais, culturais e políticas (DONEDA, 2006), a privacidade assume a natureza de um direito complexo e dinâmico, na definição de Rodotà (2008). A origem da atual dinâmica da juridificação da privacidade remete ao século XIX, especificamente na doutrina alemã com Röeder, em 1846, através da referência a um "direito natural à vida privada" (DONEDA, 2006).

No entanto, o debate moderno sobre a privacidade tem seu marco na discussão histórica apresentada no artigo publicado na *Harvard Law Review* por Warren e Brandeis (1890). A partir da associação da *privacy* à concepção de *inviolate personality,* os autores referenciaram a célebre construção do Magistrado norte-americano Thomas McIntyre Cooley do *right to be let alone*[40] (WARREN; BRANDEIS, 1890).[41] Apesar do *right to privacy* analisado por Warren e Brandeis (1890) se dar em um contexto cultural e jurídico diverso, a leitura da privacidade se desloca para uma perspectiva pessoal, e não mais patrimonial que até então definia a sua proteção (DONEDA, 2006).[42]

Apesar dessa alteração na abordagem da privacidade, a referência a um "direito a ser deixado só" é marcada por um forte componente proprietário, individualista, com uma lógica excludente que se relaciona com o espaço e, por conseguinte, com as situações subjetivas patrimoniais (DONEDA, 2006). Em moldes proprietários, apesar de reconhecida a sua natureza

---

[40] Warren e Brandeis (1890) não afirmaram que a noção do *right to be let alone* seria o conteúdo da *privacy*, mas que esta se associaria à inviolabilidade da personalidade.

[41] A eclosão do *right to privacy* nos Estados Unidos se associa à passagem do perfil rural do país para a predominância urbana, com o consequente surgimento de uma classe operária urbana e outra intelectual liberal e diante da necessidade de resolver os problemas do capitalismo financeiro (DONEDA, 2006).

[42] Embora o assunto já se fizesse presente na jurisprudência do *common law* e na literatura anterior, Warren e Brandeis (1890) propõem uma força inédita ao *right to privacy*, sendo mais do que um mero reflexo da época, com a extensão da sua influência partindo das mudanças trazidas à sociedade pelas tecnologias da informação e pela atribuição da natureza pessoal à privacidade, não se aproveitando mais da tutela da propriedade (DONEDA, 2006). Como argumenta Doneda (2006), o artigo de Warren e Brandeis assumiu um caráter programático diante de tendências jurisprudenciais esparsas sobre o que se tornaria o novo *right to privacy,* especialmente na experiência jurisprudencial norte-americana, com o posterior reconhecimento da natureza constitucional da privacidade.

pessoal, a privacidade depositava na propriedade uma condição para a sua fruição. A conotação essencialmente negativa então assumida pela privacidade constituía um dever geral de abstenção, conjuntura na qual chegavam a sustentar a incompatibilidade da privacidade com a pobreza, apontando-a como um direito da "era de ouro" da burguesia (SCHREIBER, 2014).

A associação da matriz individualista da privacidade à identidade burguesa é vislumbrada a partir de John Locke como um "individualismo possessivo", relacionando a liberdade humana à propriedade privada, então concebida como essencial ao desenvolvimento da pessoa (DONEDA, 2006). Como observa Rodotà (2008), a privacidade surge como a aquisição de um privilégio por parte de um grupo, e não como uma demanda natural do indivíduo.

Posteriormente, ao integrar a Suprema Corte norte-americana, Louis Brandeis capitaneou a defesa da privacidade não como uma prerrogativa de isolamento, mas como uma expressão da personalidade através de recurso a valores intrínsecos do homem, o que ficou consagrado no seu voto dissidente no caso *Olmstead v. United States*, em 1928, primeira oportunidade em que a Suprema Corte dos Estados Unidos foi chamada a se manifestar sobre o novo *right to privacy* (DONEDA, 2006).[43]

Com base em uma interpretação consentânea à sua época da Quarta Emenda da Constituição dos EUA,[44] que até então era interpretada como ingresso não autorizado na propriedade privada, Louis Brandeis sustentou que a *ratio* da previsão constitucional era proteger a intrusão na vida privada pelo governo, o que teve seu alcance alterado com o impacto dos progressos tecnológicos.[45] Sobre o voto paradigmático de Brandeis, Lessig (2006) reconhece que o propósito seria o de traduzir a proteção originalmente concebida pela Constituição para o contexto no qual as tecnologias utilizadas para a invasão da privacidade foram elevadas a outro patamar.[46]

A decisão no caso *Olmstead v. United States* vigorou durante 40 anos, quando foi superada no caso *Katz v. United States* através do reconhecimento pela Suprema Corte norte-americana de que a Quarta Emenda protegeria pessoas, e não lugares, na linha do voto

[43] Para uma análise da evolução jurisprudencial norte-americana sobre o *right to privacy* ver Doneda (2006).
[44] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (Passed by Congress September 25, 1789. Ratified December 15, 1791)" (ESTADOS UNIDOS, 1789, sem paginação).
[45] No caso, debatia-se a licitude de interceptações de "grampos" promovidos pelo Governo dos EUA sem uma autorização judicial (DONEDA, 2006).
[46] "Brandeis' technique should be ours as well. His approach was to first identify values from the original Fourth Amendment, and translate those values into the context of cyberspace. Brandeis read beyond the specific applications that the framers had in mind to find the meaning that they intended to constitutionalize. His aim was to carry that meaning of the framers into the context of 1928" (LESSIG, 1999, p. 59).

dissidente de Louis Brandeis (DONEDA, 2006). Entretanto, passado pouco mais de uma década, no caso *Smith v. Maryland*, o entendimento então construído foi esvaziado (DONEDA, 2006).

A construção do *right to privacy* nos Estados Unidos apresenta contornos diferentes do que seria o direito à privacidade na conjuntura europeia e, mais adiante, no contexto brasileiro. O *right to privacy* constitucional apenas pode ser arguido frente ao Estado norte-americano, de acordo com a sua tradição constitucional, além de que múltiplos valores e interesses são protegidos através da privacidade no contexto dos Estados Unidos, associando a sua construção a uma liberdade civil (DONEDA, 2006).[47] Com esse panorama, é importante destacar que a abordagem norte-americana da *privacy* sempre evidenciou a promoção do fluxo de dados, ao encarar a tutela da privacidade como "um sistema de ajustes e vedações de práticas abusivas, a serem verificadas quase sempre em concreto, *a posteriori*" (DONEDA, 2006, p. 318).

No decurso da evolução histórica da privacidade, a Revolução Industrial é apontada como um marco temporal razoável no qual a tecnologia passou a ocupar um lugar de destaque na dinâmica social, ao que se seguiu, na década de 60, o advento do *Welfare State*, repercutindo em um significativo aumento das demandas sociais e no crescimento do fluxo de informações (DONEDA, 2006). Enquanto noção dinâmica, a privacidade passou progressivamente a ser associada ao armazenamento de informações em bancos de dados, sendo ilustrativo que a primeira lei norte-americana sobre a *privacy* é o *Fair Credit Reporting Act* de 1970, direcionado a escritórios de proteção ao crédito e a cadastro de consumidores (DONEDA, 2006).

A massificação dos meios materiais, antes restritos a determinadas esferas da sociedade, e o surgimento dos meios de comunicação em massa modificaram a expectativa de privacidade, assim como os mecanismos sociais que neutralizavam ou diminuíam o impacto causado pela intrusão na vida privada da pessoa (DONEDA, 2006). O desenvolvimento da tecnologia redesenhava, portanto, a maneira pela qual a pessoa poderia determinar a sua exposição na sociedade.

A relação da privacidade com o que seria "monitorável" ou "buscável",[48] segundo Lessig (1999), mantém uma dependência da tecnologia existente que se deu em um crescente até a contemporaneidade: a capacidade de monitoramento, que até então era restrita, alcançou

[47] Nos EUA, o *right to privacy* é evocado para uma constelação de questões, sendo possível considerar que essa ampla funcionalidade é "reflexo do reconhecimento da privacidade como questão fundamental para a liberdade e a democracia norte-americanas", sendo um dos aspectos a chamada *informational privacy* (DONEDA, 2006, p. 264). Exemplificativo do caráter múltiplo da *privacy* nos EUA é o *fundamental-decision privacy*, entre outros que podem ser conferidos em Doneda (2006).

[48] Os termos utilizados pelo autor no original são "monitored" e "searchable", respectivamente.

gradualmente a possibilidade de ser permanente, gerando cada vez mais informações sobre os indivíduos, o que aumenta as possibilidades do que pode ser procurado, além de promover a queda dos custos de acesso a essas informações.[49] As possibilidades técnicas, neste sentido, influenciaram qual seria o conteúdo da privacidade. A perspectiva de isolamento, do individualismo e da lógica proprietária não mais atendiam aos novos contornos da esfera privada que começavam a se delinear a partir da transformação do fluxo informacional.

O conceito de informação pessoal passou de algo pressuposto, enquanto meio para a proteção da privacidade diante de documentos e informações privados, para progressivamente definir-se como um conceito central para a privacidade (MACHADO; DONEDA, 2018).[50] A propósito, Doneda (2011) apresenta a distinção entre os termos "dado" e "informação", destacando o primeiro com uma conotação primitiva, como uma informação em estado potencial antes de ser transmitida, enquanto a informação se refere a algo além da representação contida no dado, chegando ao limiar da cognição.[51] Apesar da distinção, a lógica que deve nortear a disciplina da proteção de dados pessoais deve abranger a informação pessoal (DONEDA, 2006).

É paradigmático o estabelecimento de bancos de dados pelo Governo do Estado Federal de Hesse, na Alemanha, a partir da coleta de dados voltados para a parte de finanças, seguridade, saúde, entre outros, em meados da década de 1960 (SIMITIS, 2010). A capacidade de exploração dos dados coletados, acrescidos dos riscos de vigilância permanente dos cidadãos, mobilizaram o Parlamento de Hesse que, em 10 de outubro de 1970, adotou a primeira norma de proteção de dados no mundo, a qual tinha como foco o próprio governo (SIMITIS, 2010). [52]

---

[49] "For by increasing the efficiency of a search, the changing technologies reduce the legal justifications for interfering with the searches. As searches become more efficient, the scope of 'reasonable' searches increases" (LESSIG, 1999, p. 60).

[50] "In their famous 1890 article, Samuel Warren and Louis Brandeis merely assumed that privacy regulation would always involve information identifiable to a person. They conceived of privacy as a right of 'personality.' Although the two authors did not define this concept in any detail, they drew on continental philosophy to argue that every person deserves protection against certain kinds of harms as a consequence of her status as a human" (SCHWARTZ; SOLOVE, 2011, p. 1819 apud MACHADO; DONEDA, 2018, p. 103).

[51] "O dado estaria associado a uma espécie de 'pré-informação', anterior à interpretação e ao processo de elaboração. (...) Sem aludir ao significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido de uma redução de um estado de incerteza" (DONEDA, 2006, p. 152).

[52] Na primeira metade do século passado bases de dados sobre cidadãos haviam sido utilizadas por regimes totalitários para fins discriminatórios, como o largo banco de dados mantido pela empresa italiana FIAT sobre seus trabalhadores que foi direcionada nas décadas de 1930 e 1940 para controle social pelo Estado italiano (DONEDA; MONTEIRO, 2015).

Em 1973, a Suécia[53] foi marcada como o primeiro país a estabelecer um regime jurídico para a proteção de dados pessoais, seguida por diversos países.[54]

O marco da primeira geração das leis sobre proteção de dados era a regulação de centros elaboradores de dados que concentrariam a coleta e a gestão de informações pessoais, normatizando a concessão de autorizações para a criação desses bancos e a posterior fiscalização pelos órgãos públicos (MAYER-SCÖNBERGER, 1997 apud DONEDA, 2011). O Estado era vislumbrado como controlador e principal usuário de tais dados e, por conseguinte, o destinatário central das respectivas normas (DONEDA, 2006).[55]

Com a multiplicação dos centros de processamento de dados sucedeu a segunda geração de leis, em que o eixo se deslocou do fenômeno computacional para considerar a personalidade (MAYER-SCÖNBERGER, 1997 apud DONEDA, 2011). A associação da liberdade negativa à proteção de dados que se fez presente nesta segunda geração, notadamente a lei *Informatique et Libertées* francesa, se revelou como insuficiente diante do fornecimento dos dados pessoais pelos cidadãos apresentar-se como requisito indispensável para a participação na vida social (DONEDA, 2006).

Em 1983, a Corte Constitucional alemã redefiniu as condições de acesso aos dados pessoais diante da pretensão da realização de um censo por parte do governo para coleta detalhada de informações sobre os cidadãos para realizar o processamento automatizado daqueles dados (SIMITIS, 2010). Na observação de Simitis (2010), os receios da população alemã de vigilância e de manipulação a partir dos dados geraram espontâneos protestos públicos sem precedentes. Na oportunidade, a Corte Constitucional da Alemanha estabeleceu que

> o dever de respeito à dignidade da pessoa e a liberdade de desenvolver a sua personalidade deve, especialmente em vista das tecnologias permitirem um processamento de uma quantidade cada vez maior de dados pessoais, ser

[53] "Não foi coincidência que países que por primeiro propuseram tais normativas foram países que tiveram problemas concretos de discriminação pelo tratamento de dados pessoais no passado, como a Alemanha, ou então países que foram pioneiros em tratar do tema da transparência governamental e também no tratamento de dados dos seus cidadãos para o desenvolvimento do estado de bem-estar social e, por isto mesmo, compreenderam a necessidade de criar salvaguardas para um espaço privado de seus cidadãos. Assim, é relevante que o primeiro país que adotou uma lei de proteção de dados pessoais (a Suécia, em 1970) seja o mesmo país que tenha adotado a primeira lei de acesso à informação no sentido moderno, no ano de 1766" (DONEDA; MONTEIRO, 2015, sem paginação).

[54] "A common characteristic of nearly all these laws is their omnibus approach. In other words, they all contain rules applicable to every kind of processing of personal data. An approach like this openly contrasts with the prevalence of sectoral-oriented provisions in the United States. Clearly sectoral rules depart from an omnibus regulation approach and instead deliberately focus on a specific context of data processing, such as credit reporting, information collected for insurance purposes, or the processing of personal data by the police as well as the various health agencies" (SIMITIS, 2010, p. 1996).

[55] Com relação à estrutura tecnocrática das normas, destacavam-se princípios demasiado abstratos, voltados à tutela dos bancos de dados, e não à privacidade em si, além da ausência de previsão da participação do cidadão (MAYER-SCÖNBERGER,1997 apud DONEDA, 2011).

> complementada pelo "direito à autodeterminação informativa" (SIMITIS, 2010, p. 1997).[56]

A autodeterminação informativa definia-se como o direito de o indivíduo determinar quem pode utilizar os seus dados, para qual finalidade, sob quais condições e por quanto tempo, erigindo-se como uma condição indispensável para uma sociedade democrática (SIMITIS, 2010).[57] Segundo Simitis (2010), a utilização da autodeterminação informativa como um pré-requisito para uma sociedade democrática, como apontado na decisão da Corte Constitucional alemã, confirma o papel central do indivíduo, mas não confere a ele um poder sem limites para decidir sobre as suas informações.[58] A perspectiva individual, por si só, não é suficiente para atender à finalidade da proteção dos dados pessoais. Neste sentido, a privacidade progride para ser compreendida não em uma lógica excludente, mas em caráter positivo de indutor da cidadania, da atividade política em sentido amplo e das liberdades (DONEDA, 2006).[59]

Com o marco da decisão da Corte Constitucional da Alemanha, o tratamento de dados enquanto um processo que demanda a participação ativa e consciente do titular é característico da terceira geração de leis, na qual emerge a autodeterminação informativa como extensão das liberdades negativas consagradas nas leis de segunda geração, embora a caracterização do seu exercício como privilégio de uma minoria que conseguiria arcar com os seus custos econômicos e sociais (MAYER-SCÖNBERGER,1997 apud DONEDA, 2011). Começou a se delinear, assim, uma quarta geração de leis voltada a suprir as defasagens da perspectiva individualista existente até então, com o imperativo de elevar a proteção de dados a um padrão coletivo (DONEDA, 2011).

---

[56] Tradução livre de: "the duty to respect the individual's dignity and his freedom to develop his personality must, especially in view of technologies allowing a processing of an ever greater amount of personal data, be complemented by a 'right to informational self-determination'".

[57] "Only then, the Court added, would individuals be able to freely form, express, and defend their opinions. The Court concluded that the more personal privacy is curtailed, the more individuals will gradually give up their constitutional rights. Informational self-determination, the Court stated, must therefore be seen and treated as an elementary precondition of a democratic society. Both its existence and functioning depend, thus, on the capacity of citizens to autonomously act and participate in society, a capability irrevocably linked to the knowledge and control of their personal data" (SIMITIS, 2010, p. 1997-1998). Para tanto, a Corte Constitucional alemã reconheceu a inexistência de dado pessoal irrelevante, uma vez que ainda que aparentemente sem valor, o dado pessoal pode vir a adquiri-lo (DONEDA, 2006).

[58] "Another equally relevant example of the need to consider the close relationship between data protection and a democratic society is the expanding commercialization of personal data. It has been justified as a perfectly normal result of either the data subject's property right, or more specifically, the subject's right to determine the use of his or her data. But although both these approaches recognize that information processing implies a range of economic interests, they ignore the full social costs of data use" (SIMITIS, 2010, p. 1999).

[59] Em 1981 a Convenção de Strasbourg representa o ponto de referência inicial do modelo europeu sobre proteção de dados, associando-a diretamente aos direitos humanos e às liberdades fundamentais, como pressuposto de um estado democrático (DONEDA, 2006).

A quarta geração de leis sobre proteção de dados é resultado do reconhecimento do patente desequilíbrio nas relações entre as entidades coletoras de dados e os titulares, de forma que o mero reconhecimento do direito à autodeterminação informativa no âmbito formal não bastava (DONEDA, 2011). Além disso, pode ser destacada a disseminação do modelo das autoridades independentes para a atuação da lei, associada à noção de *enforcement*, e a criação de normativas específicas para a proteção de dados (MAYER-SCÖNBERGER, 1997 apud DONEDA, 2006).

Paradoxalmente, foi reduzido o papel da decisão individual do titular, uma vez reconhecido que a proteção de certos dados deveria se dar em seu maior grau, como no caso dos dados sensíveis (DONEDA, 2011). As limitações inerentes aos poderes individuais, neste processo, indicam para a necessidade de um controle institucional que assegure o respeito aos dados pessoais por parte daqueles que têm sobre eles poder e, por consequência, sobre as pessoas que tiveram os seus dados coletados (RODOTÀ, 2019).

A autodeterminação informativa influenciou os países do sistema jurídico romano-germânico, e foi a partir da decisão da Corte Constitucional alemã que a proteção de dados foi consolidada como um direito fundamental, com um forte componente social (DONEDA, 2006). A LGPD expressamente elenca entre os seus fundamentos a autodeterminação informativa no art. 2º, inciso II (BRASIL, 2018), embora algumas ressalvas devam ser apresentadas com relação ao termo. Eventual leitura da autodeterminação informativa em uma "chave liberal" poderia gerar contornos negociais,[60] especialmente com relação ao consentimento da pessoa para o tratamento de seus dados, podendo conduzi-las a uma falsa impressão de propriedade sobre as suas informações, transportando esta fenomenologia para a esfera das situações

[60] Na medida em que as pessoas consentem para a utilização comercial dos seus dados para fins negociais, mais elas se integram em um sistema que melhora as chances do mercado de influenciar o seu comportamento (SIMITIS, 2010). Segundo Simitis (2010), a comercialização de dados promove uma manipulação de longo prazo sobre os titulares dos dados, o que gera implicações democráticas. O citado caso da *Cambridge Analytica* é exemplificativo dos riscos à democracia advindos do uso de dados. Essa dose de pragmatismo ganha relevância porque "a existência de um mercado para as informações pessoais é algo com que o direito deve conviver, e não somente pela dose de pragmatismo necessária à ação do jurista, porém principalmente porque o mercado é um dos agentes capazes de promover o fluxo de informações – que, conforme verificamos, não é absolutamente um mal em si. Ao jurista, a pergunta que cabe ser feita é sobre qual mercado e quais regras, mais do que sobre a existência ou a recusa automática deste mercado" (DONEDA, 2006, p. 363-364). Na experiência europeia, Simitis (2010, p. 2002) destaca os seguintes casos exemplificativos desse interesse do mercado: "Thus, for example, a British Biobank has been established to investigate diseases, such as Parkinson's, that are typical of an aging society. As a result, information from about half a million persons, aged between forty-five and sixty-nine years, is now regularly collected in the United Kingdom. The Biobank includes medical and genetic data as well as information regarding family members, professional activities, specific preferences and habits, and social contacts. The constantly perfected profiles of registered persons have quickly led security agencies and insurance companies to express their interest in Biobank's data. While the regulation governing the activities of the Biobank finally denied insurance companies access, it explicitly permits security agency use. Comparatively extensive collections were, for instance, discussed in France with regard to plans to diagnose cancer as early as possible and to link future insurance payments to patients strictly following a prescribed lifestyle".

patrimoniais e comprometendo a sua natureza de direito fundamental (DONEDA, 2006). Em última análise, essa percepção influenciou a quarta geração de leis sobre proteção de dados. Portanto, mais adequada seria a utilização da terminologia da "proteção de dados pessoais", com o propósito de fugir das citadas concepções (DONEDA, 2006).

No decorrer dessa evolução normativa, a matéria da proteção de dados pessoais associou-se a uma disciplina jurídica de princípios que constituíram, no dizer de Doneda (2011), a "espinha dorsal" de diversas leis, tratados, convenções e acordos entre instituições privadas. Conhecidos como *Fair Information Principles*, são os princípios da publicidade, da exatidão, da finalidade, do livre acesso e da segurança física e lógica.[61] De acordo com as suas particularidades e em vista dos avanços tecnológicos, esses princípios estão previstos no GDPR e na LGPD.

A partir desse panorama é possível identificar que o paradigma da privacidade passa a ir além do tradicional poder de exclusão para atribuir cada vez maior relevância ao poder de controle; o campo de aplicação da privacidade se amplia como "efeito do enriquecimento da noção técnica de esfera privada", de forma a associar o "privado" não necessariamente às razões de intimidade (RODOTÀ, 2008, p. 93). Como define Rodotà a partir da experiência europeia, a privacidade como direito complexo insere no seu conteúdo a autodeterminação informativa, entendida como o "direito de manter controle sobre as suas informações e de determinar a maneira de construir sua esfera particular" (RODOTÀ, 2008, p. 15). Por esfera privada entende-se "aquele conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo" (RODOTÀ, 2008, p. 92).[62]

Qualquer noção de privacidade deve ser fundada em uma percepção do indivíduo com a sociedade, com um caráter relacional que determina o nível de relação da personalidade com as demais e com o mundo ao seu redor, a partir da qual a pessoa tem a prerrogativa de determinar o seu grau de inserção e de exposição (DONEDA, 2006).[63] A relação, portanto,

---

[61] De acordo com o princípio da publicidade (ou da transparência), a existência de um banco de dados deve ser de conhecimento público, seja através da necessidade de autorização prévia para funcionar, da notificação a uma autoridade da sua existência, ou do envio de relatórios periódicos; o princípio da exatidão estabelece que os dados armazenados devem ter correspondência com a realidade, de forma que a coleta e tratamento devem se dar com cuidado e correção, atentando-se para a necessidade de atualizações periódicas; o princípio da finalidade prevê que utilização dos dados deve se dar nos limites da finalidade informada ao interessado antes da coleta; o princípio do livre acesso dispõe que o indivíduo deve ter acesso ao banco de dados no qual suas informações estão armazenadas, o que inclui o direito à obtenção de cópias desses registros e ao controle desses dados; o princípio da segurança física e lógica prevê que os dados devem ser protegidos contra os riscos que impliquem em seu extravio, destruição, modificação, transmissão ou acesso não autorizado (DONEDA, 2011).

[62] Em outros termos, a informação seria o elemento objetivo, ao passo que a finalidade seria a construção da esfera privada (RODOTÀ, 2008).

[63] A privacidade se relaciona diretamente aos valores e projeções do homem na sociedade e de seus grupos, a implicar em um forte conteúdo social e ideológico (DONEDA, 2006, p. 139).

entre privacidade e o livre desenvolvimento da personalidade é direta. Em decorrência, segundo Rodotà (2008, p. 92-93), "a privacidade pode ser identificada com a tutela das escolhas de vida contra toda forma de controle público e de estigmatização social, em um quadro caracterizado justamente pela liberdade das escolhas existenciais". Nesse sentido, como considera Moraes (2010, p. 108):

> O princípio da liberdade individual consubstancia-se, hoje, numa perspectiva de privacidade, intimidade e livre exercício da vida privada. Liberdade significa, cada vez mais, poder realizar sem interferências de qualquer gênero, as próprias escolhas individuais – mais: o próprio projeto de vida, exercendo-o como melhor convier.

A privacidade estreita, portanto, o seu vínculo com a identidade. Na medida em que a privacidade emerge como prerrogativa da pessoa determinar o seu grau de exposição e de inserção na vida social, esse grau de exposição corresponderá à representação da sua personalidade perante a sociedade. O conceito complexo de privacidade se conjuga com o reconhecimento da construção dinâmica da identidade pessoal como "novas formas de manifestação da proteção jurídica da pessoa humana contra as ameaças de estigmatização e discriminação oriundas do desenvolvimento tecnológico" (KONDER, 2019, p. 451).[64]

Como ressalta Konder (2019, p. 451), a partir de decisões italianas da década de 1970 foi legitimada a "defesa da pessoa contra imputação de características que não sejam compatíveis com a maneira pela qual ela é conhecida no meio social", a emergir o conceito de identidade pessoal que se converte em garantia do próprio processo dinâmico de construção dialógica da identidade (KONDER, 2019).[65] A identidade, que se delineia através do

---

[64] A noção de direito ao esquecimento enquanto pedido para que "determinada informação não esteja mais acessível publicamente" (BRANCO, 2017, p. 144), compreendido neste trabalho enquanto integrante da privacidade, estabelece relação com a construção da identidade da pessoa. Branco (2017, p. 180) define o direito ao esquecimento como "violação à privacidade por meio de publicação de dado verídico, após lapso temporal, capaz de causar dano a seu titular, sem que haja interesse público, conservando-se em todo caso a liberdade de expressão e desde que não se trate de fato histórico, cuja demanda é direcionada, em última instância, ao Poder Judiciário, que deverá, se entender cabível, ordenar a sua remoção ao meio de comunicação onde a informação se encontra (e nunca ao motor de busca)". Contudo, como apontam Machado e Negri (2017, p. 372), apesar de reconhecida a privacidade enquanto direito, "não basta que seja mobilizada de forma abstrata para que se afirme, sem maior cautela e ônus argumentativo, o direito ao esquecimento, como seu mero e linear desdobramento". A propósito, recomenda-se a leitura da análise empírica realizada por Negri e Korkmaz (2019b) sobre a aplicação do direito ao esquecimento pelo Superior Tribunal de Justiça no Recurso Especial n. 1.660.168/RJ.

[65] A identidade pessoal, abrangente de uma representação pluridimensional da pessoa, na sua trajetória apresentou diversos paralelos com a privacidade, o que é exemplificado na Itália com a tutela de interesses considerados em outros países como pertinentes à privacidade através da identidade pessoal (DONEDA, 2006). A propósito, Doneda (2006) sustenta que as concepções do *diritto alla riservatezza* e da *privacy* não apresentam uma equivalência no direito italiano, porque àquela estava restrita uma noção de isolamento pessoal. Na experiência italiana, como destaca Doneda (2006), em face de episódios que chamaram a atenção da sociedade italiana envolvendo informações pessoais, foi possível se falar no *diritto alla riservatezza* abarcando proteção de dados pessoais, por outro lado, problemas conexos foram tratados a partir da identidade pessoal. O alargamento da noção

reconhecimento do outro, apresenta como predicados para o livre desenvolvimento da personalidade a tutela da liberdade para decidir os valores, atributos, características e preferências que sejam consentâneas à própria pessoa no diálogo com as demais (TAYLOR, 2013; KONDER, 2019). Em última análise, diferentes formas de proteção convergem e dialogam para a tutela integral da pessoa, com fundamento na dignidade, como a proteção da privacidade e da identidade.

Nessa direção, gradualmente perde relevância a referência a um "direito à privacidade" em termos de espaços ou bens (DONEDA, 2006). O caráter individualista e exclusivista que caracterizavam a privacidade como uma liberdade negativa[66] atualmente está diluído diante de novos contornos do instituto que se atenta cada vez mais para a liberdade e o livre desenvolvimento da personalidade (DONEDA, 2006).

A passagem da privacidade à proteção de dados pessoais atende a critérios metodológicos direcionados a promover a funcionalidade de alguns valores fundamentais do ordenamento jurídico (DONEDA, 2006). A proteção de dados pessoais desdobra-se da privacidade, permanece compartilhando o mesmo fundamento ontológico que é a dignidade humana, contudo passa a ostentar um caráter significativamente objetivo,[67] essencialmente dinâmico e a elevar-se a uma dimensão coletiva (RODOTÀ, 2008). A clássica sequência "pessoa-informação-sigilo" é superada para alcançar a noção de "pessoa-informação-circulação-controle", na qual o imperativo é a circulação controlada de dados (RODOTÀ, 2008, p. 93).

Ao direcionar-se a uma tutela dinâmica, a proteção de dados não se concentra na perspectiva individual do sujeito, como acontece na privacidade (DONEDA, 2006). Por intermédio da proteção de dados pessoais, as garantias então relacionadas à privacidade passaram a ser visualizadas de uma forma mais ampla, para considerar outros interesses e diversas formas de controle que foram viabilizadas a partir da manipulação dos dados pessoais (DONEDA, 2006). Nesta perspectiva, o controle não se apresenta como uma forma de proteger

---

de *riservatezza* nos anos de 1970 para abranger a tutela de informações se seguiu da utilização da nomenclatura em inglês, como representativa da sua nova concepção (DONEDA, 2006).

[66] Apesar da tutela da privacidade não dispensar a responsabilidade civil enquanto instrumento, o instituto por si só não promove um avanço na proteção oferecida pelo ordenamento à privacidade, que continuaria a ser encarada como liberdade negativa, a desconsiderar a evolução da matéria, o seu caráter positivo e a sua função promocional na lógica da Constituição (DONEDA, 2006).

[67] Apesar de um processo de objetivação de caráter instrumental permear a proteção dos dados pessoais, não é possível sustentar a sua patrimonialização (DONEDA, 2006). O próprio termo "proteção de dados pessoais", em que pese remeter a uma falaciosa ideia da finalidade de tutela de algo externo à pessoa, tem por objetivo a não proteção dos dados *per se*, mas as pessoas às quais eles se referem (DONEDA, 2006).

apenas o indivíduo, mas igualmente o grupo social ao qual ele pertence, interesses coletivos e as gerações futuras (TEPEDINO; TEFFÉ, 2019).

As potencialidades tecnológicas avançam no sentido de promover uma erosão do que é "buscável", na referida terminologia de Lessig (1999), submetendo a condição de pessoa a um campo de descoberta. Diante dos múltiplos interesses que concorrem em busca do novo petróleo, a necessidade é de fortalecimento da perspectiva de controle. Quando se fala em controle não se quer remeter a um controle impossível em termos fáticos de ser realizado pelo titular no paradigma do *Big Data*, o que tem conduzido diversos pesquisadores, principalmente em uma orientação de matriz norte-americana, a sustentar uma análise voltada aos riscos de tratamento, uma evidência da autorregulação[68] e a uma abordagem contextual da proteção da privacidade.[69]

Em vista dos interesses que fundamentam a privacidade e a proteção de dados que, como visto, se eleva a uma abrangência coletiva, desde a dignidade até os próprios valores democráticos, a completa apreciação do problema não se dará se limitada ao traço visível de violação da privacidade (DONEDA, 2006). Aliada, portanto, à perspectiva de controle com base no regime jurídico que autorizará o tratamento dos dados pessoais, emerge a análise do contexto da utilização daqueles dados para verificar a sua legitimidade e a sua consonância com o próprio imperativo de controle. Neste sentido, como considera Simitis (2010, p. 1998-1999), "somente enquanto o respeito ao direito de cada pessoa também for entendido como um dever de sempre considerar o contexto do processamento, a autodeterminação pode ser garantida e, ao mesmo tempo, atender às exigências de uma sociedade democrática".[70]

Embora as variadas definições de privacidade que sucederam e sucederão, não importa uma defesa de prevalência ou de exclusividade, porque as diferentes definições baseiam-se em

---

[68] A autorregulamentação, enquanto derivada de fontes não estatais, é incompatível com a natureza de direito fundamental dos dados pessoais (DONEDA, 2006). De acordo com Simitis (2010), a autorregulação não se apresenta como um instrumento genuíno para afastar a intervenção legislativa, podendo, no máximo, suplementar a intervenção legal. Na proposta de Doneda (2006), a incidência da autorregulação poderia ser limitada aos contornos da matéria que se afastasse da natureza de direito fundamental. Parece razoável afirmar que depender do mercado para proteger dados pessoais é ilusório, na medida em que de regra o mercado é orientado por valores patrimoniais.

[69] A propósito, ver Nissenbaum (2010).

[70] Tradução livre com supressão de texto do original: "Most data protection laws may still begin by categorically asserting that processing of personal data can be either justified by the data subject's consent or by an explicit legal regulation. (…) As with labor relations, experiences in the credit area have consistently shown that a transfer of data concerning borrowers to third parties must be restricted to a few necessary cases. The German legislature tried to at least partially reach this result in the latest amendments to the Federal Data Protection Act. Thus, labor relations and credit policies illustrate that informational self-determination presupposes definitely more than the mere abstract acceptance of everyone's right to define the use of his or her data. The ability to influence the processing depends on its particular context. Therefore, only as long as the respect of every person's right is also understood as a duty to always consider the context of the processing can self-determination be guaranteed while also yielding to the exigencies of a democratic society" (SIMITIS, 2010, p. 1998-1999).

diferentes requisitos e operam em níveis diferentes (RODOTÀ, 2008). Sobretudo, importa a "inclusão progressiva de novos aspectos de liberdade num conceito ampliado de privacidade" (RODOTÀ, 2008, p. 15). A questão é se podemos nos considerar livres na era digital com a circulação dos nossos dados pessoais desvinculada de um paradigma de controle, que logicamente não se restringe aos nossos limites humanos. Sem controle, ainda que sem a existência de um dano direto ou da própria violação palpável da privacidade, os nossos dados circularão e repercutirão, mais cedo ou mais tarde, no desenvolvimento da nossa personalidade, ainda que não seja diretamente sinalizado. Permita-se a referência a Rodotà (2008, p. 37):

> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações. Além disso, é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em "controle". Aliás, a insistência em meios de controle exclusivamente individuais pode ser o álibi de um poder público desejoso de esquivar-se dos novos problemas determinados pelas grandes coletas de informações, e que assim se refugia em uma exaltação ilusória dos poderes do indivíduo, o qual se encontrará, desta forma, encarregado da gestão de jogo do qual somente poderá sair como perdedor. A atenção, consequentemente, deve deslocar-se dos meios de reação individual para instrumentos de controle social: e poderá ocorrer que, seguindo esse caminho, alguns meios que estavam tradicionalmente à disposição do indivíduo venham ser perdidos; perda, no entanto, que pode ser compensada pela criação, em nível coletivo, de um aparato de controle globalmente mais incisivo e vigilante do que o atual.

A defesa do controle dos dados pessoais resiste na medida em que o enfraquecimento do controle tornaria ainda mais precária a possibilidade de uma distribuição de poderes mais equilibrada na sociedade (RODOTÀ, 2008). A proteção de dados assume, portanto, o papel de definir a quem cabe o controle dos dados e, por conseguinte, proceder a uma forma de distribuição de poder que leve em conta o livre desenvolvimento da personalidade (DONEDA, 2006). O controle representa, em última análise, um instrumento de equilíbrio nessa nova distribuição de poder que vai se delineando, evidentemente irrealizável se limitado à perspectiva individual (RODOTÀ, 2008).

4. DADOS SENSÍVEIS

A partir da experiência europeia, Simitis (1990 apud MENDES, 2014) destaca que a evolução histórica da proteção de dados pessoais foi acompanhada do debate sobre os dados sensíveis. A primeira legislação nacional a respeito do tema na Suécia, em 1973, abordou a categoria dos dados sensíveis, assim como as normas que a seguiram da França (1978), Dinamarca (1978), Noruega (1978) e Luxemburgo (1979) (SIMITIS, 1990 apud MENDES, 2014).

Diante da possibilidade de classificar as informações pessoais em categorias ou subcategorias e, por conseguinte, utilizar tal classificação como pressuposto para a qualificação das normas aplicáveis, é possível identificar nessa setorização consequências diversas (DONEDA, 2006). Por um lado, poderia ser gerada uma fragmentação e, portanto, um enfraquecimento da tutela, mas se a categorização for situada em um panorama de tutela integral da pessoa seria justificada por uma especificação da abordagem direcionada à proteção das informações segundo as características próprias (DONEDA, 2006).

Nesta direção, Rodotà (2008) estabelece cinco premissas a um ambiente jurídico favorável à circulação de informações. Entre as premissas, tem pertinência direta com a categorização dos dados sensíveis duas delas: primeiro, deve ser estabelecida uma disciplina legislativa de base que se constitua essencialmente por cláusulas gerais e normas processuais, em outros termos, representando a moldura jurídica geral sobre o tratamento de informações (RODOTÀ, 2008). Conciliada com a primeira premissa, é necessária a previsão de normas voltadas a casos específicos referentes à atividade de determinados sujeitos ou à disciplina de categorias específicas de informações. A categoria dos dados sensíveis parece se inserir nessa proposta como integrante de um panorama de tutela integral da pessoa.[71]

A previsão da categoria dos dados sensíveis nas primeiras leis sobre proteção de dados era acompanhada de disposições mais severas que o regime comum de proteção de dados

[71] Além das duas premissas mencionadas, Rodotà (2008) destaca a necessidade de: uma autoridade administrativa independente, que eventualmente titularize poderes para adaptar a situações particulares os princípios previstos nas cláusulas gerais; previsão de uma disciplina de recurso à autoridade judiciária, não apenas nos sistemas nos quais tal se depreende de exigência constitucional, mas de modo geral, com o fim de enraizar nesta seara princípios análogos aos de um *Bill of Rights* ou do *Due Process*, no caminho de uma linha tendente a aproximar a matéria estudada dos direitos civis; e, por fim, previsão de um controle difuso pela iniciativa de grupos e cidadãos. De outra parte, é importante destacar a consideração de Doneda (2006, p. 357) no sentido de que: "Não é mero acaso que outros países com experiências mais frutíferas na proteção de dados pessoais tenham especificações bastante sofisticadas sobre a forma da tutela e seus mecanismos – já se afirmou que no enfoque dos direitos relacionados à tecnologia o recurso aos princípios não basta frente à maleabilidade e a dinamicidade do fenômeno tecnológico, que requer instrumentos com alto grau de objetividade para uma tutela objetiva dos interesses em questão".

pessoais não sensíveis. O *standard* protetivo maior se refletia nos seguintes aspectos: (i) ampliação das exigências legais com relação ao consentimento do indivíduo para o tratamento dos seus dados sensíveis; (ii) ampliação de exigências legais para o tratamento desses dados pelo responsável, como a intensificação das medidas de segurança; e (iii) aumento do controle por parte da autoridade administrativa para a autorização de armazenamento, processamento e circulação dos dados (MENDES, 2014).[72]

O fundamento da criação dessa categoria autônoma de dados pessoais se deu a partir do reconhecimento de que o armazenamento, o processamento e a circulação de certos tipos de dados acarretariam um maior risco à personalidade, sobretudo em vista de práticas discriminatórias (MENDES, 2014). Entre diversos dados associáveis à pessoa, alguns são especialmente aptos a favorecer processos sociais de exclusão e segregação, o que se apresenta como a chave de qualificação de determinados dados como sensíveis (KONDER, 2019).

Emergiu, portanto, a necessidade de exorbitar os cânones tradicionais então relacionados à privacidade, em prol de outro valor digno de tutela, no caso, a igualdade material (DONEDA, 2006). Como destaca Perlingieri (2006), o princípio da igualdade é o fundamento da tutela efetiva da personalidade. Assim, quando a privacidade era compreendida em termos de autonomia e liberdade, os dados sensíveis elevaram o debate para termos de igualdade (MENDES, 2014).[73] Nas palavras de Rodotà (2019, p. 36):

> É necessário enfatizar, de fato, que os dados sensíveis são aqueles relativos a saúde e vida sexual, as opiniões e ao pertencimento étnico ou racial, com uma lista semelhante

[72] A Lei Portuguesa de Proteção de Dados n. 67/98, que teve por fim transpor para a ordem jurídica de Portugal a Diretiva 95/46/CE, foi apontada como uma das mais rigorosas a respeito do tratamento dos dados sensíveis (MENDES, 2014). Entre as suas previsões, o art. 7, item I, determina a proibição do "tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos" (PORTUGAL, 1998, sem paginação). A proibição é excetuada no art. 7, item 3, quando estiverem presentes interesses vitais do próprio indivíduo se estiver incapacitado de dar o seu consentimento, os dados manifestamente tornados públicos pelo titular, bem como os dados necessários para fins de defesa judicial (PORTUGAL, 1998). Além disso, o consentimento do titular dos dados sensíveis apenas legitima o respectivo tratamento quando este for realizado por "por fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas actividades legítimas, sob condição de o tratamento respeitar apenas aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem consentimento dos seus titulares" (PORTUGAL, 1998, sem paginação). No entanto, "Mediante disposição legal ou autorização da CNPD, pode ser permitido o tratamento dos dados referidos no número anterior quando por motivos de interesse público importante esse tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, ou quando o titular dos dados tiver dado o seu consentimento expresso para esse tratamento, em ambos os casos com garantias de não discriminação e com as medidas de segurança previstas no artigo 15.º" (PORTUGAL, 1998, sem paginação). Em 25 de maio de 2018, como dito, entrou em vigor o GDPR, com natureza de regulamento e, portanto, dispensando a replicação dos seus comandos no direito interno de cada Estado-Membro.

[73] Na medida em que se reconhece o estreito vínculo entre a proteção de dados sensíveis e a igualdade material, Sarlet e Caldeira (2019) apontam os esforços legislativos, doutrinários e jurisprudenciais no sentido de se reconhecer o direito à proteção de dados sensíveis como um direito fundamental autônomo no contexto europeu.

> às encontradas nas normas relativas a casos de discriminações. Assim, somos confrontados com algo que vai além da simples proteção da vida privada e se apresenta como defensor da mesma igualdade entre as pessoas.[74]

A necessidade de proteção foi dilatada para além das informações relacionadas à esfera íntima da pessoa, compreendidas como aquelas que o interessado excluiria de qualquer tipo de circulação (RODOTÀ, 2008). Se é possível conceber um "núcleo duro" da privacidade, a partir de informações que tradicionalmente remetem a uma necessidade de sigilo, ganha cada vez mais relevância as informações que têm uma potencialidade discriminatória, mas não podem ser confinadas na esfera privada, porque integram a esfera pública, constituindo as convicções que a pessoa deve poder manifestar publicamente e que formam, portanto, a sua identidade pública (RODOTÀ, 2008). Não obstante, a origem racial ou étnica da pessoa, abrangente de uma noção de pertencimento ao respectivo grupo social, constituem dados sensíveis que não podem circunscrever a sua tutela a uma reserva privada.

Em realidade, se a necessidade de igualdade pode determinar uma maior transparência da esfera econômica privada, a partir da disseminação do caráter político do poder econômico, a igualdade também justifica a existência de um "núcleo duro" da privacidade com o fim de impedir a discriminação entre os cidadãos (RODOTÀ, 2008). A associação realizada por Rodotà (2008) entre a privacidade e as escolhas existenciais toma contornos mais profundos diante dos dados sensíveis.

É com a finalidade de garantir a plenitude à esfera pública que são determinadas rigorosas condições para a circulação dos dados sensíveis, assegurando, paradoxalmente, segundo Rodotà (2008), um forte estatuto privado. É neste sentido que os riscos conexos ao uso das informações levaram ao reconhecimento da autodeterminação informativa como um direito fundamental, e não apenas de um sigilo, a partir da tendência de tutelar uma série de "posições individuais e coletivas relevantes no âmbito da informação" (RODOTÀ, 2008, p. 96).[75]

De outra parte, os avanços tecnológicos fomentam diversos desafios diretamente associados aos dados sensíveis, a exemplo dos dados genéticos. A compreensão da natureza complexa do corpo da pessoa humana, como físico e eletrônico, ganha maior relevância em vista de que as "inovações tecnológicas permitem uma renovada decomposição do corpo mediante a coleta de informações que reduzem a identidade do sujeito a um só detalhe – a um

---

[74] Tradução livre de: "È necessario sottolineare, infatti, che i dati sensibile sono quelli che riguardano la salute e la vita sessuale, le opinioni e l'appartenenza etnica o razziale, con una elencazione analoga a quella che si trova nelle norme riguardanti i casi di discriminazione. Siamo così di fronte a qualcosa che eccede la semplice tutela della vita privata e si pone come presidio della stessa eguaglianza tra le persone".

[75] "(...) o reconhecimento de um direito fundamental não exclui que este se manifeste concretamente através da atribuição aos interessados de uma série aberta de poderes" (RODOTÀ, 2008, p. 96-97).

traço do rosto, ao reconhecimento da íris, impressões digitais", entre outros, de forma que o corpo em si está se tornando uma senha (RODOTÀ, 2004, p. 94).

Diferentemente dos dados sensíveis pertinentes à esfera pública, os dados sensíveis que se referem às condições de saúde, à genética e à biometria da pessoa não dizem respeito propriamente a escolhas que devem ser tuteladas. A rigor, são condições relativas ao corpo físico, elevadas ao patamar do corpo eletrônico diante das potencialidades tecnológicas, que não podem ser utilizadas em detrimento da pessoa, sob pena de violação à igualdade material.

Nesta esfera, a tutela do fluxo informacional deve abarcar não apenas aquelas informações destinadas do titular para fora, como usualmente costuma se conceber, mas igualmente as destinadas de fora para dentro, melhor dizendo, aquelas informações que o seu titular talvez queira exercer o direito de não saber (RODOTÀ, 2008). Como considera Mulholland (2012, p. 8), a relação não é mais negativa, no sentido de impedir o acesso às informações da pessoa, mas positiva, que no exemplo utilizado pela autora asseguraria à pessoa que o "conhecimento de determinado dado ou informação sensível pelo seu titular não é de fato obrigatório".[76]

Conquanto qualquer dado pessoal possa ser tratado com uma finalidade discriminatória, o potencial lesivo no tratamento dos dados sensíveis apresenta maior risco que a média, seja para a pessoa, seja para a coletividade (DONEDA, 2006). A categoria dos dados sensíveis é fruto de uma observação pragmática desse desnível de potencialidade lesiva entre os dados considerados sensíveis e os demais dados pessoais. Como analisa Doneda (2006, p. 163):

> (...) deve-se ter em conta que a diferenciação conceitual dos dados sensíveis atende a uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória é potencialmente maior – sem deixarmos de reconhecer que há situações onde tal consequência pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se prestem a fins legítimos e lícitos.

Embora a chave de qualificação dos dados sensíveis seja a relação com o princípio da igualdade material e, por conseguinte, a potencialidade discriminatória, a categorização normativa dos dados sensíveis, em experiências jurídicas diversas, como a seguir será pormenorizado, é associada, geralmente, a uma enumeração de tipos de dados, com base no seu conteúdo informativo. A exemplo da previsão da LGPD, são dados sensíveis aqueles que se relacionam à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato

[76] Recomenda-se a leitura do caso referenciado por Mulholland (2012) no qual Superior Tribunal de Justiça apreciou um pedido de indenização a título de danos morais por paciente que foi informado por laboratório de que era HIV positivo, sem que houvesse qualquer solicitação médica ou do paciente neste sentido.

ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" (BRASIL, 2018a, sem paginação). Ou seja, em abstrato, são determinados quais dados pessoais são considerados sensíveis e, portanto, teriam a aptidão de atrair um regime jurídico mais protetivo. A qualificação de um dado como sensível é fruto de uma valoração de que certas espécies de informações apresentam um elevado potencial lesivo ao seu titular, de acordo com uma configuração social (DONEDA, 2006).[77]

Para Konder (2019), a configuração de um dado pessoal como sensível não poderia ser estabelecida em abstrato, na medida em que à luz do contexto de utilização do dado e da combinação com outros dados disponíveis que pode ser verificada a potencialidade lesiva do seu tratamento. Nesta linha, Konder (2019) defende que o rol normativo que determina quais dados seriam sensíveis não pode ser compreendido como exaustivo. Em última análise, como anteriormente referido, a própria lógica que fundamenta a cláusula geral de tutela da pessoa parte da compreensão de que a realização da personalidade a partir de uma complexidade de situações subjetivas pode ostentar formas distintas, demandando uma normatização aberta (MORAES, 2010).

No caso do regime normativo dos dados sensíveis, a determinação de eixos específicos de qualificação jurídica acaba por "filtrar" variadas situações nas quais a dilatada potencialidade lesiva que a tecnologia apresenta no tocante ao tratamento de certos dados restaria desconsiderada, entregando-se à proteção ao regime comum dos dados pessoais. Raciocinando em sentido diverso, é possível questionar se, de fato, todos os tipos de dados elencados nessas normativas se qualificariam efetivamente como sensíveis. As divergências sobre os dados que deveriam integrar a categoria dos dados sensíveis são exemplificadas no relatório de aconselhamento sobre categorias especiais de dados, especialmente sobre os dados sensíveis, de 2011, do então constituído *Article 29 Data Protection Working Party*.[78]

Apesar das limitações inerentes à técnica legislativa da enumeração dos dados sensíveis de forma abstrata, recorrente em diversas experiências legislativas pelo mundo, lançam-se diversos desafios para a viabilidade de considerar a qualificação dos dados sensíveis de forma ampla. De plano, considerando que qualquer dado pessoal pode ser tratado com uma finalidade discriminatória, a qualificação em concreto acabaria por configurar quase todos os dados, senão

[77] Doneda (2006) refere a um aspecto temporal dos dados sensíveis, como a inscrição na maçonaria.

[78] "With regard to the data categories listed in Art. 8 (1) of the Directive, the majority of Working Party members are in favour of explicitly including genetic data in the catalogue of sensitive data. Some DPAs are also in favour of including biometric data and the creation of personal profiles. Some DPAs also proposed as additional categories data of minors, information about individuals' financial situation and data on an individuals geo-location, in particular when the latter is processed in the context of electronic networks" (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2011, p. 10).

todos, como sensíveis.[79] A insegurança jurídica gerada poderia comprometer diversas atividades, ou mesmo inviabilizá-las, o que vai na contramão na função reguladora do direito.[80]

Em que pese o reconhecimento das limitações na categorização dos dados sensíveis no âmbito normativo, a dose de pragmatismo que justificou a consideração da existência de dados pessoais especialmente sensíveis também deve se fazer presente quando da avaliação do modelo regulatório, sob pena de comprometer a própria tutela. Vale dizer, a viabilidade da aplicação do regime jurídico, bem como a própria efetividade de instrumentos regulatórios, devem ser rigorosamente enfrentadas para a defesa de outras abordagens normativas da categoria.[81]

4. 1 Dados sensíveis e direitos fundamentais

O problema da circulação de informações não pode ser solucionado somente a partir das noções correntes de privacidade, as quais não especificam qual é o objeto de proteção (RODOTÀ, 2008). Embora a construção da privacidade tenha evoluído para além de uma concepção patrimonial, diante da sua dinamicidade e historicidade, a sua compreensão é delineada pela autodeterminação individual da pessoa. Em outros termos, a partir da vertente da privacidade enquanto autodeterminação informativa, é possível apontar um conteúdo subjetivo, no sentido de que cada individualidade determinará a sua exposição no tecido social.

Em face dos dados de natureza sensível e da sua fundamentação, essa inserção e exposição da personalidade na sociedade, através do caráter relacional da privacidade referido por Doneda (2006), se relegado tão somente ao subjetivismo do titular pode se concretizar em fatores limitadores do livre desenvolvimento da personalidade. Com o fim de promover a tutela de direitos fundamentais, é imprescindível definir quando, onde, como e para que fins poderão

---

[79] É relevante realizar um paralelo com a qualificação do risco em uma determinada atividade para fins de caracterização da responsabilidade civil objetiva. A partir de Perlingieri, Raquel Salles (2011) evidencia que o próprio juízo que permite afirmar que uma atividade é perigosa deve ser averiguado *ex ante*, a partir das circunstâncias de fato existentes no exercício da atividade, e não com base em um evento danoso já verificado, sob pena de todas as atividades serem consideradas perigosas. Apenas para esclarecer a utilização dos termos "risco" e "perigo", tem-se por risco um "fenômeno subjetivizado", referente à valoração essencialmente econômica da álea assumida em uma empresa ou negócio por um sujeito, ao passo que perigo é compreendido como um "fenômeno objetivizado" relativo a uma ameaça notável de dano a terceiro, com uma alta potencialidade de lesão decorrente de uma determinada atividade, comportamento ou situação (COMPORTI apud SALLES, 2011, p. 131). Assim, verificado que perigo corresponde a uma projeção externa de dano, isto é, a terceiros, é a atividade perigosa que se identifica como fundamento da cláusula geral da responsabilidade civil objetiva inserta no artigo 927, parágrafo único, do Código Civil, apesar de o legislador ter utilizado o termo risco (SALLES, 2011).

[80] "O estabelecimento de limites ao tratamento de dados pessoais, apesar de apresentar um limite à liberdade do empreendedor (e, consequentemente, um custo), porém também representa uma plataforma segura na qual desenvolver a atividade negocial" (DONEDA, 2006, p. 259).

[81] A propósito, recomenda-se a leitura de Negri e Korkmaz (2019a).

ser coletados dados pessoais, de forma a restringir a sua utilização como ativo do mercado[82] ou como expressão do poder político do Estado (TEPEDINO; TEFFÉ, 2019).

No paradigma do *Big Data* e do avanço de sistemas cada vez mais complexos, não raro foge à pessoa a compreensão dos riscos subjacentes à circulação de um dado sensível, que poderá prejudicá-la, ainda que acobertado pela opacidade do tratamento dos dados. Em função das possibilidades tecnológicas, é crescente a relação que se estabelece entre a utilidade das informações e a capacidade de interferir no nosso cotidiano (DONEDA, 2006).

Uma significativa parcela das liberdades individuais é exercida, em termos concretos, através de estruturas que atribuem um papel relevante à comunicação e à informação (DONEDA, 2006). Na medida em que a informação cresce em relevância para múltiplos setores da vida social, a proteção dessas informações no sentido de que delas se faça um uso adequado estabelecerá uma relação direta com a fruição de direitos fundamentais na sociedade. Os direitos fundamentais formam, especialmente na ordem constitucional do Brasil, um conjunto complexo e extremamente heterogêneo de posições jurídicas (SARLET, 2012).

Em sede do ordenamento jurídico brasileiro, além do direito fundamental à igualdade consagrado no art. 5º, *caput*, da CRFB, o inciso IV do art. 3º constitucionaliza como objetivo fundamental da República "promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação" (BRASIL, 1988, sem paginação). É nesta linha que o texto constitucional consagra diversos direitos e garantias fundamentais que se associam, na sociedade contemporânea, à proteção da informação.

É com fundamento na possibilidade de utilização discriminatória, tanto por parte do mercado, quanto do Estado, que os dados sensíveis se associam a conjunturas em que podem estar presentes potenciais violações a direitos fundamentais (MULHOLLAND, 2018). Em outro ângulo, proteger dados sensíveis permite a efetivação de diversos direitos, como saúde, liberdades comunicativas, religiosa, de associação, entre outros (MULHOLLAND, 2018).

A partir de Westin (1967), Doneda (2006) observa que o aspecto informacional da privacidade desempenha funções essenciais nas perspectivas do indivíduo e da sociedade, na medida em que se erige como garantia de tolerância, liberdade de opinião, de associação e de religião, liberdade na pesquisa científica, lisura do processo eleitoral, entre várias outras finalidades que apresentam o contexto no qual situamos a privacidade. A proteção de dados

[82] De acordo com o Superior Tribunal de Justiça, em acórdão da relatoria da Ministra Nancy Andrigui, "o fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo 'mediante remuneração' contido no art. 3º, § 2º, do CDC deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor" (BRASIL, 2011c, sem paginação).

sensíveis como as opiniões políticas, a título de exemplo, autoriza uma participação mais ampla e igualitária do cidadão na vida pública (BAIÃO; GONÇALVES, 2014). Sobretudo, a própria fruição da igualdade e do livre desenvolvimento da personalidade estabelecem relação mais estreita com a proteção dos dados sensíveis, no sentido de prover campo para que a pessoa possa decidir livremente as questões fundamentais da sua vida, sem que as informações então geradas possam ser utilizadas para fins de estigmatização.

Anunciado em 2014, o *Social Credit Score* chinês ilustra de forma patente a relação entre tratamento de dados pessoais e o exercício de liberdades fundamentais. O sistema, que será implementado de forma obrigatória até 2020, tem por fim avaliar a "fidelidade" dos 1,3 bilhão de cidadãos chineses aos valores do país, bem como é conjecturado para substituir o debate público, no raciocínio de que o conhecimento dos dados a respeito dos cidadãos chineses possibilitaria compreendê-los, bem como as suas inclinações políticas (LARSON, 2018).[83] Além disso, com base no *score* do cidadão, seria determinado se ele teria acesso a um determinado serviço de saúde ou não, em qual escola o seu filho poderia estudar, entre vários outros. Apesar da China representar um exemplo extremo no panorama global em termos de controle e vigilância, é representativa dos riscos de exclusão dos cidadãos do acesso a diversos direitos fundamentais, como igualdade, liberdade, saúde, educação, moradia, além do pleno exercício democrático que concretamente não existe na China (MULHOLLAND, 2018).

De uma forma menos ostensiva, a utilização de dados sensíveis como uma informação relativa à saúde fragilizada de uma pessoa para a finalidade de definir uma taxa de juros relativa a empréstimo poderia ser determinante para inviabilizar àquela pessoa o acesso ao crédito, repercutindo no impedimento ou na dificuldade de acesso a bens e serviços, inclusive referentes à própria saúde, por exemplo. Em outra perspectiva, Frazão (2018c) evidencia a utilização de dados biométricos, como imagens faciais ou impressões digitais, para conhecer características físicas, comportamentais ou promover uma psicometria da pessoa. Na hipótese citada por Rodotà (2008), o conhecimento pelo empregador ou por parte de uma seguradora de informações relativas à infecção de uma pessoa pelo vírus HIV, ou de características genéticas específicas, são dados sensíveis com amplo potencial de gerar discriminações, que poderia se dar na forma de demissão, não admissão, recusa em firmar um contrato de seguro ou condicionamento do contrato a um alto prêmio, fora dos padrões regulares.

---

[83] "Hu Jintao, China's leader from 2002 to 2012, had attempted to solve these problems by permitting a modest democratic thaw, allowing avenues for grievances to reach the ruling class. His successor, Xi Jinping, has reversed that trend. Instead, his strategy for understanding and responding to what is going on in a nation of 1.4 billion relies on a combination of surveillance, AI, and big data to monitor people's lives and behavior in minute detail" (LARSON, 2018, sem paginação).

Proteger dados sensíveis, portanto, permite efetivar o direito à saúde, à liberdade de expressão e de comunicação, à liberdade religiosa, bem como a liberdade de associação, na medida em que, resguardando essas informações, resguarda a pessoa para se desenvolver livremente (RODOTÀ, 2008). Assim, se a associação entre privacidade e liberdade é cada vez mais forte (RODOTÀ, 2008), a autodeterminação informativa da pessoa toma contornos mais profundos com os dados sensíveis, a justificar a sua tutela diferenciada pela implicação direta em múltiplos direitos fundamentais.

4.2 Críticas à categoria dos dados sensíveis

É relevante apresentar determinadas críticas endereçadas à categoria dos dados sensíveis. Entre as mais referidas está o argumento da impossibilidade de definir antecipadamente quais os efeitos do tratamento de uma informação, independente da sua natureza (DONEDA, 2006). Em outros termos, destaca-se que dados não considerados sensíveis podem ser tratados com uma finalidade ou com um resultado discriminatório, bem como dados sensíveis podem ser tratados e não gerarem um efeito discriminatório, mas que, ao contrário, atenda a um propósito legítimo.

É possível compreender dentro dessa crítica a indicação de uma análise contextual do uso dos dados pessoais, sob o argumento de que uma abordagem abstrata não seria suficiente para assinalar a potencialidade lesiva de um tratamento de dados. Para Nissenbaum (2010), o determinante não seria o conteúdo da informação, mas o contexto informacional, abrangente da informação, da sua obtenção, da forma e da finalidade da sua utilização, a permitir considerar que a categorização dos dados sensíveis não seria suficiente para assegurar uma pretendida integridade no tratamento de dados, sobretudo diante dos avanços tecnológicos.[84]

Apesar do imperativo da circulação de informações econômicas e de uma tendência de restrição de coleta aos dados particularmente considerados sensíveis, permanece a necessidade de avaliar qualquer coleta de informações no contexto global em que ela ocorre (RODOTÀ, 2008). É por esta razão que Rodotà (2008, p. 77) reconhece a tendência de regras a respeito da circulação de dados considerarem contextos, funções e associações, na medida em que "nenhuma informação tem valor por si mesma, mas em virtude do contexto no qual está

[84] "One would also expect a range of varying restrictions to apply to information of different types depending on whether or not its release may cause harm, whether or not it is about intimate activities and relationships, and whether or not it is the legitimate business of government. But these are not the only variations that conceivably may affect restrictions we may wish to prescribe on the flows of personal information" (NISSENBAUM, 2010, p. 126).

inserida, ou pelas finalidades para as quais é utilizada, ou pelas outras informações às quais tem sido associada".

Além disso, como adverte Doneda (2006), a classificação dos dados como sensíveis não deve ser absoluta e nem deve funcionar como última instância de legitimação para o tratamento daqueles dados.[85] A rigor, é certo que atender formalmente aos cânones normativos para o tratamento de dados pessoais não dispensa uma verificação concreta do uso que deles se faça.

Embora se admita a importância de uma análise contextual do uso das informações, não é razoável sedimentar a proteção de dados pessoais em um casuísmo, sobretudo diante da incipiência da proteção de dados no Brasil. Em vista do princípio da igualdade material, uma análise tão somente casuística e contextual repercutiria em sérios riscos de insegurança jurídica e desigualdade nas práticas de tratamento de dados. É neste sentido que Simitis (2010) sustenta que qualquer normatização de dados pessoais orientada pelo contexto deve ser concebida e aplicada como parte de um sistema uniforme, como parte de uma fundamentação comum, além de uma principiologia a ser estabelecida como norte da análise.[86]

Rouvroy (2016), por seu turno, sustenta que no contexto do *Big Data* as discriminações não são geradas a partir de uma lógica tradicional, ou seja, de uma subsunção a categorias pré-existentes consideradas como aptas à promoção de processos discriminatórios.[87] A rigor, pouco importariam os dados de uma pessoa individualmente considerada, mas a possibilidade de enquadrá-la em um modelo gerado através de um processamento de dados (ROUVROY, 2016). Portanto, verificam-se novas formas de discriminação sem que seja necessário recorrer à lógica tradicional que costuma integrar a categoria dos dados sensíveis (MARTINS, 2019). De acordo com Rouvroy (2016, p. 28), nas análises baseadas em *Big Data*[88]

---

[85] O mencionado caso da *Cambridge Analytica*, no panorama geral de proteção de dados, é exemplificativo da necessidade de uma análise contextual do uso de dados, porque em sua grande parte os dados utilizados estavam amparados no consentimento dos titulares. Foi a verificação do desvio de finalidade, entre outros, a partir de uma análise da concreta utilização daqueles dados que se evidenciaram as práticas abusivas às quais eles serviram.

[86] "In sum, there is a pressing need to thoroughly review regulatory approaches that, as in Europe, primarily rest on omnibus laws. Any further reflection should be guided by two requirements. First, legislators must limit themselves to the few core principles that every regulation of the use of personal data must observe. Second, all context-oriented rules must be conceived and applied as part of a uniform system based on a common foundation. (…) Divergences may occur, but such exceptions should still fulfill two conditions: lawmakers should provide a specific justification for deviations, and should compensate any potential reduction in data protection with clearly defined measures. Thus, an exception from the common foundation would neither imperil the flexibility of the regulation nor the protection of personal data" (SIMITIS, 2010, p. 2001-2002).

[87] "It is important here, in order to appreciate fully what is at stake, to make a clear distinction between two separate ways of categorising individuals and/or their behaviour. In the traditional processes of classification which it was possible to conduct before the digital revolution and the new Big Data-type assessment techniques, the categories (statistical, social, cultural and others) existed before the categorisation procedures, which consisted in looking at these pre- existing categories and working out which features could be used to identify or predict that a person belonged to a group and hence to place that person into the corresponding category" (ROUVROY, 2016, p. 28).

[88] Tal Z. Zarsky (2017) chega a apontar a incompatibilidade das práticas do *Big Data* com balizas de proteção de dados, como a limitação da coleta e sua minimização, categorias especiais de dados e o tratamento automatizado.

> o objetivo dos processos de criação de perfil em grupos ou *clustering*, por outro lado, é realçar categorias anteriormente desconhecidas, social e visualmente imperceptíveis, com base na análise de dados, sem qualquer referência a informações pré-existentes sobre esses novos grupos ou categorias. Nos processos de *clustering*, os indivíduos são colocados por outra pessoa - que pode ser um sistema automático de processamento de dados - em "categorias" social e existencialmente sem significado, imperceptíveis (porque emergem apenas à medida que o processo se desenrola) e, na maioria das vezes, sem a possibilidade de estar ciente do que está acontecendo ou se reconhecer.[89]

Nesta perspectiva, Rouvroy (2016) defende uma abordagem funcional do tratamento de dados, que ao invés de dificultar ou impedir o acesso a dados como os considerados sensíveis, considera uma análise concreta e setorial das informações em vista do fim a que se destinam, ganhando relevo uma própria estrutura de fiscalização diante do estudo empírico e técnico para cada setor (MARTINS, 2019). Em que pese a relevância das considerações de Rouvroy (2016), a regulação setorial dos dados a partir de contextos de atividades específicas vem sendo desaprovada, na medida em que tem sido vista pelos controladores de dados como uma oportunidade de limitar as restrições do uso intencional de dados (SIMITIS, 2010). Os riscos de uma fragmentação e, por conseguinte, um enfraquecimento da tutela (DONEDA, 2006), devem ser assinalados na proposta de uma abordagem funcional.[90]

Em última análise, as práticas discriminatórias, ilícitas ou abusivas, são vedadas pelo princípio da não discriminação consagrado no art. 6º, inciso IX, da LGPD (BRASIL, 2018a), independentemente da qualificação do dado como sensível. Entretanto, diante dos dados sensíveis, a maior probabilidade da utilização discriminatória desses dados em face dos demais dados pessoais fundamentou um juízo *ex ante* para estabelecer, além da principiologia aplicável ao regime geral dos dados pessoais, o regime jurídico próprio dos dados sensíveis.

4.3 Potencialidade lesiva na era digital

[89] Tradução livre de: "The aim of the processes of group profiling or clustering on the other hand is to highlight previously unknown, socially and visually imperceptible categories on the basis of data analysis without any reference to pre-existing information about these new groups or categories. In clustering processes, individuals are placed by another person – which can be an automatic data processing system – into socially and existentially a-significant "categories", which are imperceptible (because they emerge only as the process unfolds), and most often without any possibility of being aware of what is happening or recognising themselves".

[90] Uma tutela fragmentada abre margem para a consideração de interesses setoriais nem sempre legítimos, como o exemplo pragmático da presença de *lobby* no modelo norte-americano (DONEDA, 2006).

A abordagem dos dados sensíveis deve ter em vista a crescente importância da informação no tecido social, o paradigma da hiperconectividade[91] e o progresso das potencialidades tecnológicas baseadas em dados.[92] Com o desenvolvimento da inteligência artificial, enquanto subcampo da informática que tem por fim habilitar o desenvolvimento de computadores capazes de emular a inteligência humana ao realizar tarefas, no conceito do pesquisador de Stanford, McCarthy (1956), a humanidade é conduzida a desafios sem precedentes.[93]

Os sistemas de IA são cada vez mais utilizados fora de um modelo de regras pré-fixadas por algoritmos simples, mas a partir da "alimentação" de grande quantidade de dados para que os próprios sistemas construam os seus padrões decisionais complexos, associando mais dados a uma maior acurácia (DONEDA et. al., 2018). A crescente complexidade dos algoritmos é atribuída à utilização de *machine learning*, *deep learning* e *neural networks*,[94] com base nos quais podem ser geradas conclusões e decisões automatizadas inescrutáveis aos próprios programadores (KNIGHT, 2017).[95] O corpo eletrônico da pessoa é instrumentalizado no processo em que a utilidade dos sistemas automatizados é crescente em função da maior disponibilidade de dados (DONEDA; ALMEIDA, 2016).

---

[91] A exemplo, como noticiado pelo Jornal O Globo, a companhia Samsung previa na sua política de privacidade o alerta para o risco de captura e transmissão de dados sensíveis para terceiros no caso da utilização da função de reconhecimento de voz, nos seguintes termos: "esteja ciente que se suas palavras incluírem dados pessoais ou outras informações sensíveis, essa informação estará entre os dados capturados e transmitidos para terceiros pelo uso do reconhecimento de voz". Disponível em: https://oglobo.globo.com/economia/samsung-adverte-cuidado-com-que-voce-diz-em-frente-sua-tv-inteligente-15286181. Acesso em: 08 ago. 2017.

[92] No paradigma do *Big Data* "(…) os dados passam a ser analisados não mais em pequenas quantidades ou por amostras, mas em toda a sua extensão. Há um salto quanto ao volume de dados processados, tornando-se possível correlacionar uma série de fatos (dados), estabelecendo-se entre eles relações para desvendar padrões e, por conseguinte, inferir, inclusive, probabilidades de acontecimentos futuros" (BIONI, 2019, p. 41).

[93] O patamar tecnológico atual está restrito à "IA fraca", que se destina à realização de tarefas específicas. A tecnologia capaz de simular o raciocínio humano, se moldando a diferentes situações, é denominada de "IA forte" ou "IA geral", a qual até o momento não foi desenvolvida (MAGRANI, 2019).

[94] A dinamicidade da tecnologia apresenta dificuldades de conceituação desses sistemas, no entanto com a finalidade de esclarecer o leitor procurou-se trazer definições frequentes para uma melhor compreensão da proposta deste trabalho. *Machine learning*, ou aprendizado de máquina, é o gênero de qualquer metodologia ou técnica que emprega dados para desenvolver novos padrões e conhecimentos, com a aptidão de gerar modelos preditivos sobre dados e de modificar os seus padrões decisionais de forma autônoma (OTTERLO apud MAGRANI, 2019, pp. 25-26). *Deep learning* refere-se a um princípio mais geral de aprendizagem de vários níveis de composição, não necessariamente inspirados nos sistemas neurais humanos (MAGRANI, 2019). *Neural networks* representam uma rede de vários processadores simples, geralmente cada um deles com memória local, constituindo um sistema adaptativo complexo que pode alterar a sua estrutura interna com base nos dados fornecidos (MAGRANI, 2019).

[95] "The workings of any machine-learning technology are inherently more opaque, even to computer scientists, than a hand-coded system. This is not to say that all future AI techniques will be equally unknowable. But by its nature, deep learning is a particularly dark black box" (KNIGHT, sem paginação). Neste sentido, é possível identificar argumentos no sentido de que a explicabilidade de como os sistemas de IA chegaram a uma determinada conclusão como um direito fundamental (KNIGHT, 2017), sobretudo diante da sua interferência na vida da pessoa.

Enfrentar o tema da proteção dos dados sensíveis sem atentar às potencialidades tecnológicas dos sistemas aos quais os dados são submetidos seria infrutífero. Os desafios lançados à proteção de dados sensíveis no paradigma da IA, além do *Big Data*, podem ser ilustrados com o programa *Deep Patient*. Em 2015, um grupo de pesquisa no *Mount Sinai Hospital*, em Nova Iorque, decidiu utilizar *deep learning* em um grande banco de dados composto por informações referentes a 700 mil pessoas (KNIGHT, 2017). O *Deep Patient*, como ficou conhecido, quando testado em novos registros foi capaz de prever doenças futuras, além de antecipar possíveis distúrbios psiquiátricos em pacientes, como a esquizofrenia, de difícil diagnóstico médico (KNIGHT, 2017). A partir de dados sensíveis, como os relativos à saúde, o programa traçou sérios prognósticos, sem que fosse possível saber como chegou a uma conclusão (KNIGHT, 2017).

De outra parte, os dados pessoais também são utilizados como insumo para tratamentos automatizados destinados a produzir decisões sem a apreciação humana, com o fim de avaliar aspectos da personalidade do titular dos dados, produzindo efeitos na sua esfera jurídica ou a afetando de maneira significativa (RODOTÀ, 2019). Cohen (2000) destaca os dados sensíveis, como aqueles relativos às condições genéticas e preferências sexuais ou religiosas, direcionados para decisões de emprego, seguro de saúde, decisões de habitações, entre outros.

As decisões automatizadas são cada vez mais recorrentes no tecido social e responsáveis pela definição de perfis, prognoses, concessão de crédito, seleção profissional, acesso a bens e serviços, alocação de recursos públicos, dosimetria de penas, entre outros, o que muitas vezes foge à ciência do afetado pela decisão.[96] As possibilidades tecnológicas que até então se expressavam quantitativamente se ampliam em uma dimensão qualitativa, assumindo faculdades habitualmente consideradas humanas (DONEDA et. al., 2018).

A infiltração dessas tecnologias com aptidão decisória no tecido social sem mecanismos de controle para assegurar a autonomia da pessoa conduziu Rodotà (2019) a nos alertar para a "ditadura dos algoritmos", como origem de novas discriminações, na qual o cidadão não é mais livre, mas prisioneiro de mecanismos que não sabe ou não pode controlar. [97] A gravidade do tema se acentua quando algoritmos podem ser considerados opiniões embutidas em uma forma

[96] "Already, mathematical models are being used to help determine who makes parole, who's approved for a loan, and who gets hired for a job. If you could get access to these mathematical models, it would be possible to understand their reasoning. But banks, the military, employers, and others are now turning their attention to more complex machine-learning approaches that could make automated decision-making altogether inscrutable" (KNIGHT, 2017, sem paginação).

[97] "L'algoritmo disegna le modalità di funzionamento di larghe aree delle nostre organizzazioni social, e così redistribuisce poteri" (RODOTÀ, 2019, p. 38).

matemática (O'NEIL, 2017), além do fato de que esses sistemas falham (KNIGHT, 2017), embora a aparência de neutralidade.[98]

A forte presença das relações remotas na sociedade atual, na qual a representação da pessoa frequentemente pode se restringir aos seus dados, aponta nas possibilidades de equívoco ou de discriminação a partir dos algoritmos ou dos dados utilizados uma restrição indevida na autonomia da pessoa, limitando sua liberdade de ação, suas decisões econômicas e mesmo as existenciais (LYON, 2003 apud DONEDA et. al., 2018). Como anuncia o Rodotà (2019, p. 40):

> Quando a relação entre poderes públicos e privados e as pessoas vem baseada em uma mineração ininterrupta de dados, na coleta ilimitada de qualquer informação a respeito deles e depois confiada ao algoritmo, as pessoas são transformadas em abstrações, a construção das suas identidades é subtraída de sua consciência, seu futuro confiado ao determinismo tecnológico. Tudo isso afeta os direitos fundamentais, põe em questão a livre construção da personalidade e a autodeterminação, impondo, assim, perguntar-nos se e como a sociedade do algoritmo pode ser democrática.[99]

É possível sintetizar em dois grupos as razões pelas quais existe potencialidade de discriminação no uso de algoritmos (DONEDA et. al., 2018). Primeiro, na medida em que o funcionamento do algoritmo é condicionado ao *input* de dados, a qualidade da decisão automatizada, do *output* do sistema, dependerá da qualidade dos dados processados. Se utilizados modelos estatísticos com base em dados com alto potencial discriminatório, como os dados sensíveis, é provável que a decisão seja discriminatória (DONEDA et. al., 2018).

Segundo, por operar através de padrões de classificação, os sistemas impõem dificuldades para os que não se encontram com a maioria, potencializando a estigmatização e a repressão de minorias (DONEDA et. al. 2018).[100] A preferência por condutas conformes aos perfis historicamente dominantes é um obstáculo ao livre desenvolvimento da personalidade e a uma dinâmica social emancipatória e democrática, na medida em que a construção autônoma da individualidade se contrapõe a um poder externo que apresente padrões de normalidade e exerça um controle ostensivo, porém sutil (BAIÃO; GONÇALVES, 2014).

---

[98] Acrescente-se a necessidade de conhecer o *input* de dados do algoritmo e o método estatístico usado, frequentemente acobertados pelo sigilo comercial (DONEDA et. al., 2018).

[99] Tradução livre de: "Quando la relazione tra i poteri pubblici e privati e le persone viene basata su di un ininterrotto *data mining*, sulla raccolta senza limiti di qualsiasi informazione che le riguardi, e affidata poi all'algoritmo, le persone sono trasformate in astrazioni, la costruzione delle loro identità viene sottratta alla loro consapevolezza, il loro futuro affidato al determinismo tecnologico. Tutto questo incidi sui diritti fondamentali, mette in discussione la libera costruzione della personalità e l'autodeterminazione, imponendo così di chiedersi se e come la società dell'algoritmo possa essere democratica".

[100] O uso de correlações e não de causalidades nas análises baseadas em *Big Data* é um desafio adicional nesse campo. Dados aparentemente insignificantes podem ser utilizados para fins discriminatórios, na medida em que são infinitas as correlações estatísticas sobre fatos de interesse dos tomadores de decisão, sem qualquer relação de causalidade com as atividades daquele setor (DONEDA et. al., 2018).

Powles e Nissenbaum (2019) asseveram que sistemas conduzidos por dados sobre o mundo reproduzem e ampliam discriminações de gênero,[101] raça[102] e desigualdades sociais.[103] De outra parte, Barocas (2014) sustenta que embora as atividades de *data mining*[104] podem ser eficientemente utilizadas para fins discriminatórios, esta finalidade não é inerente ao seu processo.[105] São demandados, portanto, parâmetros éticos e normativos, em vista da necessidade de transparência, controle e correção dos dados utilizados como *inputs* do sistema (DONEDA et. al., 2018). Neste sentido, determinadas formas de governança atuam sobre os dados fornecidos aos algoritmos (DONEDA; ALMEIDA, 2016).

No GDPR, por exemplo, é vedada a utilização de dados sensíveis como insumo para esses sistemas, conforme o art. 22º, item 4, salvo se forem previstas "medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular" (UNIÃO EUROPEIA, 2016, p. 46).[106] Na LGPD, não há uma previsão específica para os dados sensíveis no âmbito das decisões automatizadas, embora o §2º, do art. 20,[107] estabeleça a possibilidade da ANPD realizar auditoria para a verificação de aspectos discriminatórios no tratamento automatizado, desde que resguardados os segredos comercial e industrial. Ganha relevância, portanto, a abordagem dos dados sensíveis como insumo para esses sistemas, na medida em que a sua caracterização pela potencialidade discriminatória pode repercutir em resultados discriminatórios, de forma a ampliar a sua potencialidade lesiva.

---

[101] Ficou clássico o artigo assinado por um grupo de professores da Universidade de Boston que demonstra a existência de discriminações sexistas nos sistemas de aprendizado de máquina em razão da fonte mais comum de dados, a Internet, ser permeada de correlações como "dona de casa − ela" e "gênio − ele" (PASCUAL, 2019).

[102] Sobre filtragens automatizadas de currículos profissionais, um grupo de pesquisadores do MIT enviou, em 2002, 5.000 currículos em resposta a ofertas de emprego publicadas em jornais, sendo que a metade dos perfis inventados tinham nomes tipicamente associados a brancos e a outra metade a negros. Como resultado, os perfis associados a brancos receberam um número 50% maior de ligações, indicando viés étnico (PASCUAL, 2019).

[103] Como apontam Doneda e Almeida (2016), a seleção, a classificação, a correlação e outras técnicas acabam por repetir vieses ambientais em razão da capacidade de imitar as condições sociais e pessoais.

[104] "Consiste na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grande de dados, com o auxílio de instrumentos estatísticos e matemáticos. (...) A possibilidade de se obter informações úteis a partir do *data mining* cresce à medida que aumenta a quantidade de informação em 'estado bruto' disponível, bem como as técnicas para obter a dita informação útil" (DONEDA, 2006, p. 176).

[105] "This brief survey reveals that commentators see at least three rather different ways through which data mining gives rise to discrimination. The first involves conscious intentions to disadvantage members of protected class in ways that would be difficult to detect; the second focuses on problems with the data mining process itself that result in seemingly avoidable errors; and the third concerns the unwelcome effects when data mining significantly enhances certain decision-makers' powers of discernment. Describing each of these as discrimination can be confusing because each raises different concerns" (BAROCAS, 2014, sem paginação).

[106] "4. As decisões a que se refere o n.o 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.o, n.o 1, a não ser que o n.o 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular" (UNIÃO EUROPEIA, 2016, p. 46).

[107] "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" (BRASIL, 2018a, sem paginação).

Entre as decisões automatizadas é de se destacar o *profiling*, no qual os dados pessoais, seja em uma perspectiva coletiva ou individual, são tratados para obter uma "metainformação", consistente em uma síntese de hábitos, preferências, entre outros registros da vida da pessoa, com a possibilidade de ser utilizado para apontar tendências comportamentais (DONEDA, 2006).[108] Rodotà (2008) sustenta que a formação de perfis baseados em dados sensíveis pode gerar discriminação seja porque dados pessoais que aparentemente não se qualifiquem como sensíveis podem se tornar sensíveis se contribuem para a elaboração de um perfil, seja porque a esfera individual da pessoa pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas.[109]

A partir da captação em *bits* do ser humano, a sua classificação e segmentação geram verdadeiros estereótipos que estigmatizam a pessoa perante os seus pares (BIONI, 2019). Vale dizer, a finalidade de "rotular" pessoas e associá-las a um padrão de hábitos e comportamentos assume um grave potencial discriminatório, sobretudo diante dos dados sensíveis (TEFFÉ; MORAES, 2017).[110] Emerge a lição de Rodotà (2019) no sentido de que a diversidade das pessoas, situadas em contextos diversos, são irredutíveis a um esquema, porque devem ser respeitadas na sua singularidade, o que parece estar na contramão dos avanços tecnológicos.[111]

---

[108] O perfil então gerado é transformado na representação virtual daquela pessoa, configurando não raras vezes o único aspecto visível daquele indivíduo, tendente a confundir-se com a própria pessoa, de certo modo definindo-a (DONEDA, 2006).

[109] Como destaca Frazão (2018c, sem paginação), "discussões mais recentes apontam para a ocorrência de fenômeno de publicidade comportamental voltado à formação de perfis de consumo, fato que se relaciona diretamente à regulação do tratamento de dados pessoais, em especial os dados sensíveis. Na verdade, na seara consumerista, assim como na seara trabalhista, são inúmeros os riscos da utilização de tais dados para praticar toda sorte de discriminações e violações a consumidores, empregados e candidatos a emprego em processos de seleção ou recrutamento". Dois casos ocorridos nos EUA que se referiram à contratação de serviços médicos e de seguridade mencionados por Mulholland (2018) são exemplificativos dos malefícios da utilização do *profiling*. No primeiro caso, seguradoras utilizaram dados pessoais de vítimas de violência doméstica que constavam em bancos de dados públicos. O tratamento desses dados gerou uma discriminação negativa a essas vítimas, na medida em que sugeriu que mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez (MULHOLLAND, 2018). No outro caso, relacionado aos dados sensíveis relativos à saúde, quando uma pessoa é acometida de um derrame, instituições financeiras, ao descobrir a ocorrência, davam início à cobrança de empréstimos realizados (MULHOLLAND, 2018).

[110] "Com efeito, um acervo suficientemente amplo de informações permite a elaboração de perfis de consumo, o que se, de um lado, pode ser utilizado para incrementar e personalizar a venda de produtos e serviços, de outro, pode aumentar o controle sobre a pessoa, desconsiderando sua autonomia e dificultando a participação do indivíduo no processo decisório relativo ao tratamento de seus dados pessoais, de seu patrimônio informativo" (TEFFÉ; MORAES, 2017, p. 121). Neste sentido, como adverte Rodotà (2008, p. 62), "torna-se possível não só um controle mais direto do comportamento dos usuários, como também a identificação precisa e atualizada de certos hábitos, inclinações, interesses, preferências. Daí decorre a possibilidade de uma série de usos secundários dos dados, na forma de 'perfis' relacionados aos indivíduos, família, grupos. Trata-se de uma nova 'mercadoria' cujo comércio pode determinar os tradicionais riscos para a privacidade: mas pode, sobretudo, modificar as relações entre fornecedores e consumidores de bens e serviços, reduzindo a autonomia destes últimos de tal forma que pode chegar a incidir sobre o modelo global de organização social e econômica".

[111] Com efeito, o âmbito propício ao pleno desenvolvimento da personalidade demanda que seja assegurada a maior autonomia possível, conferindo à pessoa a faculdade de rever e construir a sua identidade fora de uma lógica cristalizada (BAIÃO; GONÇALVES, 2014).

A repercussão na esfera de liberdade individual é direta, na medida em que pressupõe um determinado comportamento futuro de forma antecedente, restringindo a autodeterminação da pessoa e contrapondo-se à sua realidade (DONEDA, 2006). Em outubro de 2017, o *Article 29 Data Protection Working Party* publicou as *Guidelines on Automated Individual Decision Making and Profiling*, que apesar de não vinculantes, são referências interpretativas fundamentais do GDPR. No documento, dentre as situações evidenciadas que podem afetar a esfera jurídica e os interesses dos titulares dos dados pessoais está o tratamento de dados sensíveis (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2017).[112]

A Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica 2015/2103 (INL), endereçou especificamente o tema dos dados sensíveis. De acordo com o documento, o posicionamento dos robôs em espaços tradicionalmente protegidos e íntimos, aliado à capacidade de extrair informações referentes a dados sensíveis e transmiti-los, apresenta-se como uma ameaça importante à privacidade das pessoas (UNIÃO EUROPEIA, 2017).

Entre alguns dos múltiplos desafios que se apresentam para a proteção da pessoa na era digital, os dados sensíveis ganham uma particular relevância, na medida em que os avanços tecnológicos parecem dilatar a sua potencialidade lesiva. Entretanto, com o imperativo de reafirmar o valor fundamental da pessoa neste cenário, releva analisar os mecanismos de tutela específicos para os dados sensíveis no marco regulatório geral brasileiro.

[112] As *Guidelines on Automated Individual Decision Making and Profiling* delimitam exemplos de atividades consideradas de alto risco, como avaliações ou *scorings*, decisões automatizadas com efeitos jurídicos ou análogos, monitoramento sistemático, dados sensíveis, dados processados em larga escala, *datasets* que forem combinados ou misturados, uso inovador ou aplicação tecnológica ou soluções organizacionais, transferência de dados entre fronteiras fora da União Europeia e processamentos que impedem titulares de dados do exercício de direitos, da contratação ou da utilização de determinado serviço (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2017).

5 MECANISMOS DE TUTELA DOS DADOS SENSÍVEIS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Com o imperativo de promover um controle sobre o fluxo informacional, tanto em uma abordagem individual, quanto coletiva, foi promulgada a Lei Geral de Proteção de Dados Pessoais – n.º 13.709, em 14 de agosto de 2018. Entre os seus fundamentos, expressamente elencados no art. 2º, da LGPD, estão o respeito à privacidade, a autodeterminação informativa, o livre desenvolvimento da personalidade e a dignidade da pessoa.[113] Antes do advento da LGPD, o Brasil já contava com mais de quarenta normas que tratavam direta ou indiretamente de questões relacionadas à privacidade e à proteção de dados pessoais, a serem complementados ou substituídas com a sua vigência (MONTEIRO, 2018).

O âmbito de aplicação da LGPD diz respeito ao tratamento de dados pessoais da pessoa natural, independente de o responsável pelo tratamento ser uma pessoa física ou jurídica, bem como do meio em que os dados estiverem situados ser físico ou digital, como prescreve o art. 1º (BRASIL, 2018a). Além disso, como dispõe o rol exemplificativo do art. 5º, inciso I, da LGPD,[114] por tratamento de dados entende-se qualquer operação à qual os dados sejam submetidos, indicando uma vasta abrangência da norma.

Em experiências jurídicas diversas, no panorama mundial, não é possível identificar uma uniformidade no que poderia ser considerado como um dado pessoal. Em outros termos, a definição do que é considerado dado pessoal na esfera jurídica e, portanto, a atração de um regime de proteção, depende da conformação normativa estabelecida em um determinado ordenamento. É neste sentido que se fala em uma abordagem restrita ou ampla de dado pessoal.

Na conceituação restrita, "por dado pessoal entende-se a representação de fatos sobre pessoa identificada, isto é, representação referente a alguém que se conhece e individualiza em meio a certo grupo ou coletividade" (MACHADO; DONEDA, 2018, p. 105). De acordo com o *Article 29 Data Protection Working Party* (2007, p. 12), "a identificação é normalmente obtida através de informações específicas que podemos chamar de 'identificadores' e que

[113] "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais" (BRASIL, 2018a, sem paginação).

[114] "Art. 5º (...) 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" (BRASIL, 2018a, sem paginação).

mantêm uma relação particularmente privilegiada e próxima com o indivíduo".[115] A conceituação restrita do dado pessoal é exemplificada nos Estados Unidos, que tipifica no seu ordenamento jurídico os dados pessoais no *Privacy Act*, de 1974, e no *Children's Online Privacy Protection Act* (COPPA) (MACHADO; DONEDA, 2018).[116]

De outra parte, a conceituação ampla de dado pessoal estende o seu alcance para a pessoa identificável, de forma que há dado pessoal independente da presença de identificadores diretos ou indiretos que diferem precisamente um indivíduo (MACHADO; DONEDA, 2018). O entendimento que considera a identificabilidade de pessoa natural não só por esforços do responsável pelo tratamento, mas também de qualquer pessoa, é chamada de absoluta (MACHADO; DONEDA, 2018). O Considerando 26 do GDPR deixa clara a adoção da perspectiva absoluta, nos seguintes termos:

> Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica (UNIÃO EUROPEIA, 2016, p. 5).[117]

A LGPD adotou o modelo europeu para definir o conceito de dado pessoal de uma forma ampla, como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL,

---

[115] Tradução livre de: "identification is normally achieved through particular pieces of information which we may call 'identifiers' and which hold a particularly privileged and close relationship with the particular individual".

[116] De acordo com o U. S. Code, Title 15, Chapter 9, § 6501 (8): "Personal information. The term "personal information" means individually identifiable information about an individual collected online, including — (A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph" (ESTADOS UNIDOS, 1998, sem paginação).

[117] O critério dos meios suscetíveis de identificação do titular dos dados depende de aspectos contextuais, como os próprios avanços tecnológicos, o que gera uma caracterização dinâmica do que seria ou não considerado como dado pessoal (PURTOVA, 2018). Nas palavras de Purtova (2018, p. 47), "The resulting standard of the reasonable likelihood of identification is quite broad and context-dependent, leading to one major consequence: the status of data as 'personal' is dynamic, ie the same data-set may not obviously be personally identifiable at the start of processing, or from the perspective of the controller, given the tools and data available to him, but become, or appear to have been all along, identifiable from the perspective of another person or once the circumstances change". A propósito, recomenda-se a leitura de Purtova (2018) a respeito de em um futuro próximo as normas sobre proteção de dados serem aplicáveis a todas as esferas, na medida em que tudo será ou conterá dados pessoais. De acordo com a autora: "in the near future everything will be or will contain personal data, leading to the application of data protection to everything: technology is rapidly moving towards perfect identifiability of information; datafication and advances in data analytics make everything (contain) information; and in increasingly 'smart' environments any information is likely to relate to a person in purpose or effect" (PURTOVA, 2018, p. 1).

2018a).[118] Nestes termos, de acordo com a LGPD não existe dado pessoal insignificante, estando todos eles na abrangência da normativa, com exceção das limitações dispostas no art. 4º.[119] Por consequência, os dados que não podem ser associados a uma pessoa identificada ou identificável não estariam diretamente na abrangência da norma, como é o caso dos dados anônimos.[120] Entre os dados pessoais regulados pela LGPD, é identificada a categoria específica dos dados pessoais de natureza sensível.

O ordenamento jurídico brasileiro conta com a normatização da categoria de dados sensíveis desde a promulgação da Lei de Cadastro Positivo – n.º 12.414 de 2011. O art. 3º, § 3º, inciso II, dispõe sobre a proibição de anotações em bancos de dados voltados para análise de crédito de "informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas" (BRASIL, 2011a). Ou seja, o propósito de analisar a concessão de crédito a partir do estabelecimento de um cadastro positivo não autoriza a utilização de dados sensíveis.

Especificamente, dados sensíveis como os genéticos, já haviam sido objeto de tratamento jurídico, como na Lei n.º 12.037 de 2009 a respeito de identificação criminal do civilmente identificado, enquanto regulamentação do art. 5º, inciso LVIII, da CRFB, com fundamento na segurança (BRASIL, 2009). É relevante observar que a LGPD, em seu art. 4º, inciso III, exclui da sua abrangência o tratamento de dados pessoais realizados exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou de atividades de investigação e repressão de infrações penais (BRASIL, 2018a), o que lança múltiplos desafios para a proteção dos dados sensíveis que não estão no alcance da LGPD.[121]

---

[118] O conceito amplo de dado pessoal já se fazia presente no ordenamento jurídico brasileiro na Lei de Acesso à Informação – Lei nº. 12.527/2011, a qual definiu informação como "aquela relacionada à pessoa natural identificada ou identificável" (BRASIL, 2011b).

[119] O art. 4º da LGPD exclui expressamente da sua abrangência o tratamento de dados pessoais: "I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - 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 nesta Lei" (BRASIL, 2018a, sem paginação).

[120] "Com uma abordagem orientada pelo risco, há o surgimento de propostas que visualizam entre o dado pessoal e o dado anônimo um gradiente de cores ou um *continuum* com categorias que superam a lógica binária dado pessoal/dado anônimo, informações a que se aplicam o regime de proteção de dados pessoais/informações a que não se aplicam o regime de proteção de dados pessoais. É nesse contexto que se coloca a ideia de dado pseudonimizado" (MACHADO; DONEDA, 2018, p. 111).

[121] No nível infralegal, é exemplo de regulamentação dos dados sensíveis o Decreto n. 7.950, de março de 2013, a respeito do Banco Nacional de Perfis Genéticos e a Rede Integrada de Bancos de Perfis Genéticos (BRASIL, 2013).

Com efeito, o estabelecimento de um regime jurídico específico para os dados sensíveis tem por finalidade conduzir a sua regulação a cânones mais rígidos, o que a LGPD buscou endereçar na Seção II intitulada "Do Tratamento de Dados Pessoais Sensíveis", dentro do Capítulo II sobre "Tratamento de Dados Pessoais" (BRASIL, 2018a).[122] O Projeto de Lei 5.276 de 2016, que acabou por integrar em significativa parte o conteúdo da LGPD, estabelece que a finalidade do tratamento normativo diferenciado dos dados sensíveis é a de impedir a discriminação da pessoa com base nas suas informações:

> (...) O anteprojeto estabelece normas específicas para o tratamento de dados cujo tratamento possa ensejar discriminação ao titular (os chamados 'dados sensíveis', por se referirem a orientação sexual, convicções religiosas, filosóficas ou morais, ou opiniões políticas, por exemplo), prevendo como regra geral que esses dados não devem ser tratados e que ninguém pode ser obrigado a fornecer informações de tal natureza a seu respeito, ressalvadas as hipóteses previstas em lei, assim como um regramento mais rígido quando o tratamento desses dados for permitido (BRASIL, 2016, sem paginação).

Como observa Mulholland (2018), o propósito de um tratamento limitado dos dados sensíveis é o de evitar a sua eventual utilização para fins que não atendam aos fundamentos republicanos do Estado Democrático de Direito. Com essa premissa, a LGPD buscou endereçar o tema, definindo no seu art. 5º, inciso II, o dado pessoal sensível como

> 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 (BRASIL, 2018a, sem paginação).

A rigor, não é estabelecido um conceito sobre os dados sensíveis, de forma que a sua compreensão se dá a partir de determinados tipos de dados. Em princípio, o dado pessoal sensível é delimitado por intermédio de eixos de *fattispecie*, ou seja, através de um esquema taxativo e, portanto, limitado de situações jurídicas objetivas, embora dentro de cada um dos tipos de dados é possível vislumbrar uma gama de situações relativas ao conteúdo informacional. Qualificado um dado como sensível, é atraído o regime jurídico mais severo.

É relevante proceder a um cotejo com o modelo europeu neste aspecto. O GDPR estabelece um regime jurídico específico para os dados sensíveis, mais rigoroso que o aplicável aos dados pessoais não considerados sensíveis. O fundamento dessa tutela diferenciada é destacado nos Considerandos 51 e 71 do GDPR, respectivamente:

---

[122] A Seção II, dentro do Capítulo II da LGPD, não trata exclusivamente dos dados sensíveis, apesar do seu título, a exemplo da abordagem dos dados anonimizados.

> 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 (UNIÃO EUROPEIA, 2016, p. 10).
>
> (...) 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 ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas (UNIÃO EUROPEIA, 2016, p. 14).[123]

Apesar de não referir à nomenclatura "dados sensíveis" na disposição da norma, o art. 9, item 1, enumera os dados considerados como tal. Além disso, apesar de, assim como a LGPD, não apresentar um conceito propriamente do que seria um dado sensível, define no seu art. 4º três tipos de dados indicados no art. 9, item 1. Respectivamente dispõe o GDPR:

> É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (UNIÃO EUROPEIA, 2016, p. 38).
>
> 13) «Dados genéticos», 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;

[123] Não obstante, ao mencionar diversas situações nas quais são verificados riscos para os direitos e liberdades das pessoas, os dados indicados no GDPR como sensíveis são citados no Considerando 75, que assim dispõe: "O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados" (UNIÃO EUROPEIA, 2016, p. 15). Sobre a proteção de dados de crianças e adolescentes, permita-se remeter a Negri, Fernandes e Korkmaz (2019).

> 14) «Dados biométricos», 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;
> 15) «Dados relativos à saúde», dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde (UNIÃO EUROPEIA, 2016, p. 34).

A redação do dispositivo se estrutura em uma forma proibitiva do tratamento de dados a partir de uma enumeração dos dados que seriam considerados sensíveis. Todavia, essa proibição é excetuada em dez circunstâncias que são dispostas no item 2, que se fundamentam desde o consentimento qualificado do indivíduo, da proteção dos seus interesses vitais, até razões consideradas como sendo de interesse público.

É possível identificar uma identidade dos tipos de dados disciplinados como sensíveis na LGPD e no GDPR, com a adoção de técnica jurídica similar. A propósito, as críticas inicialmente identificadas em desfavor de uma abordagem taxativa dos dados sensíveis podem ser vislumbradas com maior nitidez na exemplaridade dos dados pessoais referentes a condenações criminais, que não são enumerados como sensíveis na LGPD e no GDPR. Contudo, o GDPR disciplinou separadamente o tratamento[124] desses dados, estabelecendo requisitos como o controle da autoridade pública e o estabelecimento de garantias adequadas para os direitos dos titulares dos dados.[125] Na LGPD, de outra parte, não há qualquer previsão de proteção específica desses dados, embora a patente potencialidade discriminatória.[126]

É também possível referir o tratamento de dados relacionados às capacidades cognitivas das pessoas ou ao seu desempenho profissional, que, coletadas em situações específicas, podem circular e serem utilizadas, no regime comum de proteção de dados da LGPD, para atender ao

---

[124] Segundo o art. 4º, item 2, do GDPR, tratamento se define por: "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (UNIÃO EUROPEIA, 2016, p. 33).

[125] O artigo 10, do GDPR prescreve que "O tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas com base no artigo 6.o, n.o 1, só é efetuado sob o controle de uma autoridade pública ou se o tratamento for autorizado por disposições do direito da União ou de um Estado-Membro que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados. Os registos completos das condenações penais só são conservados sob o controlo das autoridades públicas" (UNIÃO EUROPEIA, 2016, sem paginação).

[126] Como se sabe, o ordenamento jurídico brasileiro é permeado de institutos que têm por fim assegurar ao indivíduo que, após cumprida a sua penalidade imposta através do devido processo legal, se reabilite para a vida em sociedade, podendo nela se reintegrar. É inquestionável que essas informações afetas a condenações criminais revelam nítida potencialidade de gerar situações de discriminação e desigualdade e que, se tratadas, por exemplo, com uma finalidade econômica e atendendo a esta lógica, poderiam cristalizar o indivíduo na condição de condenado, mitigando o exercício da sua autonomia.

interesse legítimo ou a uma finalidade econômica do controlador[127] dos dados (BRASIL, 2018a). Rodotà (2008) destaca que uma atividade antidiscriminatória a partir das informações poderia fundamentar a resistência a formas de controle sobre a atividade de trabalho e o comportamento do trabalhador na empresa. O próprio nível de produtividade ou a avaliação cognitiva poderiam ser utilizadas com a finalidade de discriminar abusivamente o trabalhador.

Na experiência jurídica da Argentina, que exerceu um papel de vanguarda em sede de proteção de dados na América do Sul, a Lei 25.326 de 2000 normatizou a categoria dos dados sensíveis, definindo-os da seguinte forma: "dados sensíveis são aqueles que revelam sua origem racial e étnica, opiniões políticas, convicções religiosas, filosóficas ou morais, afiliação sindical e informações sobre sua saúde ou vida sexual"[128] (ARGENTINA, 2000).[129] As convicções morais da pessoa são apontadas como um dado sensível, de acordo com a norma argentina, o que não encontra correspondente na LGPD ou no GDPR.

Em outra perspectiva, é necessário questionar se todos os dados elencados como sensíveis na LGPD se relacionariam diretamente com o princípio da igualdade material e ostentariam um potencial discriminatório nítido. A exemplo, é possível questionar se convicções filosóficas seriam por sua natureza qualificáveis como dados sensíveis. Com efeito, uma abordagem crítica da LGPD nestes termos ganha relevância para uma melhor compreensão do seu alcance, embora a sua abordagem sobre os dados sensíveis indique para uma taxatividade na qualificação dos dados considerados sensíveis.

De outra parte, entre a principiologia consagrada no art. 6º da LGPD, se associam mais estreitamente aos dados sensíveis os princípios da finalidade e o da não discriminação (MULHOLLAND, 2018).[130] O princípio da finalidade tem uma relevante aplicação prática, pois "com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros,

---

[127] De acordo com a LGPD, o controlador define-se por "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", ao passo que o operador é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (BRASIL, 2018a, sem paginação).

[128] Tradução livre de: "Los datos sensibles son aquellos que revelan tu origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a tu salud o a tu vida sexual".

[129] Em 2000, a Argentina promulgou a Lei 25.326 sobre proteção de dados pessoais, que igualmente regulamentou o processo da ação de *habeas data*. À época, como apontado por Doneda (2006), a lei inspirou-se nas linhas da Diretiva 95/46/CE e teve seu reconhecimento de adequação pela União Europeia, em 2003. Em 2016, foi dado início a um projeto de reforma da legislação argentina sobre proteção de dados. O Governo da Argentina, inclusive, disponibiliza uma plataforma *online* com amplos recursos para que os titulares dos dados pessoais conheçam os seus direitos de uma forma interativa, promovam consultas sobre as bases de dados registrados, acessem serviços, entre outros. Disponível em: https://www.argentina.gob.ar/aaip/datospersonales. Acesso em: 09 set. 2019.

[130] A LGPD é orientada pelos seguintes princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (BRASIL, 2018a). A análise da principiologia consagrada na LGPD revela uma preocupação sobre qual deve ser a carga participativa da pessoa no fluxo das suas informações (BIONI, 2019).

além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade, (fora da qual haveria abusividade)" (DONEDA, 2006, p. 216). Com o imperativo do princípio da finalidade, a LGPD determina a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018a, sem paginação).

O princípio da não discriminação estabelece a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (BRASIL, 2018a, sem paginação). Em última análise, na medida em que é vedado o uso discriminatório associado à ilicitude ou à abusividade, parece admissível um tratamento distintivo com base nos dados pessoais, desde que lícito e não abusivo (MULHOLLAND, 2018).[131] A determinação do que seria ilícito ou abusivo, uma vez não estabelecido na LGPD, se daria segundo os critérios definidos pelas regras expressas de direito civil e penal, bem como por princípios como a boa-fé objetiva (MULHOLLAND, 2018), além da própria força normativa da CRFB como baliza nesta análise.

Mulholland (2018) questiona se esse tratamento segregado, desde que lícito ou não abusivo, poderia ser realizado em face dos dados sensíveis, notadamente se consideradas as características personalíssimas por eles veiculadas. Neste âmbito, deve-se ter em vista que a diferenciação pode se erigir como um instrumento direcionado à concretização da igualdade material, por vezes necessário. Portanto, como baliza, o princípio da não discriminação deve ser aplicado em todas as situações em que o uso de dados, sejam sensíveis ou não, gere algum tipo de desvalor da pessoa ou induza resultados inequitativos (MULHOLLAND, 2018). Como propõe Mulholland (2018), o princípio da não discriminação erige-se como uma base de sustentação da tutela dos dados sensíveis, sobretudo diante do exercício de prerrogativas democráticas e do acesso a direitos sociais, como o trabalho, a saúde e a moradia.

Realizadas as presentes considerações sobre a categorização dos dados sensíveis na LGPD, como parte da ampla abrangência dos dados pessoais, releva identificar os mecanismos de tutela estabelecidos especificamente no regime jurídico dos dados pessoais sensíveis. A rigor, a partir de uma comparação com o regime comum dos dados pessoais, pretende-se analisar a prescrição de um padrão normativo significativamente mais severo.

5.1 O consentimento qualificado

[131] Como analisa Mulholland (2018, p. 164), "aparentemente, seria legítimo ao operador de dados realizar tratamentos de segregação, no sentido de diferenciação, sem que, com isso leve a consequências excludentes que poderiam ser consideradas ilícitas".

O consentimento emerge como um poder conferido à pessoa para modificar a sua própria esfera jurídica, podendo ser compreendido como síntese da atuação da autonomia privada e como instrumento por excelência da manifestação da escolha individual, inclusive no campo das diversas configurações da personalidade (DONEDA, 2006). Neste âmbito, a evolução da tecnologia promoveu uma ampliação das possibilidades de escolhas que podem repercutir diretamente na personalidade, como é o caso da utilização de dados pessoais (DONEDA, 2006).

A partir da normativa reservada ao consentimento é possível identificar a natureza do sistema de proteção de dados pessoais. Se de índole patrimonialista, Doneda (2006) assevera que o consentimento assumirá uma função "predominantemente legitimadora" para colocar os dados no mercado e, em um arranjo extremo, conduzir estes dados a um processo de *commodification*, ou seja, transformá-los em *commodity*. Compreendida a privacidade como uma liberdade negativa, com a atribuição de autodeterminação ao indivíduo sobre a sua esfera privada, o consentimento é constituído como elemento essencial do exercício deste poder (DONEDA, 2006). Por outro lado, o alcance do consentimento pode ser reduzido em determinados sistemas, com a possibilidade de condicionar o uso de dados pessoais a uma específica disposição legislativa ou a um instrumento designado em lei (DONEDA, 2006).

É importante assinalar o risco de se transpor o instituto do consentimento do seu contexto tradicional dos mecanismos negociais para o âmbito da proteção de dados sem proceder a uma adequação, sobretudo porque a adaptação de uma estrutura formal a uma realidade que apresenta com o seu meio de origem uma semelhança enganosa pode não raro compreender uma escolha ideológica (DONEDA, 2006). A inadequada atribuição de uma natureza negocial ao consentimento reforçaria o sinalagma entre o consentimento para o tratamento dos dados pessoais e uma vantagem econômica por parte daquele que consente, fortalecendo, portanto, um esquema proprietário para a proteção de dados pessoais (TEPEDINO; TEFFÉ, 2019).

Embora o consentimento seja um caminho entre a *regulation* e a *deregulation*, são múltiplos os perigos de erigi-lo como um pilar para a proteção de dados (RODOTÀ, 2008).[132] A partir de uma perspectiva unidimensional e proprietária dos dados pessoais, a utilização do consentimento nesta lógica acaba por comprometer a dimensão coletiva da proteção de dados e pode gerar consequências para o próprio interessado (RODOTÀ, 2008). Além disso, a relação

[132] Para as linhas centrais do debate entre *regulation* e *deregulation* ver Doneda (2006, p. 390-393).

de dependência verificada entre o consentimento e a fruição de bens e serviços muitas vezes acrescenta à sua concessão a autorização para o uso secundário de dados (RODOTÀ, 2008).

A utilização do consentimento pode ser "instrumentalizada pelos interesses que pretendem que a sua disciplina não seja mais que uma via para legitimar a inserção dos dados pessoais no mercado" (DONEDA, 2006, p. 375). Com o verniz de juridicidade, o consentimento poderia, em última análise, legitimar uma apropriação do corpo eletrônico da pessoa por parte do mercado com diversas repercussões em desfavor da própria pessoa e da coletividade. A partir de Rodotà, Doneda (2006) evidencia que uma falsa premissa de conceder o consentimento como instrumento para determinar livremente a utilização dos dados pessoais poderia, por parte do Estado, representar um "falso álibi" para não interferir na situação que, em realidade, demandaria a sua atuação positiva na defesa de direitos fundamentais.

Por esta razão, a análise do consentimento deve ser situada no paradigma de que proteção de dados diz respeito à personalidade, e não à propriedade (RODOTÀ, 2008). Na medida em que a proteção de dados envolve diretamente elementos da personalidade, a especificidade do consentimento demanda uma funcionalização da sua própria natureza jurídica, como a impossibilidade de disposição dos dados pessoais (DONEDA, 2006). Vale dizer, o papel do consentimento para a proteção de dados pessoais deve ser ponderado, sob pena de, amparado na tecnicidade, neutralizar a atuação de direitos fundamentais (DONEDA, 2006).

Traçadas linhas gerais que devem nortear a análise do consentimento, compete-nos adentrar à sua disciplina na LGPD sobre os dados sensíveis. No regime comum de proteção de dados pessoais, a LGPD define o consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018a, sem paginação). De outra parte, para o tratamento dos dados sensíveis, a normativa estabelece uma qualificação do consentimento, para exigir que adicionalmente seja dado "de forma específica e destacada, para finalidades específicas", de acordo com o art. 11, inciso I (BRASIL, 2018a, sem paginação).

A possibilidade de desmembrar o consentimento em espécies com requisitos próprios, de acordo com a natureza dos interesses em um certo perfil de tratamento de dados pessoais, é o que estabelece um regime diferenciado para o consentimento relativo ao tratamento de dados sensíveis, aproximando-o do seu campo de interesses (DONEDA, 2006). Como considera Rodotà (2008), o consentimento do titular dos dados sensíveis deve ser qualificado, porque estamos diante de um contratante vulnerável, caracterizado pelo comprometimento da liberdade substancial no momento da manifestação da vontade.

Por detrás de toda adjetivação ou qualificação do consentimento está uma modulação da carga participativa exigida de cada pessoa para o tratamento dos seus dados (BIONI, 2019).[133] Em face da potencialidade lesiva subjacente ao tratamento dos dados sensíveis, portanto, a carga participativa deve ser máxima, o que se relaciona com o grau de consciência a respeito do tratamento por parte do titular, como verdadeira advertência dos riscos anormais daquela prática, na observação de Bioni (2019).[134]

No regime geral do consentimento na LGPD é apresentada a sua caracterização como livre. A princípio, a fundamentação do consentimento reside na possibilidade de autodeterminação do indivíduo em relação aos seus dados (DONEDA, 2006). Assim, ao se referir ao consentimento livre, quer-se assegurar o poder de o titular escolher entre aceitar ou não a utilização dos seus dados, sem quaisquer intervenções ou situações que viciem o seu consentimento, com o imperativo de averiguar a assimetria entre as partes envolvidas (TEPEDINO; TEFFÉ, 2019).

Com fundamento na liberdade das escolhas pessoais, o seu exercício livre manifesta-se menos no momento do consentimento em si, do que na possibilidade de concedê-lo ou não, e reside justamente neste poder que se limitado pela estrutura negocial perderia a sua razão de ser (DONEDA, 2006).[135] Nesta direção, é indispensável verificar qual o é "poder de barganha" do cidadão com relação ao tratamento dos seus dados, quais são as opções da pessoa com relação ao tipo de dados coletados e ao uso que deles será feito (BIONI, 2019). Na advertência de Doneda (2006, p. 373):

> O confronto com situações reais revela que, em tais situações, a pessoa que opta por exercer o seu poder de autodeterminação e não revelar seus dados pessoais, no mais das vezes se vê alijado do acesso a determinados bens ou serviços – para cuja fruição o fornecimento dos dados era um passo essencial. A disparidade de meios entre a pessoa, de quem são exigidos os dados pessoais, e aquele que os solicita faz com que a verdadeira 'opção' seja tantas vezes a de "tudo ou nada", "pegar ou largar".

A lei estabelece que se o tratamento de dados pessoais for apresentado como condição para o fornecimento de produto ou serviço ou para exercício de direito, o titular deverá ser

---

[133] A LGPD demanda a existência de um consentimento qualificado em face de diferentes situações, quais sejam, quando há o envolvimento de terceiros que não tenham relação direta com o titular para o tratamento dos seus dados (art. 7, §5º), em vista da vulnerabilidade das crianças e adolescentes (art. 14, §1º), na transferência internacional de dados para um país que não ostente o mesmo patamar protetivo estabelecido no Brasil (art. 33, VIII) e, por fim, para o tratamento dos dados de natureza sensível (BRASIL, 2018a).

[134] A propagação do acesso à internet veio acompanhada da aparência de absoluta neutralidade e como possibilidade de acesso a um simulacro de cidadania digital, o que repercutiu em um considerável deslocamento de contingente populacional para a rede, sem maior zelo com os seus dados (SARLET; CALDEIRA, 2019).

[135] A existência de condicionamentos que excluem uma real possibilidade de escolha manifesta-se, por exemplo, na cumulação da autorização da pessoa à qual os dados se referem para a realização de perfis com base nas informações coletadas, como exemplificado por Rodotà (2008).

informado com destaque sobre esse fato, bem como sobre os meios dos quais poderá se valer para o exercício dos direitos elencados no art. 18, da LGPD, de acordo com o art. 19, §3º da norma (BRASIL, 2018a). Como apontam Tepedino e Teffé (2019), é possível ler esse dispositivo como uma proposta de regulação da lógica binária das políticas chamadas de tudo ou nada (*take-it-or-leave-it-choice*), nas quais para ter acesso a um determinado serviço ou produto, o indivíduo deve aceitar todas as condições apresentadas. Contudo, é de se questionar a suficiência da informação em destaque sobre o condicionamento, quando está em questão a real possibilidade de não consentir para o tratamento dos dados. Aliás, o direito à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa, previsto no inciso VIII, do art. 18 (BRASIL, 2018a), embora funcione como um instrumento de transparência, não parece significativo em termos de liberdade no ato de consentir.

Com o propósito de garantir uma determinação por parte do indivíduo de quais dados pessoais poderão ser utilizados, para quais finalidades e sob quais termos, ganha relevância o chamado "consentimento granular" como forma de permitir uma oxigenação dos processos de tomada de decisão, através do qual a pessoa pode emitir autorizações fragmentadas no tocante ao fluxo de seus dados (BIONI, 2019). Nesta perspectiva, abre-se margem "para que o controle dos dados seja fatiado de acordo com cada uma das funcionalidades que são ofertadas e se deseja ter e que demandam, respectivamente, tipos diferentes de dados" (BIONI, 2019, p. 197-198). Essa granularidade emerge como um fator caracterizante da própria liberdade no ato de consentir, como pode ser extraído do Considerando 43, do GDPR:

> A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. 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 (UNIÃO EUROPEIA, 2016, p. 8).

De outra parte, a vontade individual não é um valor em si, mas um "vetor vazio" (SCHREIBER, 2014). Com fundamento na dignidade humana, o exercício da liberdade é legitimado na medida em que corresponder ao seu fundamento (SCHREIBER, 2014), repercutindo na necessária verificação dos valores atendidos por aquela manifestação da vontade. Vale dizer, não pode ser tomado como válido um consentimento que comprometa os

vínculos sociais de intimidade em relação à própria pessoa (BAIÃO; GONÇALVES, 2014). Nesta direção, para além das limitações pertinentes ao próprio instituto do consentimento, é possível inferir a sua fragilidade como instrumento legitimador do tratamento de dados sensíveis em vista do próprio princípio da não discriminação, que, em última análise, poderia deslegitimar um tratamento de dados consentido, mas que pudesse gerar uma discriminação ilícita ou abusiva em desfavor da pessoa à qual os dados se referem. Não obstante, está em debate quais são os contornos de um consentimento livre, quando não raro a pessoa não tem consciência da potencialidade lesiva do uso daquele dado, sobretudo diante dos exponenciais avanços tecnológicos.

Rodotà (2008) defende a impossibilidade de operar o consentimento em todas as situações, principalmente em se tratando dos dados necessários à proteção dos valores individuais. Diante de vários interesses em jogo, sobretudo do mercado, emerge a necessidade de tutelar os dados de todos aqueles que poderiam sofrer uma "perda de dignidade" ou de autonomia através do seu consentimento para a coleta, tratamento e difusão das informações (RODOTÀ, 2008).

Em face de fortes desníveis de poder, o consentimento individual é profundamente limitado, a exemplo do recolhimento pelo empregador de convicções políticas e sindicais do empregado, do requerimento de exames de doenças como HIV, informações genéticas, entre outros, qualificados como dados sensíveis (RODOTÀ, 2008). A proteção de dados, na medida em que se configura como expressão de liberdade e dignidade, não admite a utilização dos dados pessoais para submeter o indivíduo a uma situação de vigilância (RODOTÀ, 2008).

Assim sendo, o aumento ou a redução do papel decisional do titular se erige como mecanismo de proteção da pessoa (DONEDA, 2006). O fundamento, em realidade, está na compreensão de que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no mais elevado alto grau, que não pode ser atendido exclusivamente por uma decisão individual (DONEDA, 2006). Nesta direção, a alínea "a" do item 2, do art. 9, do GDPR estabelece que o direito da União ou de um Estado-Membro pode afastar o consentimento como hipótese legitimadora do tratamento de um dado sensível (UNIÃO EUROPEIA, 2016).[136] No entanto, não há uma previsão correspondente na LGPD.

[136] Rodotà (2019) faz referência ao regime jurídico dos dados sensíveis no artigo 26 do antigo Código de proteção de dados italiano que prescreve, para além do consentimento escrito do interessado para autorizar o tratamento, a prévia autorização da Autoridade Garante. Não bastaria, portanto, a vontade do interessado, mas a ela deve se acrescentar a autorização do sujeito público em avaliar a admissibilidade social e compensar a fragilidade relacionada a estes dados que incidem profundamente sobre a personalidade (RODOTÀ, 2019).

Em outro eixo, a LGPD exige no regime jurídico geral do consentimento que este seja informado.[137] O objetivo da previsão é o de prover o titular dos dados das informações que se façam necessárias ao entendimento das circunstâncias adjacentes ao tratamento dos seus dados pessoais. Com a finalidade de diminuir a assimetria entre as partes envolvidas, prescreve a LGPD que à pessoa sejam fornecidas "informações transparentes, adequadas, claras e em quantidade satisfatória acerca dos riscos e implicações do tratamento de seus dados" (TEPEDINO; TEFFÉ, 2019, p. 301).[138] Maior relevo ganha o consentimento informado ao se considerar a opacidade que permeia o tratamento de dados (DONEDA, 2006).

A exigência de que o consentimento seja realmente informado toma por premissa, no mínimo, a leitura dos termos de consentimento para tratamento de dados, os quais devem ser fidedignos às práticas pertinentes ao tratamento, em sentido amplo. Ocorre que a forma de apresentação dos usuais termos de consentimento se dá de maneira não atrativa para o titular dos dados, melhor dizendo, são termos geralmente extensos que se valem de uma linguagem elaborada e visualmente não estimulam a leitura do seu conteúdo.

Em termos concretos, Madrigal (2012) relata uma pesquisa realizada no ano de 2008 por Lorrie Faith Cranor e Aleecia McDonald, à época no Carnegie Mellon, identificando que se o titular dos dados fosse ler todos os termos de consentimento a respeito dos seus dados pessoais ao ano gastaria 76 dias de trabalho. Ao calcular um custo hipotético de oportunidade

---

[137] A partir da análise do desenvolvimento do consentimento informado na área da saúde, Sarlet e Caldeira (2019, p. 12) destacam que "historicamente a obrigatoriedade do consentimento informado remonta às graves atrocidades vivenciadas durante a II Guerra Mundial. A banal utilização de prisioneiros nos campos de concentração em experiências médicas, dentre outros agravos, gerou uma nervura na História e conduziu à formulação do Código de Nuremberg (1947), que se constitui até hoje como o documento mais relevante da ética da investigação em seres humanos. Estas circunstâncias motivaram ainda a celebração de convenções, designadamente a Declaração Universal dos Direitos Humanos (1948), a Convenção Europeia dos Direitos Humanos (1950) e a Convenção de Helsinque (1964), revista no Brasil, mais especificamente na cidade de Fortaleza em 2013, constituindo-se em verdadeiros alicerces éticos e jurídicos para a proteção da informação de saúde na internet, notadamente por reconhecerem a dignidade, a liberdade e a autonomia do ser humano. Igualmente digno de nota foi a elaboração do Relatório Belmont (1978) e do Guia de Boas Práticas Clínicas adotado pela OMS em 1995, que têm contribuído para a defesa da privacidade dos pacientes e dos participantes em ensaios clínicos, relacionando-a diretamente com o fortalecimento do consentimento informado como uma relação gnoseológica".

[138] "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; 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; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. § 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. § 2º Na hipótese em que o consentimento é requerido, 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" (BRASIL, 2018a, sem paginação). Sobre uma abordagem dos direitos do titular dos dados em uma perspectiva dos remédios, permita-se remeter a Souza e Silva (2019).

a partir de balizas econômicas, o "custo da privacidade", de acordo com as pesquisadoras, seria de 781 bilhões de dólares no contexto pesquisado dos Estados Unidos, com tendência de crescimento nos dias atuais (MADRIGAL, 2012).

A rigor, o consentimento deve estar inscrito em uma constelação de circunstâncias para ser pleno e válido, demandando "uma temporalidade estrita ao uso previamente informado e esclarecido, o qual tenha sido ampla e livremente objeto de deliberação de pessoa autônoma" (CALDEIRA; SARLET, 2019, p. 23). Contudo, na conjuntura brasileira são múltiplos os desafios para que essas circunstâncias sejam concretamente verificadas, sobretudo em vista das altas taxas de analfabetismo funcional (CALDEIRA; SARLET, 2019).[139]

A natureza dos interesses em questão demanda que seja averiguada a condição de compreensão efetiva das implicações daquele tratamento, bem como dos seus termos por parte da pessoa à qual os dados se referem para caracterizar o consentimento informado (DONEDA, 2006). Nesta direção, o consentimento deve ser avaliado de forma realista diante dos limites gerados pela assimetria de poder entre aquele que consente e o responsável pelo tratamento dos dados.[140] Nesta linha, Sarlet e Caldeira (2019, p. 13) destacam a importância do consentimento

> como fruto de uma relação gnoseológica, ou seja, como um processo de conhecimento em que, no caso, devem ser previamente esclarecidos em linguagem clara, precisa, apropriada e suficiente, a pertinência, a finalidade, a adequação, o tempo da coleta, o armazenamento, o tratamento e a transmissão dos dados obtidos no sentido de possibilitar a renúncia, a alteração, o uso, a cessão, e a disponibilidade ou a recusa daquele que consente.

Por este ângulo, Sarlet e Caldeira (2019) se referem à natureza processual[141] do consentimento, a demandar a garantia de todas as condições, inclusive as temporais e as informacionais, para a livre tomada de decisão em um paradigma de responsabilidade. O princípio da transparência interfere nesse processo, na medida em que assegura à pessoa "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os

---

[139] "Três em cada dez jovens e adultos de 15 a 64 anos no País - 29% do total, o equivalente a cerca de 38 milhões de pessoas - são considerados analfabetos funcionais. Esse grupo tem muita dificuldade de entender e se expressar por meio de letras e números em situações cotidianas, como fazer contas de uma pequena compra ou identificar as principais informações em um cartaz de vacinação. Há dez anos, a taxa de brasileiros nessa situação está estagnada, como mostram os dados do Indicador do Alfabetismo Funcional (Inaf) 2018". Disponível em: https://epocanegocios.globo.com/Brasil/noticia/2018/08/epoca-negocios-tres-em-cada-10-sao-analfabetos-funcionais-no-pais-aponta-estudo.html. Acesso em: 09 ago. 2019.

[140] "A investigação social nota que a impessoalidade que impera em relações comerciais (e principalmente nas realizadas *on-line*) é um fator que induz a uma falsa segurança na revelação de informações de caráter pessoal e, consequentemente, no consentimento para o seu tratamento" (DONEDA, 2006, p. 374).

[141] "(...) Não se pode olvidar que a construção do processo de consentir implica, à guisa de exemplificação, o emprego de linguagem não diretiva e, no momento atual em que se sobressai o ambiente digital, aponta especialmente para a garantia da transparência no que tange à coleta, à finalidade, ao armazenamento, ao tratamento e à transmissão dos dados" (SARLET; CALDEIRA, 2019, p. 14).

respectivos agentes de tratamento, observados os segredos comercial e industrial" (BRASIL, 2018, sem paginação). Com efeito, Frazão (2018a, sem paginação) pondera que

> o direito à informação está intrinsecamente relacionado ao princípio da transparência e prestação de contas e somente não é absoluto em razão da ressalva mencionada no inciso II, em relação aos segredos comercial e industrial. Tal questão tem especial relevância para as discussões sobre a utilização de algoritmos e inteligência artificial para o tratamento de dados, o que será abordado posteriormente com maior cuidado. O que precisa ser esclarecido, por ora, é que, com exceção daquilo que possa ser considerado como segredo comercial e industrial, todas as demais informações sobre o tratamento de dados devem ser prestadas ao titular, sem o que não restará observado o requisito do consentimento informado.

Um outro ponto que deve ser assinalado na LGPD é que em seu regime comum o consentimento deve ser inequívoco, ao passo que em se tratando de dados sensíveis deve ser específico e destacado (BRASIL, 2018a). Algumas imprecisões são apontadas com relação a essa exigência legal. É relevante verificarmos o modelo europeu. De acordo com o item 1, do art. 4, do GDPR, "o consentimento consiste em 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" (UNIÃO EUROPEIA, 2016, p. 34). No regime jurídico dos dados sensíveis, o GDPR prescreve na alínea "a", do item 2, do art. 9, a exigência de que o consentimento seja explícito e para uma ou mais finalidades específicas.[142]

Em termos literais, é possível identificar diferentes exigências, na medida em que a LGPD qualificou o consentimento como específico para o tratamento de dados sensíveis, ao passo que o GDPR qualificou o consentimento como expresso e, mais adiante, explícito. Do ponto de vista da técnica legislativa seria redundante exigir que o consentimento seja específico, na medida em que o princípio da finalidade demanda que o tratamento de dados atenda a propósitos específicos e explícitos, a demandar um direcionamento do próprio consentimento

[142] É relevante citar o Considerando 32 a respeito do consentimento no GDPR: "O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido" (UNIÃO EUROPEIA, 2016, p. 6).

que não pode ser, portanto, genérico (BIONI, 2019).[143] De fato, a ideia de um consentimento genérico é incompatível com a própria compreensão dos dados pessoais como representação da personalidade (DONEDA, 2006). A própria declaração de vontade, por si, deve ser dirigida a finalidades determinadas (BIONI, 2019).[144]

Apesar da diferença semântica entre a qualificação do consentimento como específico ou expresso e deste último representar melhor o nível de participação pretendido da pessoa com relação ao fluxo dos seus dados, a consequência normativa deve ser a mesma, na medida em que o propósito da qualificação é reservar uma autorização singular por parte da pessoa à qual os dados se referem (BIONI, 2019). Em realidade, esse consentimento especial deve ser compreendido como um vetor para que haja uma maior assertividade do titular com relação aos movimentos específicos dos seus dados (BIONI, 2019).

Uma outra questão é a qualificação do consentimento como inequívoco no regime comum dos dados pessoais na LGPD. Segundo Bioni (2019, p. 199), por inequívoco entende-se que o consentimento não pode ser ambíguo, mas sim evidente e se dar uma forma clara, ou seja, deve-se verificar um comportamento concludente por parte da pessoa à qual os dados se referem, compreendido como uma "ação afirmativa que não deixe dúvidas sobre a intenção do cidadão" (BIONI, 2019, p. 199).[145]

Para os dados sensíveis, todavia, além de inequívoco o consentimento deve ser destacado, como se depreende do art. 11, inciso I, da LGPD (BRASIL, 2018a). Com base nesta exigência legal, é relevante evidenciar que o processo de tomada da decisão deve ir muito além da previsão de cláusulas contratuais destacadas, banalizadas como forma de obter o consentimento trivial,[146] mas o imperativo é de que todo o processo seja específico e pontual, abrangente da informação até o aceite proferido pelo titular dos dados (BIONI, 2019). É fundamental, portanto, que a pessoa tenha plena ciência de que está consentindo especificamente a respeito do tratamento de dados de natureza sensível, de forma que a

---

[143] O Projeto de Lei n 5.276 estabelecia a exigência do consentimento expresso para o tratamento de dados sensíveis (BRASIL, 2016). Além disso, no Marco Civil da Internet o consentimento também é qualificado como expresso (BRASIL, 2014).

[144] Tepedino e Teffé (2019, p. 298) sustentam que o consentimento deve ser interpretado de forma restritiva, "não podendo o agente estender a autorização concedida para o tratamento dos dados para outros meios além daqueles pactuados, para momento posterior, para fim diverso ou, ainda, para a pessoa distinta daquela que recebeu a autorização".

[145] "(...) o grau e a qualidade da interação do usuário serão determinantes para qualificar o consentimento como sendo inequívoco. Será necessário, sobretudo, chegar a maneira pela qual o *design* de um ambiente (*on-line* e *off-line*) deve incutir no cidadão um controle visceral sobre seus dados, em vez de manipular as suas escolhas. Algo que está intrinsecamente ligado ao princípio da boa-fé" (BIONI, 2019, p. 200).

[146] A propósito, com relação aos usuais termos de uso e políticas de privacidade, Schulman (2016, p. 339) acentua que "considerá-lo apenas sob a ótica patrimonial não dará conta de sua complexidade, seja por seu caráter dinâmico, seja pela permissividade que conduziria no tocante à cessão de dados pessoais".

qualificação do consentimento como destacado contribui para uma maior carga participativa da pessoa no contexto da manifestação da vontade.

No que toca a exigência da finalidade específica, nos termos do inciso I, do art. 11, da LGPD, é importante novamente remeter ao princípio da finalidade. A exigência de que o tratamento de dados se dê para propósitos específicos já é estabelecida na principiologia da LGPD, a partir do princípio da finalidade e aplicável ao tratamento de qualquer dado pessoal, seja ele sensível ou não.[147] A própria noção do consentimento para atos existenciais é associada a uma finalidade específica, relacionando-o diretamente aos vínculos e relacionamentos correspondentes (SCHULMAN, 2016). Entretanto, é possível compreender essa previsão específica para os dados sensíveis como uma ênfase a uma especificidade no seu tratamento, sobretudo diante da sua potencialidade lesiva.

É importante remetermos a um aspecto do regime geral do consentimento na LGPD, mas que ganha particular atenção em se tratando dos dados sensíveis. Como aponta Schulman (2016), o consentimento pode perder a sua razão de ser com o passar do tempo ou se tornar extremamente nocivo. Portanto, como ato jurídico unilateral, o consentimento para o tratamento de dados pessoais é revogável de forma incondicional, o que se coaduna com a caracterização dos dados pessoais como representação da personalidade, que são, em última análise, indisponíveis (DONEDA, 2006). Nesta direção, a LGPD estabelece a revogabilidade facilitada a qualquer tempo do consentimento dado pelo titular, de acordo com o art. 8, §5º (BRASIL, 2018a).[148]

5.2 Hipóteses autorizativas restritas

O tratamento dos dados de natureza sensível não encontra autorização legal exclusivamente através da manifestação da vontade da pessoa à qual os dados se referem. Ao considerarmos a importância da informação no tecido social é possível identificar que a sua utilização, conforme certas balizas e sobretudo diante do princípio da não discriminação, pode ser útil aos indivíduos e à própria coletividade. Para além do consentimento, portanto, a LGPD estabelece um rol de hipóteses autorizativas para o tratamento dos dados sensíveis.

---

[147] Nesta linha, verifica-se a obrigatoriedade de um novo consentimento em razão da necessidade de alteração do emprego dos dados.

[148] "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" (BRASIL, 2018a, sem paginação).

A princípio, trata-se de uma ponderação entre o interesse exclusivo do titular dos dados, de interesses de natureza pública e de outros interesses voltados a promover a proteção da própria pessoa, independente da manifestação da sua vontade. Mulholland (2018, p. 168) endereça críticas a esse posicionamento legislativo porque, segundo a autora, "a proteção do conteúdo dos dados pessoais sensíveis é fundamental para o pleno exercício de Direitos Fundamentais, tais como os da igualdade, liberdade e privacidade".

No entanto, não parece contraditório proteger dados sensíveis e, por outro lado, autorizar a sua utilização em situações legítimas diante do valor social da informação. A própria noção contemporânea da privacidade encontra o seu fundamento na inserção da pessoa na sociedade, não mais em uma prerrogativa de isolamento. Em que pese o estabelecimento de um *standard* protetivo mais rigoroso para os dados sensíveis, a ampla vedação ao seu tratamento se coloca na contramão das diversas utilidades às quais eles podem servir. Restringir desproporcionalmente o tratamento de dados sensíveis, nesta direção, acabaria por inviabilizar várias atividades socialmente relevantes, a exemplo de instituições políticas, religiosas, de saúde, entre outras, que não prescindem do tratamento de dados de natureza sensível.[149]

Todavia, as razões de coleta, especialmente em face de dados sensíveis, devem ser objetivas e limitadas (MORAES, 2008). Com o propósito de objetividade e limitação, os seus contornos são definidos pela finalidade legítima do tratamento dos dados, que se condiciona à comunicação preventiva ao interessado sobre a utilização dos seus dados pessoais, além de que, em determinadas situações envolvendo dados sensíveis, a única finalidade admissível será o interesse da pessoa (RODOTÀ, 2008).[150] Sobretudo, as hipóteses autorizativas não são um "cheque em branco", de forma que a sua utilização como base legal não prescindirá de uma análise concreta e contextual dos termos do tratamento dos dados, especialmente diante da principiologia consagrada na LGPD. As hipóteses que autorizam o tratamento de dados sensíveis no art. 11, inciso II, são:

> (...) a) cumprimento de obrigação legal ou regulatória pelo controlador;

[149] No princípio da evolução normativa em sede de proteção de dados pessoais, é relevante mencionar o exemplo da Resolução (73) 22 do Conselho da Europa (*Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the privacy sector*) que vedava a coleta e, se coletados, a disseminação de dados potencialmente discriminatórios. O primeiro princípio da resolução determinava: "In general, information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated" (CONSELHO DA EUROPA, 1973, p. 74). A orientação da Resolução (73) 22 influenciou normativas nacionais subsequentes (DONEDA, 2006).

[150] A título de exemplo, é possível identificar uma gradação dentro da categoria dos dados sensíveis, como os dados relativos à vida sexual da pessoa, os quais poderiam ter o seu âmbito de utilização sobremodo restrito em face das hipóteses autorizativas estabelecidas na LGPD.

> 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, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> 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 (Redação dada pela Lei nº 13.853, de 2019)
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL, 2018a, sem paginação).

A LGPD estabelece sete hipóteses que autorizam o tratamento de dados sensíveis quando estes forem indispensáveis para as finalidades elencadas (BRASIL, 2018a). De início, a natureza dos dados sensíveis enseja hipóteses mais restritas que as hipóteses que autorizam o tratamento de dados pessoais não sensíveis. No regime jurídico comum dos dados pessoais, além do consentimento, são identificadas as seguintes bases legais para o tratamento na LGPD:

> (...) 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;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)
> 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 (BRASIL, 2018a, sem paginação).

É possível verificar, inicialmente, que a execução de contrato ou procedimentos preliminares relacionados a contrato do qual seja parte o titular, ainda que a pedido do titular dos dados (art. 7º, V), o interesse legítimo do controlador ou de terceiro (art. 7º, IX) e a proteção ao crédito (art. 7º, X) não autorizam o tratamento de dados sensíveis, mas apenas de dados pessoais não sensíveis (BRASIL, 2018a). Como observa Konder (2019), os interesses

patrimoniais associados a estas hipóteses autorizativas dispostas no artigo 7º não justificam os riscos inerentes ao tratamento de dados sensíveis. A rigor, o legislador promoveu uma significativa restrição ao tratamento dos dados sensíveis se comparado ao regime comum dos dados pessoais. Por outro lado, o cumprimento de obrigação legal ou regulatória pelo controlador se apresenta como base legal para o tratamento de dados pessoais, sejam eles sensíveis ou não, conforme os artigos 11, II, "a" e 7º, II, respectivamente (BRASIL, 2018a).

Com relação à administração pública, é autorizado o tratamento compartilhado de dados sensíveis necessários à execução de políticas públicas previstas em leis ou regulamentos (art. 11, II, "b") (BRASIL, 2018a). No regime comum dos dados pessoais, o rol dos instrumentos aptos legitimar o tratamento de dados necessários à execução de políticas públicas é alargado para incluir, além de leis e regulamentos, os contratos, convênios ou instrumentos congêneres (art. 7º, III) (BRASIL, 2018a). Em outros termos, instrumentos normativos mais restritos autorizariam o tratamento de dados sensíveis para a execução de políticas públicas.

Nas duas hipóteses autorizativas anteriormente citadas para o tratamento de dados sensíveis, quais sejam, cumprimento de obrigação legal ou regulatória pelo controlador e para a execução de políticas públicas, a LGPD prescreve a obrigatoriedade de publicização da dispensa do consentimento para o tratamento dos dados quando da aplicação dos dispositivos pelos órgãos e pelas entidades públicas, conforme o §2º, do art. 11 (BRASIL, 2018a). O dispositivo faz remissão à disciplina do tratamento de dados pessoais pelo poder público, que determina o fornecimento de "informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos" (BRASIL, 2018a, sem paginação). [151] Com fundamento no princípio da transparência,[152] de outra parte, é possível inferir a obrigatoriedade da publicidade por parte dos agentes privados quando do tratamento

[151] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: (...) § 2º Nos casos de aplicação do disposto nas alíneas 'a' e 'b do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei. (...) 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 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, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; (...)" (BRASIL, 2018a, sem paginação).

[152] A LGPD define o princípio da transparência como "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" (BRASIL, 2018a).

de dados sensíveis com base na hipótese autorizativa do cumprimento de obrigação legal ou regulatória.

A realização de estudos por órgão de pesquisa autoriza tanto o tratamento de dados pessoais não sensíveis como dos sensíveis. Nas duas disposições, respectivamente no art. 7º, IV e no art. 11, II, alínea "c", da LGPD, é previsto o imperativo de anonimização dos dados, sempre que possível, o que, uma vez realizado, acabaria por afastar os dados da abrangência da LGPD, segundo o *caput* do art. 12 (BRASIL, 2018ª).[153] É razoável depreender uma maior necessidade de anonimização dos dados sensíveis que os demais dados pessoais nesta hipótese de tratamento. No entanto, caso esses dados anonimizados sejam utilizados para a formação de perfil comportamental de uma pessoa identificada, passarão a ser considerados como dados pessoais, de acordo com o art. 12, §2º (BRASIL, 2018a).[154]

A propósito, Rodotà (2008) aponta os riscos subjacentes ao tratamento dos dados anônimos, que podem ser manipulados de forma lesiva aos direitos dos indivíduos, como é o caso de uma coletânea de dados anônimos relativos a uma minoria racial ou linguística, ou quando utilizados para a tomada de uma decisão política. Não obstante, Machado e Doneda (2018) apontam o debate no sentido de que sempre existirá o risco de identificação ou reidentificação de pessoas através do tratamento de dados anonimizados no contexto atual do enorme volume de dados disponibilizados e dos avanços na capacidade de processamento e análise de algoritmos, de *data mining* e de sistemas de *machine learning*.[155]

O exercício regular de direitos em processo judicial, administrativo ou arbitral autoriza o tratamento de dados pessoais sensíveis e não sensíveis, de acordo com os artigos 11, II, "d" e 7º, VI, respectivamente (BRASIL, 2018a). De uma forma contraditória, o regime dos dados sensíveis neste aspecto é mais amplo, porque admite a sua aplicação a contratos, inclusive, o

---

[153] "Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta 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" (BRASIL, 2018a, sem paginação). No relatório do Deputado Orlando Silva na Comissão Especial destinada a proferir parecer sobre o Projeto de Lei 4.060 de 2012 que, posteriormente, após diversas alterações, foi aprovado pela Câmara dos Deputados e deu origem à LGPD, foi destacado que: "É fato que o desenvolvimento do poder computacional é crescente e contínuo. Dessa forma a anonimização de dados de hoje pode se tornar obsoleta amanhã. Ademais, apesar de um responsável utilizar técnicas apropriadas de anonimização e de segurança, a adição de outros dados, oriundos de outro provedor, ou novas tecnologias poderão permitir a identificação de titulares. Por isso, é razoável admitir que a anonimização absoluta e a prova de falhas é impossível de ser atingida e garantida a qualquer tempo". Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=Tramitacao-PL+4060/2012. Acesso em: 10 out. 2018.

[154] "§ 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, 2018a, sem paginação).

[155] Nesse sentido, o § 1º, do art. 12 dispõe 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" (BRASIL, 2018a, sem paginação).

que não é previsto para o regime comum de dados pessoais. A rigor, se para dados pessoais em geral é previsto um regime mais restrito neste ponto, é razoável que igualmente se aplique para os dados sensíveis que são, em realidade, dados pessoais associados a um *plus* protetivo.[156]

O art. 7, incisos VII e VIII e o art. 11, inciso II, alíneas "e" e "f" buscam endereçar o tratamento dos dados pessoais para a proteção da vida e da saúde, com previsões idênticas. Em outros termos, diante do propósito de tutelar a vida e a saúde da pessoa ou de terceiro, a LGPD autoriza o tratamento de qualquer tipo de dado pessoal, o que envolverá, em significativa parte, dados sensíveis relativos à saúde.[157] A área da saúde é um exemplo da crescente automatização e da aplicação da robótica no ambiente laboratorial e farmacêutico, lançando múltiplos desafios com relação aos dados pessoais, especialmente pela natureza sensível desses dados, pela posição nuclear do tema na vida da pessoa e pela condição de vulnerabilidade que a pessoa geralmente se encontra nessa esfera (SARLET; CALDEIRA, 2019). Segundo Sarlet e Caldeira (2019, p. 9), é possível identificar um processo de "transformação digital da saúde":

> Em se tratando de um sistema demasiadamente complexo que envolve diversos órgãos e pessoas, a e-Saúde oferece alguns riscos à confidencialidade inerente à relação médico-paciente e à segurança do tratamento e da livre circulação dos dados de saúde. Ou seja, trata-se de todas as informações sobre o estado físico ou mental dos cidadãos, incluindo as que se referem à prestação de serviços que revelem informações sobre as suas condições de saúde. A perda da confidencialidade pode ocorrer à medida que são utilizadas aplicações em dispositivos inteligentes, por meio das quais vão sendo recolhidas cada vez maiores quantidades de dados para o tratamento e para prestações de serviços inovadores, podendo, entretanto, ser sujeitas a diversas modalidades de tratamento posterior, tendo em vista fins econômicos a despeito do consentimento do paciente. Não obstante, assiste-se assim, por todo o mundo, a um processo de transformação digital da saúde a que designamos e-Saúde ou Cibermedicina e que conta já com bons exemplos em vários países: Alemanha (*Eletronic Health Card*), Brasil (verifica-se um aumento de aplicativos para celulares tendo em vista a saúde), Portugal (aplicativo Knok), Reino Unido (aplicativo Babylon), Suécia (*website* KRY) entre outros.[158]

---

[156] É oportuno questionar se a inserção do contrato nessa hipótese autorizativa se justifica pela não reprodução da hipótese constante do regime geral dos dados pessoais relativa à execução do contrato ou procedimentos preliminares no regime dos dados sensíveis.

[157] A partir da experiência portuguesa com relação aos dados sensíveis referentes à saúde, Sarlet e Caldeira (2019, p. 15) destacam que: "O legislador clarifica a titularidade dos dados de saúde, atribuindo às unidades do sistema de saúde a função de depositários da informação, a qual não pode ser utilizada para outros fins que não os da prestação de cuidados e da investigação em saúde e outros estabelecidos pela lei. Por esta razão, é indefensável que os dados de saúde dos pacientes registrados em instituições de saúde pública, sejam considerados 'documentos administrativos'. A natureza e a titularidade da informação não se alteram em função dos depositários da informação de saúde, sejam entidades públicas ou privadas".

[158] No Brasil temos o DATASUS, que é o departamento de informática do Sistema Único de Saúde (SUS) do Brasil. É um órgão da Secretaria de Gestão Estratégica e Participativa do Ministério da Saúde, com a responsabilidade de coletar, processar e disseminar informações sobre saúde, ou seja, responsável por uma ostensiva quantidade de dados sensíveis. O DATASUS provê aplicativos para dispositivos móveis como o "Meu digiSUS", definido como uma plataforma móvel e de serviços digitais oficial do Ministério da Saúde. Disponível em: http://datasus.saude.gov.br. Acesso em: 04 jul. 2019.

No âmbito dos dados sensíveis referentes à saúde, os desafios relativos à segurança dos dados são elevados a outro patamar, na medida em que a sua disposição às entidades de saúde materializa e incrementa as possibilidades de ciberataques, a repercutir em limitações de direitos e liberdades fundamentais dos cidadãos (SARLET; CALDEIRA, 2019).[159] Um agravante nesse cenário é o interesse do mercado nessas informações, que movimentam setores como o farmacêutico e o de seguros, a fazer emergir a grande relevância do princípio da finalidade para avaliar concretamente a utilização dos dados sensíveis com base na autorização da LGPD. Como advertem Sarlet e Caldeira (2019, p. 12-13):

> (...) Na medida em que se trata de área essencial da vida humana, a saúde passou a ser evidentemente muito afetada pelo emprego por vezes desordenado das inovações biotecnológicas, pela estruturação de um mercado extremamente rentável e selvagem, pela aplicação irresponsável da tecnologia da informação e da comunicação e pelos novos paradigmas voltados para a imortalização e para o enaltecimento da ideia de perfeição em um contexto de saúde preventiva.

Como anteriormente referido, a conjuntura brasileira é marcada por uma cultura incipiente de proteção de dados pessoais. Em 2016, o Governo Federal expôs no portal Dados Abertos os dados pessoais de mais de 30 mil dependentes químicos internados em comunidades terapêuticas, dentre eles 1,3 mil crianças e adolescentes (MACHADO; MAGENTA, 2019). A situação permaneceu até o presente ano de 2019, quando, por provocação da BBC News aos Ministérios da Justiça e da Cidadania, as informações referentes a todas as pessoas internadas com custeio do governo, entre maio de 2013 e abril de 2016, como nome, data de nascimento, CPF, profissão, tipo de droga que levou ao tratamento e custo de internação foram retirados do ar (MACHADO; MAGENTA, 2019). Não é difícil perceber a ampla potencialidade lesiva de episódios como o citado na área da saúde, a demandar ainda maior rigor em se tratando dos dados sensíveis, seja por parte do Estado, seja por parte dos agentes privados.

Apesar de não estar elencado no rol do art. 11, inciso II, da LGPD como hipótese autorizativa, o art. 13[160] estabelece uma hipótese que autoriza o tratamento de dados pessoais

---

[159] "Estes desafios ganham maior dimensão tendo como critério a inescusável circulação de dados pessoais, com origem e destino em países em desenvolvimento. Estes movimentos transfronteiriços colocam obstáculos à interoperabilidade da informação de saúde, na medida em que se utilizam de formatos incompatíveis, para além das diferentes terminologias utilizadas pelos profissionais de saúde, a saber: CID, openEHR, etc" (SARLET; CALDEIRA, 2019, p. 11).

[160] "Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e 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 anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais. § 2º O órgão de pesquisa será o responsável pela segurança da informação prevista

para a realização de estudos na área da saúde pública[161]. Embora não sejam mencionados expressamente os dados sensíveis na autorização, diante do propósito do estudo, parece razoável considerar a abrangência dos dados referentes à saúde, o que se alinha com o relatório do Deputado Orlando Silva, na Comissão Especial destinada a proferir parecer sobre o Projeto 4.060 de 2016, no sentido de destacar o potencial dos dados relativos à saúde para o desenvolvimento de novos produtos e serviços, com o consequente impacto nos direitos fundamentais da pessoa.[162] Como considera Konder (2019), o princípio da finalidade ganha relevo em face dessa autorização legal, restringindo a utilização dos dados estritamente à finalidade do estudo. Neste sentido:

> Em proteção à segurança dos dados, determina-se que o tratamento somente ocorra dentro do órgão, impõe-se o respeito a práticas de segurança previstas em regulamento específico e imputa-se ao órgão de pesquisa a responsabilidade pela segurança da informação, não permitida, em circunstancia alguma, a transferência dos dados a terceiro. Impõe-se, ainda, que o tratamento deve respeitar os padrões éticos relacionados a estudos e pesquisas, como aqueles impostos por Códigos de Ética, princípios de Bioética, diretrizes internacionais e procedimentos impostos pelo Comitê de Ética em Pesquisa (CEP) da instituição, ressalvando que o acesso a esses dados deve ser objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências (KONDER, 2019, p. 459-460).

---

no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro. § 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências. § 4º Para os efeitos deste artigo, a pseudonimização é o 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" (BRASIL, 2018a, sem paginação). No item 5, do art. 4º, do GDPR, a pseudonimização é definida como: "tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável" (UNIÃO EUROPEIA, 2016, p. 33). Como referem Machado e Doneda (2018, p. 112), "a pseudonimização opera de maneira que as informações não podem ser conectadas a um titular de dados específico sem que se recorra a informações suplementares, desde que estas sejam mantidas separadamente, empregadas medidas organizativas e de segurança".

[161] Para a compreensão da abrangência do termo saúde pública, que não é definido na LGPD, é possível recorrer à Lei 8.080 de 1990, que dispõe nos seguintes termos: "Art. 4º O conjunto de ações e serviços de saúde, prestados por órgãos e instituições públicas federais, estaduais e municipais, da Administração direta e indireta e das fundações mantidas pelo Poder Público, constitui o Sistema Único de Saúde (SUS). § 1º Estão incluídas no disposto neste artigo as instituições públicas federais, estaduais e municipais de controle de qualidade, pesquisa e produção de insumos, medicamentos, inclusive de sangue e hemoderivados, e de equipamentos para saúde. § 2º A iniciativa privada poderá participar do Sistema Único de Saúde (SUS), em caráter complementar" (BRASIL, 1990, sem paginação). A partir dessa definição do sistema de saúde pública no ordenamento jurídico, verifica-se uma abertura para a iniciativa privada, o que demandaria uma cautela com relação à aplicação do art. 13, da LGPD.

[162] Entre os fundamentos dessa previsão, de acordo com o relatório do Deputado Orlando Silva, foi destacado que: "Tendo em vista o enorme potencial dos dados referentes à saúde para o desenvolvimento de novos produtos e serviços, tais como novos tratamentos e drogas para doenças crônicas e degenerativas, e, ao mesmo tempo, o alto impacto que o seu tratamento pode gerar na vida e nos direitos fundamentais das pessoas, optamos por incluir um regramento balizador para o uso destes dados". Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=Tramitacao-PL+4060/2012. Acesso em: 10 out. 2018.

Em face da autorização do art. 13, a LGPD acrescenta que sempre que possível os dados pessoais deverão ser submetidos aos processos de anonimização ou pseudonimização (BRASIL, 2018a).[163] Todavia, em se tratando da divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, é absolutamente vedada a divulgação de dados pessoais, de acordo com o § 1º, do art. 13 (BRASIL, 2018a). Em outros termos, prevalecerá o propósito do estudo na área da saúde pública, sem associação de qualquer ordem pessoal ao indivíduo.

A última hipótese autorizativa para o tratamento de dados sensíveis elencada no art. 11, inciso II, da LGPD é para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (BRASIL, 2018a), a exemplo da efetivação de transações bancárias, acesso a locais restritos, entre outros. Apesar de não existir expressamente uma hipótese correspondente no regime geral dos dados pessoais, Frazão (2018c) sustenta que esta hipótese estaria compreendida na previsão do interesse legítimo disposta no art. 7º, inciso IX, notadamente mais ampla que a previsão específica para os dados sensíveis, que, a rigor, se vincula diretamente ao interesse do próprio titular dos dados. Não obstante, a aplicação dessa hipótese autorizativa ficará condicionada ao resguardo dos direitos consagrados no art. 9, da LGPD, bem como não poderá ser utilizada em detrimento de direitos e liberdades fundamentais da pessoa à qual os dados se referem (BRASIL, 2018a).

É oportuno destacar alguns aspectos das hipóteses autorizativas para o tratamento de dados sensíveis no GDPR. De plano, verifica-se um paralelismo relativo nas previsões com a LGPD, como o cumprimento de obrigação legal pelo controlador, o interesse público, a tutela da saúde, a defesa de direitos na esfera jurisdicional, inclusive na atuação dos tribunais no que concerne à sua função, embora com contornos normativos próprios (UNIÃO EUROPEIA, 2016). O GDPR autoriza o tratamento de dados sensíveis dos membros ou antigos membros "por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais", dependendo de garantias adequadas e de outras exigências pertinentes (UNIÃO EUROPEIA, 2016, p. 38),[164] o que não encontra correspondente na LGPD.

---

[163] Como pondera Frazão (2018d), "o art. 13 da LGPD é específico para os casos de pesquisas sobre saúde pública, finalidade que, diante da sua grande relevância, faz com que se possa optar por técnica distinta da anonomização. Para as demais pesquisas, entretanto, prevalece a obrigação de que a anonimização deve ser utilizada, sempre que possível (arts. 7º, IV; 11, II, "c" e 16, II)".

[164] "Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus

O GDPR igualmente autoriza o tratamento de dados sensíveis manifestamente tornados públicos pelo seu titular, conforme art. 9, item 2, alínea "e" (UNIÃO EUROPEIA, 2016). Ao compararmos essa previsão com a LGPD, é possível identificar no §4º, do art. 7º a dispensa do consentimento para o tratamento desses dados tornados públicos pelo titular no regime jurídico comum dos dados pessoais, não existindo previsão análoga para os dados sensíveis.[165] É plausível inferir que a LGPD não dispensa o consentimento para o tratamento de dados sensíveis tornados públicos pelo titular, diferentemente do GDPR, a indicar um regime mais protetivo neste aspecto. Em realidade, o fato de o dado pessoal ter sido tornado público não dispensa a sua potencialidade discriminatória, nem mesmo corresponde a um aval para que esses dados sejam submetidos, por exemplo, a sistemas automatizados que acabariam por repercutir na vida da pessoa.[166]

Por outro lado, o art. 9, item 2, alínea "j" autoriza o tratamento de dados sensíveis para "fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos" (UNIÃO EUROPEIA, 2016, p. 39).[167] Na oportunidade do tratamento de dados com essas finalidades, deverão ser asseguradas garantias adequadas em vista dos direitos e liberdades do titular, como a pseudonimização, de acordo com o art. 89, itens 1 a 4, do GDPR (UNIÃO EUROPEIA, 2016).

A LGPD, por sua vez, apresenta uma abordagem normativa diferente e exclui da sua abrangência o tratamento de dados pessoais para fins jornalísticos e artísticos, conforme o art. 4º, II, "a" (BRASIL, 2018a), o que poderia se associar a finalidades históricas e de arquivo de interesse público. Com relação ao tratamento de dados para fins acadêmicos, o que é associável aos fins científicos e até estatísticos, a LGPD igualmente exclui da sua abrangência no art. 4º, II, "b", embora faça expressa menção à aplicação das hipóteses autorizativas dos artigos 7º e 11 da LGPD. Esta ressalva, que havia sido suprimida pela Medida Provisória 869 de 2018 (BRASIL, 2018b), não foi posteriormente confirmada, retomando a redação original (BRASIL,

objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares" (UNIÃO EUROPEIA, 2016, p. 38).

[165] O § 3º, do art. 7º, condiciona o tratamento dos dados pessoais de acesso público, nos seguintes termos: "O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização" (BRASIL, 2018a, sem paginação).

[166] Como anteriormente ressaltado, os dados sensíveis dispõem de uma normativa específica no regime das decisões automatizadas no GDPR, conforme disposto no item 4, do art. 22 (UNIÃO EUROPEIA, 2016), mas não há uma previsão análoga na LGPD.

[167] "Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados" (UNIÃO EUROPEIA, 2016, p. 39).

2018a). Portanto, o tratamento de dados pessoais, sejam eles sensíveis ou não, para fins acadêmicos deverá ser baseado nas respectivas hipóteses autorizativas dispostas na LGPD.

5.3 Extensão do regime jurídico dos dados sensíveis para o tratamento sensível de dados pessoais

O § 1º do art. 11, da LGPD, estabelece que será aplicável o regime jurídico dos dados sensíveis "a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica" (BRASIL, 2018a, sem paginação). Como denomina Mendes (2014), consiste em um "tratamento sensível de dados", na hipótese em que dados aparentemente inofensivos são transformados em informações com potencialidade discriminatória aptas a causar dano à pessoa.

Frazão (2018c) sustenta que a linha distintiva entre dados pessoais sensíveis e dados não sensíveis deve ser dinâmica, e não estática, o que justificaria a previsão da LGPD no sentido de que devem ser tutelados como sensíveis os dados pessoais que, se tratados, autorizam o conhecimento de informações sensíveis sobre a pessoa.[168] A extensão do regime dos dados sensíveis, nestes termos, configura-se como um mecanismo de tutela de forma a ampliar a proteção inicialmente concebida para os dados sensíveis a dados pessoais suscetíveis de revelar dados de natureza sensível, o que ganha relevância diante dos exponenciais avanços tecnológicos que redefinem o processamento automatizado de dados.

A princípio, Frazão (2018d) aponta a imprescindibilidade de analisar a capacidade de cada dado revelar aspectos sensíveis da pessoa. Bussche e Voigt (2017 apud FRAZÃO, 2018c) mencionam os dados pessoais como prenome, sobrenome, local de nascimento e língua nativa como potenciais reveladores da própria origem racial ou étnica da pessoa, situação que poderia se amoldar à prescrição do art. 11, § 1º, da LGPD (BRASIL, 2018a).

Em um caso mencionado por Doneda e Monteiro (2015), ocorrido na Universidade Federal de Santa Maria, com base na Lei de Acesso à Informação (LAI) – n.º 12.527 de 2011[169]

---

[168] A partir de uma interpretação dinâmica dos dados sensíveis, Frazão (2018d, sem paginação) sustenta que serão classificados enquanto tal "sempre que os perfis retratarem aspectos da personalidade ou do comportamento do usuário", o incluiria os dados anônimos utilizados para a construção de tais perfis, como mencionado anteriormente. Entretanto, dados pessoais referentes a perfis não são expressamente considerados como sensíveis pela LGPD.

[169] No que concerne aos propósitos da Lei de Acesso à Informação, Doneda e Monteiro (2015, sem paginação) destacam que: "A proteção de dados pessoais, antes de antagonizar com o princípio da transparência, serve para legitimar o fornecimento da informação de interesse público à sociedade, ao mesmo tempo em que considera o interesse individual na reserva sobre o fornecimento de determinada informação pessoal, abalizada pelo direito fundamental à proteção de dados pessoais. (...) A LAI especifica, em seu art. 31, que informações pessoais 'relativas à intimidade, vida privada, honra e imagem' não sejam fornecidas a terceiros. A referência normativa à

foi formulado um memorando por um pró-reitor da Universidade com pedido de informações pessoais sobre discentes ou docentes israelenses então presentes na instituição. O pedido foi precedido de considerandos marcados por um juízo negativo das ações praticadas pelo Estado de Israel (DONEDA; MONTEIRO, 2015). A nacionalidade não é comumente considerada como um dado sensível, embora seja possível vislumbrar o "tratamento sensível que pode ser dado a tal informação, capaz de estigmatizar, classificar, pré-julgar e mesmo comprometer a segurança dos cidadãos afetados" (DONEDA; MONTEIRO, 2015, sem paginação).[170]

Em uma exegese do art. 11, § 1º, da LGPD é possível inferir que o regime jurídico dos dados sensíveis será aplicável quando forem revelados dados sensíveis e existir potencialidade de dano (BRASIL, 2018a). No entanto, na exemplaridade do caso relatado por Doneda e Monteiro (2015), a potencialidade discriminatória era patente, mas não estávamos diante de um dado propriamente sensível, além de que a origem racial ou étnica não pode ser depreendida *per se* da nacionalidade. Para além de uma interpretação legalista, emerge a cláusula geral de tutela e promoção da pessoa humana para estender a abrangência da previsão art. 11, § 1º, da LGPD, o que poderia ser conciliado com a LAI. Em realidade, na medida em que o fundamento da categoria dos dados sensíveis é o princípio da igualdade substancial, é contraditório negar a sua concretização em situações que evidentemente representam uma tentativa da sua mitigação.

Para Konder (2019), a previsão do art. 11, § 1º, da LGPD representa um argumento favorável à necessidade de se conceber o rol dos dados sensíveis como exemplificativo, na medida em que o próprio legislador reconhece a ampliação das regras pertinentes aos dados sensíveis aos tratamentos de dados pessoais que apesar de não serem intrinsecamente sensíveis, podem vir a revelar dados sensíveis. A título de exemplo, dados referentes à localização geográfica, às preferências e ao histórico na rede, citados por Konder (2019) como aparentemente ou isoladamente inofensivos, podem vir a ser tratados em conjunto com outros dados e revelar dados sensíveis.[171] Ao tratar sobre a possibilidade de combinação dos "vestígios

qual o referido artigo alude é a cláusula geral de proteção da personalidade, que encontra seu fulcro na proteção da personalidade presente na Constituição Federal, garantindo a proteção da personalidade em todas as suas emanações, referenciada pela dignidade da pessoa humana (Art. 1º, III) e pelo repúdio a qualquer forma de discriminação (Art. 3º, IV). Desta forma, a cláusula de proteção da privacidade e dados pessoais presente no artigo 31 da LAI reflete diretamente o arcabouço normativo da cláusula geral da proteção da personalidade que, enquanto direito fundamental, deve forçosamente integrar a interpretação a ser dada em relação ao alcance das restrições ao acesso a dados pessoais".

[170] No âmbito criminal, a discriminação com fundamento na procedência nacional é tipificada como crime no art. 1º, da Lei 7.716/1989 (BRASIL, 1989).

[171] Para ilustrar, é possível conceber o histórico de compras de medicamentos de uma pessoa em uma rede farmacêutica como um amplo campo de inferências a respeito da sua condição de saúde através de processamentos automatizados, a demandar uma particular tutela. Neste exemplo, é fácil visualizar como dados não sensíveis poderiam ser tratados para revelar dados sensíveis e causar dano à pessoa.

digitais" da pessoa na rede para a definição de perfis, lógica que também poderia ser referida para identificação de dados sensíveis, o Considerando 30 do GDPR estabelece que:

> As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão (cookie) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares (UNIÃO EUROPEIA, 2016, p. 6).

Em pesquisa realizada por Kosinski, Stillwell e Graepel (2013) foi demonstrado que a partir de uma única variável consistente nos *likes* da pessoa no *Facebook*, registros digitais de fácil acesso, foi possível inferir uma série de dados pessoais sensíveis, como orientação sexual, origem étnica, orientações políticas e religiosas, além de traços de personalidade, inteligência, felicidade, uso de substâncias entorpecentes, separação dos pais, entre outros. A título de exemplo, a origem racial foi aferida com 95% de precisão, considerados os parâmetros de caucasiano e afro-americano, além de que através da diferenciação dos homens entre homossexuais e heterossexuais o modelo obteve uma acurácia de 88% (KOSINSKI; STILLWELL; GRAEPEL, 2013).[172]

O desenvolvimento da inteligência artificial abre cada vez mais campo para a realização de inferências de dados sensíveis a partir de dados não sensíveis, com combinações inescrutáveis de interações no mundo real e no mundo virtual (FRAZÃO, 2018d). Entretanto, vale ressaltar que o desenvolvimento das formas de processamento de dados levanta importantes questões a respeito da larga abrangência que o art. 11, § 1º, da LGPD poderia tomar neste cenário, atraindo, por conseguinte, uma ostensiva gama de dados para a esfera do regime jurídico dos dados sensíveis.

5.4 Possibilidade de vedação ou regulamentação da comunicação e do uso compartilhado de dados sensíveis para fins econômicos pela Autoridade Nacional de Proteção de Dados

[172] "The analysis presented is based on a dataset of over 58,000 volunteers who provided their Facebook Likes, detailed demographic profiles, and the results of several psychometric tests. The proposed model uses dimensionality reduction for preprocessing the Likes data, which are then entered into logistic/linear regression to predict individual psychodemographic profiles from Likes" (KOSINSKI; STILLWELL; GRAEPEL, 2013, p. 5802).

O tema da comunicação e do uso compartilhado de dados sensíveis com fins econômicos é diretamente endereçado pelo § 3º, do art. 11, da LGPD (BRASIL, 2018a). A princípio, é de se destacar que a comunicação de dados pessoais se insere no conceito de tratamento de dados do art. 5º, inciso X, da LGPD, bem como no conceito de uso compartilhado disposto no inciso XVI do mesmo dispositivo, que dispõe:

> Uso compartilhado de dados: comunicação, difusão, transferência internacional, 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 privados (BRASIL, 2018a, sem paginação).[173]

Como estabelece o inciso XVI, do art. 5º, o uso compartilhado de dados demanda autorização específica, independente do tratamento ser procedido por ente público ou privado (BRASIL, 2018a). Em outros termos, o uso compartilhado de dados pessoais deverá ser objeto de autorização específica porque o grau de exposição e de risco da pessoa com relação aos seus dados pessoais é elevado a outro patamar quando outros agentes se inserem na cadeia de tratamento dos dados. Todavia, deve ser destacada a disposição do § 5º, do art. 7º, da LGPD, previsto no regime geral das hipóteses autorizativas sobre proteção de dados pessoais:

> O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei (BRASIL, 2018a, sem paginação).

Através da leitura do dispositivo é possível depreender que a autorização específica referida no conceito do uso compartilhado de dados pessoais não está restrita ao consentimento específico, mas, ao que parece, também poderá se dar por uma autorização legal com base nas próprias hipóteses autorizativas. Ocorre que ao estabelecer a ressalva sobre as hipóteses autorizativas, no sentido de dispensar o consentimento específico, a redação do dispositivo faz referência àquelas previstas em lei, não restringindo às hipóteses do art. 7º (BRASIL, 2018a). É de se questionar, portanto, se e em quais termos essa potencial ampliação de agentes de tratamento dos dados pessoais, a partir do uso compartilhado de dados, é extensível ao regime jurídico dos dados sensíveis, sobretudo diante da sua potencialidade lesiva.

---

[173] A partir do conceito legal infere-se que o uso compartilhado é abrangente das atividades de comunicação de dados.

De outra parte, se direcionarmos para as disposições da LGPD pertinentes ao Poder Público, os incisos do § 1º, do art. 26,[174] abrem uma série de ressalvas para autorizar o uso compartilhado de dados pessoais constantes das bases de dados das quais a administração pública tenha acesso com entidades privadas (BRASIL, 2018a). Apesar do dispositivo destacar o norte da finalidade específica[175] quando do uso compartilhado, é inegável a grande margem que a previsão abre para a circulação de dados pessoais entre vários agentes privados, ampliando a possibilidade de danos. Não obstante, o art. 27, da LGPD,[176] dispensa a informação à ANPD do uso compartilhado de dados pessoais quando o fundamento for as hipóteses autorizativas previstas em lei ou as exceções dispostas no § 1º do art. 26 (BRASIL, 2018a), o que acaba por comprometer o controle da utilização dos dados pessoais. Com esse cenário, o § 3º, do art. 11, da LGPD, estabelece que:

> A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências (BRASIL, 2018a, sem paginação) (BRASIL, 2018a, sem paginação).[177]

De plano, a possibilidade de vedação ou regulamentação da comunicação ou do uso compartilhado de dados sensíveis disciplinada no § 3º direciona-se às atividades voltadas à

---

[174] "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. 6º desta Lei. § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ; III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei. IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019) V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)" (BRASIL, 2018a, sem paginação).

[175] O art. 23, da LGPD, que inaugura o regime jurídico próprio do Poder Público dispõe que: "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 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, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos (...)" (BRASIL, 2018a, sem paginação).

[176] "Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto: I - nas hipóteses de dispensa de consentimento previstas nesta Lei; II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou III - nas exceções constantes do § 1º do art. 26 desta Lei" (BRASIL, 2018a, sem paginação).

[177] O art. 30, da LGPD dispõe: "A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais" (BRASIL, 2018a, sem paginação).

obtenção de vantagem econômica, o que acabaria por afastar as atividades do Poder Público fundamentadas no interesse público *per se*. No entanto, a disposição do § 3º ganha significativa relevância diante da amplitude que o uso compartilhado de dados pessoais pode tomar, especialmente diante dos dados sensíveis, que ainda não contam com uma interpretação sedimentada neste tocante. Em última análise, a ANPD pode exercer um papel fundamental no sentido de proteger os dados sensíveis em face daquelas atividades direcionadas a interesses patrimoniais.[178]

Por outro lado, em face da natureza dos dados sensíveis, Frazão (2018d) sustenta que a única leitura plausível que pode ser feita do § 3º, do art. 11, é a de que a ANPD está autorizada a vedar ou restringir o uso compartilhado de dados sensíveis para fins econômicos, ainda que consentido pelo titular, porque, segundo a autora, seria vedado o compartilhamento de dados sensíveis sem o consentimento com quem quer que seja, embora as dificuldades geradas para o tratamento desses dados com base nas hipóteses autorizativas. Apesar de não termos uma orientação consolidada a respeito do tema, o § 3º, do art. 11, funciona como um importante mecanismo de tutela dos dados sensíveis, para além do regime comum de dados pessoais.

Traçados os contornos legais desse mecanismo de tutela, para uma melhor compreensão da disposição é imprescindível, brevemente, delinear questões centrais sobre as autoridades para proteção de dados e a sua configuração na LGPD, enquanto agente elementar da previsão do § 3º, do art. 11. Entre as citadas premissas apresentadas por Rodotà (2008, p. 87) para um ambiente jurídico adequado à circulação de informações está a existência de uma autoridade independente para elevar o controle a um paradigma coletivo, "eventualmente dotada de poderes para adaptar a situações particulares os princípios contidos nas cláusulas gerais".

Adotando-se, portanto, o paradigma de uma estratégia integrada de proteção de dados pessoais, a existência de órgãos públicos de vigilância é representada, por um consenso abrangente, a partir das autoridades administrativas independentes (RODOTÀ, 2008). No paradigma do Estado democrático, de uma maneira geral, é possível propor uma definição para esses órgãos administrativos, em atenção às correntes feições modernas, como

> entes ou órgãos públicos dotados de substancial independência do governo, caracterizados pela sua autonomia de organização, financiamento e contabilidade; de falta de controle e sujeição ao poder Executivo, dotadas de garantias de autonomia através da nomeação de seus membros, dos requisitos para esta nomeação e da duração de seus mandatos; e tendo função de tutela de interesses constitucionais em

[178] De maneira geral, o art. 30, da LGPD, prevê a possibilidade de a ANPD estabelecer normas complementares para a comunicação e o uso compartilhado de dados pessoais, embora sem mencionar a possibilidade de vedação (BRASIL, 2018a).

> campos socialmente relevantes (CARINGELLA; GAROFOLI, 2000, p. 10 apud DONEDA, 2006, p. 388).

A instituição das autoridades independentes para proteção de dados ganha evidência diante da agilidade gerada pelas técnicas de regulamentação não-legislativas para regular situações altamente dinâmicas, como as ligadas ao fator tecnológico, e à sua atuação específica aliada ao seu caráter eminentemente técnico, que obtém relevância diante da crescente complexidade das relações sociais e da organização do Estado (DONEDA, 2006).[179] Como analisa Doneda (2006, p. 389),

> foi necessário que a administração pública (e o próprio direito) se especializasse para atender a certas demandas com o particularismo necessário – até mesmo como uma forma de evitar que a regulação não-estatal ocupasse determinados espaços e os subtraísse à atuação do direito e, consequentemente, à aplicação dos princípios fundamentais do ordenamento em situações estratégicas.

A independência da autoridade não prescinde de localizar esse órgão fora das estruturas administrativas e burocráticas tradicionais, notadamente o executivo (RODOTÀ, 2008). Isso porque "são justamente as grandes burocracias públicas (além das privadas) que promovem as mais significativas coletas de informações, o que quer dizer que a função de vigilância deve ser estruturada de modo a obedecer uma lógica diferente daquela dos sujeitos a serem controlados" (RODOTÀ, 2008, p. 86).[180] Nessa direção, a independência das autoridades para proteção de dados pessoais é expressamente prevista na Carta de Direitos Fundamentais da União Europeia (UNIÃO EUROPEIA, 2000).[181]

---

[179] A unidade da personalidade humana e a consequente busca de equilíbrio entre as diversas garantias e direitos de natureza constitucional decorrentes suscitaram o problema da assim chamada colisão de direitos (DONEDA, 2006). Neste espaço, uma autoridade de garantia de direitos fundamentais encontra sua razão de ser, na promoção de um "equilíbrio dinâmico" entre estas situações subjetivas – organizando a "convivência pluralística" dos valores que se referem à pessoa (LAZZARA, 2001, p. 61-62 apud DONEDA, 2006, p. 398). Como pontua Doneda (2006, p. 387), "estes órgãos são hoje parte fundamental da estrutura administrativa e jurídica estatal, realizando a aproximação entre as esferas do Estado, do mercado e da pessoa em contextos por demais complexos e especializados para serem efetivamente regulados pelas instituições tradicionais".

[180] "A independência, atributo destas autoridades que reflete a sua própria razão de ser, lhes é atribuída por meio de mecanismos que afastem o máximo possível a sua atuação da influencia dos poderes estatais constituídos" (DONEDA, 2006, p. 393).

[181] "Art. 8.º Protecção de dados pessoais; 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente" (UNIÃO EUROPEIA, 2000, p. 10).

A definição do perfil da autoridade diz respeito a um juízo político (DONEDA, 2006). No Brasil, o desafio é significativo. Entre as dificuldades na atual regulamentação da ANPD[182] pela Lei 13.853 de 2019 que alterou a LGPD está a sua criação sem aumento de despesa e com a natureza jurídica transitória de órgão da administração pública federal, integrante da Presidência da República, de acordo com o art. 55-A (BRASIL, 2019b).[183] Não obstante, o Conselho Diretor, órgão máximo de direção da ANPD, será integralmente composto por indicação do Poder Executivo Federal, conforme o § 1º, do art. 55-D, da LGPD (BRASIL, 2019b). Em síntese, são vários os pontos conflitantes com o modelo de uma autoridade independente que podem gerar desafios para uma atuação consistente da ANPD no paradigma coletivo de controle dos dados pessoais e, mais especificamente, na sua atuação com relação ao referido mecanismo de tutela dos dados sensíveis.[184]

5.5 Limitações específicas ao tratamento de dados sensíveis referentes à saúde

Entre os dados sensíveis elencados no inciso II, do art. 5º, da LGPD, o legislador endereçou uma regulamentação particular sobre o tratamento dos dados pessoais referentes à saúde (BRASIL, 2019b). Como destacado, o § 3º, do art. 11, prescreve a possibilidade de vedação ou regulamentação, por parte da ANPD, em se tratando, de maneira geral, da comunicação e do uso compartilhado de dados sensíveis. Com relação aos dados referentes à saúde, o § 4º e o § 5º, do art. 11, dispõem nos seguintes termos:

---

[182] O inciso XIX, do art. 5º, da LGPD, define a autoridade nacional como "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional" (BRASIL, 2018a, sem paginação).

[183] "Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Lei nº 13.853, de 2019)" (BRASIL, 2019b, sem paginação).

[184] As dificuldades no cenário brasileiro se agravaram com a recente publicação do Decreto 10.046, de 09 de outubro de 2019, direcionado à definição de normas para o compartilhamento de dados dentro da Administração Pública Federal (BRASIL, 2019a). Além de deficiências em termos de controle e transparência, como identifica Danilo Doneda, o Decreto introduz conceitos conflitantes com a LGPD, estabelece uma perigosa concentração de dados pessoais, inclusive sensíveis, ignora a finalidade na utilização dos dados e abre largo campo para uma vigilância estatal (LUCA, 2019). Souza (2019a, sem paginação) pondera que: "O Decreto acerta ao determinar que as suas regras servem para orientar o compartilhamento de dados entre órgãos e entidades da Administração Pública Federal com a finalidade de (i) simplificar a oferta de serviços públicos; (ii) orientar a formulação, implementação e monitoramento de políticas públicas; (iii) possibilitar uma melhor análise sobre acesso a benefícios sociais e fiscais; e (iv) aumentar a eficiência das operações internas da Administração (art. 1º). O Estado brasileiro precisa mesmo ter padrões e diretrizes para o compartilhamento de dados dentro da Administração". No entanto, a criação do chamado Cadastro Base Cidadão pelo citado decreto pode representar uma janela para abusos pelo amplo acesso a um largo banco de dados (que está autorizado a incluir até mesmo a forma de andar da pessoa), além de que foi instituído sem uma participação da sociedade civil ou de qualquer forma de consulta pública, e de que o seu controle será realizado pelo Comitê Central de Governança de Dados, a ser integrado exclusivamente por membros da Administração Pública (SOUZA, 2019a).

> § 4º É vedada 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, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019)
> I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019b)
> II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019)
> § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019) (BRASIL, 2019b, sem paginação).

A princípio, a LGPD estabelece uma vedação à comunicação e ao compartilhamento desses dados quando o seu fundamento for a obtenção de vantagem econômica. Entretanto, são apresentadas três ressalvas a esta vedação, a saber, diante da prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, desde que seja demonstrado benefício ao interesse do titular dos dados e observadas uma das finalidades determinadas no dispositivo (BRASIL, 2019).

São duas as finalidades elencadas pela lei que autorizam o afastamento da vedação da comunicação ou o uso compartilhado dos dados referentes à saúde em vista de interesses econômicos: portabilidade de dados, quando solicitada pela pessoa à qual os dados se referem,[185] e as transações financeiras e administrativas resultantes do uso e da prestação dos serviços mencionados no § 4º, ou seja, no que se refere à saúde, à assistência farmacêutica ou à assistência de saúde (BRASIL, 2019b). A rigor, a LGPD estabelece uma cumulação do âmbito da comunicação ou do uso compartilhado dos dados referentes à saúde para a obtenção de vantagem econômica e a finalidade à qual a prática é destinada.

Além disso, o § 5º, do art. 11, dispõe sobre uma vedação adicional em se tratando de dados sensíveis referentes à saúde, no sentido de que planos privados de assistência à saúde não poderão realizar o tratamento destes dados para a prática de seleção de riscos na contratação de qualquer modalidade, bem como na contratação e exclusão de beneficiários. Em última análise, as condições de saúde da pessoa não poderão ser utilizadas para a definição de riscos e prêmios na contratação de seguros de saúde, assim como para fundamentar a sua exclusão. Na medida

[185] A portabilidade dos dados pessoais já figura como um direito do titular dos dados: "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) 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; (Redação dada pela Lei nº 13.853, de 2019)" (BRASIL, 2018a, sem paginação).

em que o direito social à saúde de matriz constitucional (art. 6º, CRFB) se relaciona diretamente à dignidade humana (BRASIL, 1988), é possível vislumbrar que a utilização desses dados poderia tornar excessivamente oneroso ou impedir que a pessoa pudesse ter acesso aos meios necessários à preservação da sua saúde.

A redação dos parágrafos 4º e 5º, do art. 11, é resultado da Lei 13.853 de 2019, que alterou a LGPD. Na redação original da LGPD não existia a previsão do § 5º, e o § 4º restringia a possibilidade da comunicação ou uso compartilhado dos dados referentes à saúde para fins econômicos aos casos de portabilidade ou na hipótese do consentimento da pessoa à qual os dados se referem (BRASIL, 2018a).[186] Como observam Lemos et. al. (2019), a redação original do § 4º acabaria por inviabilizar as atividades de hospitais, clínicas, laboratórios diagnóstico e operadoras de planos de saúde, que necessitam do uso compartilhado de dados pessoais para diversas operações de prestação do serviço de saúde, embora seja relevante frisar a importância do princípio da finalidade neste tocante.

No regime jurídico dos dados sensíveis, o GDPR endereça uma regulação específica para os dados referentes à saúde, em conjunto com os dados genéticos e os dados biométricos. No item 4, do art. 9º, o GDPR confere aos Estados-Membros a prerrogativa de "manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde" (UNIÃO EUROPEIA, 2016, p. 39). Portanto, competirá a cada Estado-Membro estabelecer eventuais vedações ou regulamentações ao tratamento desses dados, abrangente da comunicação e do uso compartilhado, que não contam com uma conformação prévia pelo GDPR, diferentemente do que foi verificado na LGPD.

5.6 Padrões técnicos de segurança e sigilo especiais para os dados sensíveis

A principiologia da LGPD endereça diretamente o tema da segurança e do sigilo dos dados pessoais a partir dos princípios da segurança, da prevenção e da responsabilização e

186 O § 4º dispunha originalmente nos seguintes termos: "É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular" (BRASIL, 2018a, sem paginação). A Medida Provisória 869 de 2018, que deu ensejo à Lei 13.853 de 2019, apresentava uma redação distinta e não previa o § 5º, posteriormente inserido no art. 11. Na redação do § 4º pela Medida Provisória era disposto: "§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses de: (Redação dada pela Medida Provisória nº 869, de 2018) I - portabilidade de dados quando consentido pelo titular; ou (Incluído pela Medida Provisória nº 869, de 2018) II - necessidade de comunicação para a adequada prestação de serviços de saúde suplementar. (Incluído pela Medida Provisória nº 869, de 2018)" (BRASIL, 2018b, sem paginação).

prestação de contas. Segurança[187] e sigilo representam dois elementos incontornáveis para que, de fato, seja possível falar em proteção de dados pessoais (SOUZA, 2019b).[188] As normativas dos princípios dispõem da seguinte forma:

> (...) VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> (...)
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> (...)
> X - responsabilização e prestação de contas: 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, 2018a, sem paginação).

No Capítulo VII, da LGPD, sobre "Segurança e Boas Práticas", a Seção I tem por fim tratar especificamente do tema da segurança e do sigilo dos dados (BRASIL, 2018a). A sistemática, que aborda temas como segurança da informação, ocorrência de incidentes de segurança[189] e os papéis dos agentes de tratamento e da própria ANPD no processo, faz referência específica aos dados sensíveis. De acordo com o art. 46:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

---

[187] Segundo o art. 44, da LGPD, o tratamento de dados é irregular quando não fornece ao titular a segurança que dele se espera (BRASIL, 2018a).

[188] A LGPD não inaugura uma disciplina de segurança e sigilo de dados no ordenamento jurídico brasileiro. O Código de Defesa do Consumidor não abordou diretamente tema da segurança na Seção VI, do Capítulo V, intitulada "Dos bancos de dados e cadastros de consumidores", embora a segurança do consumidor com relação aos produtos e serviços tenha sido endereçada (BRASIL, 1990). O Marco Civil da Internet, por sua vez, relacionou ao regime de guarda dos registros parâmetros de segurança, de acordo com o disposto nos artigos 13 e 15, nos seguintes termos: "Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. (...) Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento" (BRASIL, 2014, sem paginação).

[189] Incidente de segurança pode ser definido como a "violação das medidas adotadas pelos agentes de tratamento para salvaguardar a integridade e o sigilo dos dados pessoais sob a sua administração", podendo ser ocasionado por terceiro ou pelo próprio agente de tratamento, sendo que este último caso poderá ser configurado quando, por exemplo, for realizado o tratamento dos dados pessoais sob a sua responsabilidade para além da finalidade informada ao titular, a configurar a ilicitude da prática (SOUZA, 2019b, p. 430).

> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (BRASIL, 2018a, sem paginação).

No âmbito da segurança da informação, de acordo com o *Article 29 Data Protection Working Party* (2014), os processos e procedimentos devem garantir a confidencialidade, a integridade e a disponibilidade das informações durante todo o seu ciclo, sob pena de configurar um incidente de segurança.[190] As medidas de segurança elencadas pelo legislador perpassam a técnica[191] e a parte administrativa, a qual dependeria da estrutura organizacional dos agentes de tratamento.[192] Por certo, para que o fluxo informacional se desenvolva adequadamente, é imprescindível a adoção de medidas de segurança com a finalidade de impedir vulnerabilidades, acessos não autorizados ou qualquer evento que represente um tratamento inadequado ou ilícito dos dados pessoais,[193] que podem acarretar danos graves às pessoas às quais os dados se referem.[194]

No âmbito dos dados sensíveis, qualquer ocorrência dessa natureza ostentaria uma potencialidade lesiva maior que a dos demais dados pessoais.[195] Assim, ao normatizar o papel

---

[190] O *Article 29 Data Protection Working Party* (2014) categorizou os incidentes de segurança em três grupos: (i) incidente de confidencialidade, na oportunidade em que há acesso ou divulgação não autorizada de dados pessoais; (ii) incidente de integridade, quando há alteração não autorizada de dados pessoais; e (iii) incidente de disponibilidade, quando há perda de acesso ou destruição de dados.

[191] As medidas técnicas são compreendidas como aquelas adotadas no âmbito da Tecnologia da Informação (TI), a exemplo do uso de recursos informáticos dotados de funcionalidades direcionadas para a garantia da segurança da informação (JIMENE, 2018). São exemplos as ferramentas de autenticação para acesso a sistemas, mecanismos de segurança em *software* e *hardware*, recursos de controle de tráfego na rede, segregação de servidores, testes de vulnerabilidade, entre outros (JIMENE, 2018).

[192] No âmbito da segurança administrativa dos dados pessoais, Souza (2019b) afirma ser recomendável o desenvolvimento por parte do agente de tratamento de uma Política de Segurança da Informação, como uma referência de diretrizes para a segurança das informações, abrangente de orientações de condutas, proibições, boas práticas e até sanções. De acordo com o autor, o próprio art. 50, da LGPD, consistiria em um programa de governança em privacidade (SOUZA, 2019b). A propósito, o § 1º, do art. 50, da LGPD, faz expressa referência à consideração da natureza dos dados quando do estabelecimento das regras de boas práticas, o que pode remeter a uma modulação das regras em consonância com os dados de natureza sensível (BRASIL, 2018a).

[193] Recomenda-se a leitura do *Cost of a Data Breach Report* 2019 realizado pela IBM em parceria com o *Ponemon Istitute*. Disponível em: https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.113564289.747736549.1571252357-1491045400.1571252357. Acesso em: 16 out. 2019.

[194] Em episódio ocorrido recentemente, em 08 de outubro de 2019, mais de setenta milhões de brasileiros tiveram seus dados pessoais vazados pela descoberta de uma brecha de segurança no sistema do Departamento Estadual de Trânsito do Rio Grande do Norte (Dentran-RN) (GAVIOLI, 2019). Como o Detran do Brasil possui os sistemas estaduais integrados, todos os brasileiros que possuem Carteira Nacional de Habilitação tiveram os seus dados pessoais expostos no site do Detran do Rio Grande do Norte (GAVIOLI, 2019). Em 2017, foram relatados variados casos de vazamentos de dados, como o do Petágono nos Estados Unidos e o do birô de crédito Equifax, com o registro de aumento de 44,7% de ocorrências de vazamento de dados nos Estados Unidos se considerado o ano anterior (IDENTITY THEFT RESOURCE CENTER, 2017).

[195] É significativo o caso citado por Mulholland (2018, p. 160-161): "Em 2016, uma prestadora de serviços de coleta e doação de sangue na Austrália, a *Red Cross Blood Service*, sofreu um duro golpe em seu sistema de segurança de dados, quando informações referentes a 550.000 doadores de sangue vieram a público devido à transferência de um arquivo contendo informações desses doadores a um ambiente computacional não seguro, acessível por pessoas sem a devida autorização para manejar aqueles dados. Os dados se referiam a coletas de

da ANPD[196] no sentido de estabelecer padrões técnicos para a segurança dos dados consagrado no *caput* do art. 46, o § 1º faz uma ressalva especial para o contexto dos dados sensíveis, além de reiterar a importância da principiologia da LGPD (BRASIL, 2018a). A rigor, como previsto no dispositivo, os padrões de segurança devem considerar a natureza das informações, as características específicas do tratamento e estado atual da tecnologia (BRASIL, 2018a), o que repercute na necessária modulação dos padrões de segurança e sigilo a serem exigidos para os dados sensíveis, sobretudo pelas capacidades de discriminação e estigmatização ínsitas ao tratamento desses dados.[197]

Nessa direção, o Considerando 75, do GDPR, associa diretamente os riscos atinentes aos direitos e liberdades individuais aos dados considerados sensíveis, o que demandaria, de acordo com o Considerando 74, medidas de segurança e de responsabilidade condizentes com essa potencialidade lesiva.[198] Portanto, é razoável compreender a menção explícita à especialidade dos dados sensíveis em termos de padrões de segurança e sigilo, além da

---

sangue realizadas entre os anos de 2010 e 2016. Dentre as informações contidas na base de dados, uma era especialmente sigilosa, qual seja, a que especificava que determinado doador seria 'pessoa com comportamento sexual de risco'. Essa categorização era determinada por meio de questionário do tipo 'verdadeiro-falso' disponibilizado ao doador no momento da coleta de sangue, em que se perguntava se o mesmo havia participado de atividades sexuais de risco nos últimos 12 meses. Tanto as perguntas realizadas no questionário, como as respostas, compunham a base de dados e estabeleciam a conexão com o doador, individualizado por seu nome e pelas demais informações pessoais. A *Red Cross* pediu desculpas formais aos doadores e disponibilizou todo um aparato de atendimento às pessoas que tiveram seus dados violados".

[196] O art. 55-B, da LGPD, estabelece a autonomia técnica da ANPD (BRASIL, 2019b).

[197] Os questionamentos anteriormente lançados com relação à consolidação da ANPD devem ser reiterados. No entanto, para Souza (2019b), a falta de regulamentação por parte da ANPD não seria óbice à aplicação das medidas de segurança e sigilo, na medida em que poderiam ser utilizadas as definições do Decreto 8.771/16 que regulamenta o Marco Civil da Internet, detalhando padrões de segurança e sigilo dos dados pessoais, dos registros e de comunicações privadas no seu Capítulo III. Não obstante, Souza (2019b) faz referência à norma da ABNT ISSO/IEC 17799:200, conhecida como "Código de prática para a gestão da segurança da informação", que poderia ser utilizada como subsídio para os agentes de tratamento, na medida em que dispõe sobre condutas e medidas para preservar a segurança dos dados sob sua responsabilidade. Todavia, a necessária modulação desses padrões de segurança e sigilo para os dados sensíveis deve ser assinalada.

[198] De acordo com o Considerando 74: "Deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares" (UNIÃO EUROPEIA, 2016, p. 14). Por sua vez, o Considerando 75 dispõe que: "O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas (...)" (UNIÃO EUROPEIA, 2016, p. 15).

necessidade de atentar para a natureza da informação quando da fixação dos parâmetros, no § 1º, do art. 46, da LGPD, como um mecanismo de tutela. Em última análise, a tecnologia exercerá um papel elementar nesse contexto.

A interface entre direito e tecnologia apresenta desafios multifacetados, a demandar esforços de outras estruturas, como da ética[199], e da própria tecnologia. Apesar das aplicações tecnológicas estabelecerem uma relação de dependência com uma complexa coesão entre as forças do mercado, do governo e a pressão dos consumidores, compete ao direito a reafirmação do seu valor fundamental (DONEDA, 2006). Para tanto, além da mera consideração da oposição entre direito e tecnologia, busca-se o equilíbrio e a harmonização entre esses fatores, na medida em que determinados aspectos da tecnologia devem ser ajustados possivelmente valendo-se da própria tecnologia (DONEDA, 2006).

A propósito, Lessig (2006) aborda na "teoria do ponto patético" quatro formas de regulação social utilizadas com o fim de restringir comportamentos que se complementam, quais sejam, o direito, as normas sociais, o mercado e a arquitetura.[200] Através do direito é possível restringir comportamentos pela ameaça de punição. As normas sociais operam através da atribuição de um estigma imposto por uma comunidade a uma certa conduta. O mercado restringe comportamentos através do preço exigido para o desempenho de uma conduta. A arquitetura atribui uma carga física como fator limitador de um comportamento (LESSIG, 2006).

Na proposta de Lessig (1999), a arquitetura deve ser analisada criticamente, assim como analisamos criticamente a lei.[201] Embora os mecanismos tecnológicos não possam ser tomados como uma forma de tutela plenamente satisfatória, a sua interferência sobre a arquitetura sobre

---

[199] Como ramo da ética, a ética de dados tem por fim direcionar problemas morais relativos a dados (incluindo geração, registro, curadoria, processamento, compartilhamento e uso), algoritmos (incluindo AI, aprendizado de máquina e robôs) e práticas relacionadas (como inovação responsável, programação e códigos profissionais) para formular e apoiar soluções moralmente boas (FLORIDI; TADDEO, 2016). Temas éticos relacionados a privacidade, tratamento de dados pessoais, anonimato, transparência e outros podem ser endereçados a este campo da ética que se desenha na era digital, ainda que não se traduzam necessariamente em informação, no entanto exerçam um impacto significativo no comportamento humano (FLORIDI; TADDEO, 2016). A CNIL - Autoridade Francesa de Proteção de Dados - definiu a ética no seu relatório *How can humans gain the upper hand? Ethical issues of algorithms and artificial intelligence* como processo de orientação em questões legais, e o padrão ético como prefiguração do padrão da lei (DONEDA et. al., 2018).

[200] "The code or software or architecture or protocols set these features, which are selected by code writers. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it too is regulation, just as the architectures of real-space codes are regulations" (LESSIG, 2006, p. 125). "We can't help but consider the technologies, or as I've called them, the architectures of privacy in evaluating the world of privacy we are entering. For the world we are entering is about to change these architectures of privacy more completely and more extensively than any similar change in the past" (LESSIG, 1999, p. 59).

[201] A arquitetura do ciberespaço pode adotar a coleta de dados como padrão, o que a tornaria constante e invisível, sem que a pessoa fosse perturbada com a coleta e, portanto, contra ela pudesse se insurgir (LESSIG, 1999).

a qual são situados os dados pessoais evidencia a sua importância em termos de consequências para a configuração jurídica do problema, inclusive como instrumento de atuação de políticas públicas na área (DONEDA, 2006).[202] Apesar da natureza de direito fundamental da proteção de dados pessoais, a sua tutela deve valer-se de uma estratégia integrada de diversos instrumentos, representando manifestações específicas de áreas distintas da proteção de dados pessoais (DONEDA, 2006).

Em última análise, é possível vislumbrar uma desproporção entre o "dever ser" do direito e a complexidade dos avanços tecnológicos, a demandar uma atualização dos sistemas jurídicos para as novas tecnologias (FERES; OLIVEIRA, 2017). É razoável considerar que a LGPD é orientada por uma técnica legislativa permeável à consideração da influência da tecnologia em sede de proteção de dados, que é referida em diversas oportunidades na redação legal.[203] Em termos do estabelecimento de padrões de segurança e sigilo dos dados pessoais, a arquitetura pode agregar uma significativa efetividade aos comandos da LGPD.

Com efeito, como consideram Feres e Oliveira (2017, p. 251), "ao compreender a capacidade e a complexidade envolvida nos códigos tecnológicos, as medidas regulatórias podem trazer novas perspectivas para que as legislações se atualizem aos novos tempos". A atuação da ANPD é fundamental nesse tocante, na medida em que a LGPD normatiza diversos eixos a serem por ela regulamentados, em atenção aos avanços tecnológicos, evitando-se uma obsolescência e a inefetividade do marco regulatório geral brasileiro sobre proteção de dados.

A LGPD faz expressa referência à necessidade de estruturar os sistemas utilizados para o tratamento de dados pessoais no sentido de atender aos requisitos de segurança, aos padrões de boas práticas e de governança e à principiologia da norma (BRASIL, 2018a).[204] A utilização das *Privacy Enhancing Tecnologies* (PET) ganha relevo na medida em que podem impossibilitar, limitar ou mesmo facilitar determinada ação que englobe o tratamento de dados pessoais, compreendendo as tecnologias utilizadas para proteger a privacidade, com o *design* voltado a dar um maior controle técnico sobre os dados pessoais (LESSIG, 2006).

Como exemplo de PET pode ser mencionada a criptografia, enquanto técnica de confidencialidade em segurança computacional, destinada a assegurar que apenas o emissor e o destinatário da comunicação tenham acesso à chave criptográfica (simétrica ou assimétrica)

---

[202] Como acrescenta Doneda (2006, p. 370), "a utilização da tecnologia para a proteção de dados pessoais, que traz à tona o debate sobre a técnica, apresenta-se no conjunto como um contraponto a outas formas de atuação da tecnologia, que de forma alguma pode substituir a ação do direito".

[203] É exemplo a já citada possibilidade de reversão do processo de anonimização.

[204] O art. 49 prescreve que: "Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares" (BRASIL, 2018a, sem paginação).

apta a decifrar as informações nas "pontas" e, portanto, acessar e compreender o seu conteúdo informativo (MACHADO; DONEDA, 2018). Uma vez criptografado, o dado pode ser caracterizado como pseudonimizado, podendo atrair um regime jurídico particularizado, apesar de não perder a natureza de dado pessoal (MACHADO; DONEDA, 2018).[205]

Associada à noção de arquitetura, é relevante destacar a referência da LGPD à *privacy by design*, na medida em que o § 2º, do art. 46, refere-se à necessidade de adoção das medidas de segurança e sigilo dos dados pessoais da concepção do produto ou do serviço até a sua execução (BRASIL, 2018a), o que incluiria o desenvolvimento, a aplicação e a sua avaliação.[206] O conceito de *privacy by design* foi desenvolvido na década de 1990 por Ann Cavoukian, Comissária de Informação e Privacidade da Província de Ontário, Canadá, entre os anos 1997 e 2014. Parte-se do pressuposto de que o futuro da construção de um paradigma de proteção de dados depende de uma mudança organizacional, não restrita ao cumprimento de parâmetros regulatórios, mas de uma reflexão por parte dos agentes de tratamento no sentido de que, idealmente, a garantia da privacidade se torne um padrão do modo de operação (CAVOUKIAN, 2009).[207]

A referência da *privacy by design* é orientada por sete princípios fundamentais sumarizados por Cavoukian (2009): (i) proatividade e prevenção; (ii) privacidade por padrão (referida por *privacy by default*);[208] (iii) privacidade incorporada ao design; (iv) funcionalidade integral;[209] (v) segurança em todo o ciclo de vida da informação; (vi) visibilidade e transparência e (vii) respeito à privacidade do usuário (perspectiva centrada no usuário).[210] A

---

[205] A encriptação dos dados é exemplo em uma das hipóteses que dispensa a exigência do dever de notificação de incidente de segurança que resulte em altos riscos a direitos e liberdades fundamentais do titular dos dados, de acordo com o art. 34, item 3, "a", do GDPR (UNIÃO EUROPEIA, 2016).

[206] A necessidade de adoção de medidas técnicas e organizacionais desde a concepção do tratamento de dados já era prevista no art. 46, da Diretiva 95/46/CE. O GDPR, nessa direção, faz referência à "proteção de dados desde a concepção" no art. 25, além do Considerando 78 (UNIÃO EUROPEIA, 2016).

[207] Com o imperativo da *privacy by design*, "a privacidade se torna um componente essencial da funcionalidade principal do que está sendo entregue" (TEPEDINO; TEFFÉ, 2019, p. 294).

[208] Com base na *privacy by default*, os dados pessoais seriam protegidos em qualquer sistema de Tecnologia da Informação ou prática negocial por padrão, de forma que nenhuma ação por parte do indivíduo deve ser exigida para a proteção da sua privacidade, uma vez que esse cuidado já seria ínsito ao sistema (SOUZA, 2019b). Bioni (2019), por sua vez, destaca que o conceito de *privacy by default* pode ser extraído na LGPD dos princípios da necessidade e o da responsabilidade e prestação de contas.

[209] Com base no princípio da funcionalidade, Cavoukian (2009) sustenta que a *privacy by design* tem por fim conciliar todos os interesses legítimos envolvidos, que não deverão necessariamente recorrer a uma ideia de *trade-off*. Em última análise, a partir da *privacy by design* seriam evitadas falsas dicotomias, como o exemplo da privacidade contra a segurança, de forma a reconhecer que as duas podem ser conciliadas (CAVOUKIAN, 2009). "Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy)" (CAVOUKIAN, 2009, sem paginação).

[210] Ver mais em Cavoukian (2009).

partir desses fundamentos, a *privacy by design* se apresenta como uma funcionalização da arquitetura em vista da proteção da pessoa que, a rigor, opera como um dos mecanismos dispostos na LGPD para a construção de um paradigma da circulação controlada de dados.[211]

A propósito, relacionado ao tema de segurança e sigilo dos dados pessoais, é importante destacar que a ANPD poderá determinar ao controlador que elabore um relatório de impacto à proteção de dados pessoais[212], incluindo os dados sensíveis, com relação aos termos do tratamento de dados, de acordo com o art. 38, da LGPD (BRASIL, 2018a),[213] que, em última análise, se inspira no regime do art. 35, do GDPR. A elaboração do relatório não depende de requisição por parte da ANPD, mas poderá ser realizado de forma proativa pelo controlador como medida de garantir uma melhor compreensão do impacto do tratamento dos dados pessoais (SOUZA, 2019b). A sua relevância para o tratamento de dados sensíveis deu ensejo à previsão do art. 35, item 3, "b", do GDPR, que determina a obrigatoriedade da realização da avaliação de impacto quando se tratar de "Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.o, n.o 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o", sendo os dados elencados no art. 9, item 1, os dados considerados sensíveis (UNIÃO EUROPEIA, 2016, p. 53).

Em verdade, uma vez reconhecida a progressiva relevância da tecnologia no tecido social, Rodotà (2005, 2008) evidencia que a sua legitimação não pode ser confiada apenas ao imperativo da segurança pública, da eficiência ou da lógica econômica, de forma que a disponibilidade de uma tecnologia não legitima todas as formas da sua utilização, que deve ser avaliada com base em valores diferentes dos fornecidos pela técnica. Em um paradigma constitucional, a tutela da pessoa, como valor fundamental do ordenamento jurídico, representa o valor que deve funcionalizar a tecnologia, ganhando particular relevo para a proteção dos dados sensíveis e, mais adiante, do princípio da igualdade material.

---

[211] Para Jimene (2018, p. 338), "a dinâmica por trás do conceito do *privacy by design* é a perfeita associação entre direito e tecnologia, de modo a implementar no desenho da arquitetura da rede mecanismos técnicos que possam garantir a efetividade de direitos dos seus usuários, por padrão, a benefício do ser humano".

[212] A LGPD define no inciso XVII, do art. 5º, o relatório de impacto à proteção de dados pessoais como "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (BRASIL, 2018a, sem paginação).

[213] O parágrafo único, do art. 38, dispõe que: "Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados" (BRASIL, 2018a, sem paginação).

6. CONCLUSÃO

Em termos de pós-modernidade e da crescente importância da informação em diversas estruturas da sociedade, o livre desenvolvimento da personalidade estabelece uma relação intrínseca com a privacidade e com a proteção de dados pessoais. Entre os múltiplos desafios, o processo de fragmentação da pessoa em dados promovido pelos avanços tecnológicos cresce exponencialmente no paradigma de hiperconectividade, aliado ao desenvolvimento das potencialidades de extração de valor dos dados. O interesse no petróleo dos novos temos, por parte de agentes públicos e privados, promove diversas repercussões econômicas, políticas, sociais e, por conseguinte, jurídicas.

A privacidade, enquanto direito dinâmico e complexo, se desenvolveu para situar nos dados pessoais a centralidade da sua tutela com a inserção na sua definição da autodeterminação informativa, compreendida como o direito da pessoa manter controle sobre as suas informações e de determinar a forma de construir a sua esfera privada. A proteção de dados pessoais desdobra-se da privacidade, permanece compartilhando o mesmo fundamento ontológico da dignidade humana, mas assume funções centrais em face de valores socialmente compartilhados, como a democracia e diversos direitos fundamentais. A referência a uma sociedade movida a dados é representativa de uma conjuntura sem precedentes.

A agenda da circulação controlada de dados pessoais delineia uma nova forma de distribuição de poder. O controle de dados pessoais, a partir da perspectiva individual e da coletiva, concorre para assegurar a proteção do corpo eletrônico da pessoa, constituído por dados pessoais e coexistente com o corpo físico. A instrumentalização, portanto, do corpo eletrônico como eixo de múltiplos interesses heterônomos não colhe em um paradigma de proteção da pessoa, devendo ser protegido assim como o corpo físico, sobretudo em face da cláusula geral de tutela e promoção da pessoa humana.

O debate da proteção de dados pessoais em diversas experiências jurídicas pelo mundo foi acompanhado da categoria dos dados de natureza sensível. Entre os dados pessoais é situada a categoria dos dados sensíveis, qualificados por extrapolar o tema da proteção de dados, alçando-o diretamente a termos de igualdade material. A ontologia dos dados sensíveis é associada à sua potencialidade de discriminar e estigmatizar, repercutindo no livre desenvolvimento da personalidade e na fruição de múltiplos direitos fundamentais.

O fluxo de dados sensíveis carrega consigo aspectos fundamentais da pessoa que podem interferir direta e indevidamente na sua vida. Não proteger os dados sensíveis equivale a não

permitir que a pessoa tome livremente as decisões estruturantes da sua personalidade sem ser estigmatizada, além de abrir campo para que a pessoa seja subjugada por condições das quais não escolheu, a exemplo das suas características genéticas. Embora sejam formuladas críticas à categorização dos dados sensíveis no desafiador contexto do *Big Data*, a proteção desses dados ganha ainda maior relevo diante da sua potencialidade lesiva na era digital. As possibilidades tecnológicas que até então se expressavam quantitativamente se ampliam em uma dimensão qualitativa, com sistemas que não raro reproduzem e ampliam as discriminações que são, de certa forma, endereçadas pela proteção dos dados sensíveis, não raro utilizados como insumo desses sistemas.

Em face dos avanços tecnológicos, que não ostentam limites intrínsecos e não se submetem *per se* a condicionamentos extrínsecos, o direito se apresenta como uma das estruturas que podem condicionar a realidade com a centralidade na tutela da pessoa, como decisão política à frente da natureza das coisas. A Lei Geral de Proteção de Dados Pessoais, o primeiro marco regulatório geral brasileiro em sede de proteção de dados, emerge com o imperativo de controle, fortemente inspirado no modelo da União Europeia do *General Regulation Data Protection*, embora o Brasil conte com uma cultura incipiente de proteção de dados pessoais.

Com a referência teórica de Stefano Rodotà sobre a ontologia dos dados sensíveis e partir dos delineamentos de pesquisa bibliográfica e documental, foi traçada uma análise qualitativa da LGPD com a finalidade de identificar os mecanismos de tutela previstos especificamente para os dados sensíveis, para além do regime jurídico geral dos dados pessoais na regulação brasileira. Para tanto, o regime comum dos dados pessoais da LGPD e o modelo do GDPR foram utilizados com o propósito de uma abordagem comparativa, notadamente para melhor compreender as distinções que a LGPD estabelece para o tratamento dos dados sensíveis.

Através do desenvolvimento da pesquisa foi possível identificar que dentro de um conceito amplo de dado pessoal, definido como informação relacionada a pessoa natural identificada ou identificável, a LGPD categoriza os dados sensíveis não a partir de um conceito, mas de um rol de conteúdos informacionais considerados sensíveis, na mesma direção do GDPR. Uma vez qualificado o dado pessoal como sensível atrai-se um regime jurídico particularizado, no qual foram identificados seis mecanismos de tutela específicos.

O primeiro mecanismo de tutela identificado na LGPD foi uma maior qualificação do consentimento para o tratamento de dados sensíveis. Apesar das limitações do instituto do consentimento em razão da sua perspectiva unidimensional, há de ser reconhecida a sua

relevância como instrumento para a autodeterminação informativa, desde que situado no paradigma de que os dados pessoais dizem respeito às situações existenciais. Para além do regime comum dos dados pessoais, no qual o consentimento deve ser livre, informado, inequívoco e, inquestionavelmente, destinado a finalidades determinadas em atenção ao princípio da finalidade, em face dos dados sensíveis o consentimento demanda uma carga participativa maior da pessoa em razão dos riscos subjacentes ao seu tratamento, oportunidade em que a LGPD o qualifica adicionalmente como destacado e expresso, como se depreende da *ratio* por detrás do qualificador "específico".

As hipóteses legais que autorizam o tratamento dos dados sensíveis são mais restritas que as previstas no regime comum dos dados pessoais, embora a amplitude que essas hipóteses podem assumir, a demandar uma maior cautela. A rigor, em que pese a consideração de interesses que não exclusivamente a vontade da pessoa, como os de ordem pública, a saúde e o exercício de direitos, os interesses essencialmente patrimoniais foram alijados das hipóteses que autorizam o tratamento de dados sensíveis, como a proteção ao crédito e a execução de contrato.

Os avanços das possibilidades tecnológicas em termos de processamento de dados foram endereçados, de certa forma, pela expansão do regime jurídico dos dados sensíveis para o tratamento sensível de dados pessoais, ou seja, o tratamento de dados pessoais não sensíveis que tem a aptidão de revelar dados sensíveis e causar dano. Apesar da larga abrangência que essa previsão pode assumir, erige-se como uma forma de ampliar a proteção dos dados sensíveis através da antecipação da potencialidade lesiva que dados pessoais não sensíveis podem revelar.

Com relação ao uso compartilhado de dados sensíveis que tem a propensão de ampliar os agentes da cadeia de tratamento de dados e, portanto, dilatar a sua potencialidade lesiva, a LGPD estabelece a possibilidade de vedação ou regulamentação por parte da ANPD quando o uso compartilhado se destinar a fins econômicos. Constitui-se, a princípio, como um importante instrumento na defesa da pessoa através dos seus dados sensíveis, sobretudo em razão do caráter existencial dos dados. No entanto, a efetivação desse mecanismo de tutela dependerá, em última análise, da constituição e, por conseguinte, da atuação consistente da ANPD.

Os dados sensíveis relativos à saúde, notadamente diante da vulnerabilidade que a pessoa se encontra nesse âmbito, ganham uma regulação adicional. A própria LGPD restringe as hipóteses em que poderá ocorrer o tratamento compartilhado desses dados para fins econômicos, além de vedar a sua utilização pelos agentes privados da área de assistência à saúde para a seleção de riscos em termos de contratação e exclusão de beneficiários.

A LGPD faz referência à especialidade dos padrões técnicos de segurança e sigilo de

dados sensíveis a serem estabelecidos pela ANPD. A tecnologia emerge, portanto, como um forte eixo para promover a proteção dos dados pessoais sensíveis em uma estratégia integrada de tutela. Desde que norteada por valores diferentes dos oferecidos pela técnica, a tecnologia é um instrumento importante para a proteção da privacidade e dos dados pessoais, embora reconhecida a sua insuficiência para promover a tutela em se tratando de direitos fundamentais. Em última análise, a permeabilidade ao fator tecnológico que a LGPD estabelece, inclusive através da atuação da ANPD, configura-se como uma medida relevante para fins de efetividade e atualização do marco regulatório.

Na direção de diversas experiências jurídicas pelo mundo, é possível depreender que a LGPD normatizou o entendimento de que os dados pessoais sensíveis demandam um *standard* de proteção acima dos dados pessoais não sensíveis, por veicularem um conteúdo informacional tradicionalmente associado a práticas discriminatórias. Com efeito, a hipótese inicial da pesquisa foi confirmada, na medida em que foi verificado o estabelecimento, por parte da LGPD, de uma proteção para os dados sensíveis significativamente acima do regime comum dos dados pessoais a partir de mecanismos de tutela próprios, embora devam ser assinalados desafios com relação à interpretação e à implementação da normativa.

Em realidade, as múltiplas adversidades para a proteção integral da pessoa são elevadas a um outro patamar com o fluxo informacional. Para além dos desafios no plano imediato da materialidade, que no Brasil dizem respeito a deficiências na educação, desigualdade social, preconceitos, saúde, miséria e outros, a exponencial evolução da tecnologia adiciona outros obstáculos. Os avanços tecnológicos podem operar para amplificar os problemas de ordem social, política e econômica, com novos desenhos de concentração de poder, ou podem ser funcionalizados para a pessoa e, portanto, para os valores compartilhados socialmente. Sobretudo, importa ampliar a visão para se atentar à proteção da pessoa em novos cenários a serem desbravados na realidade brasileira, como é o caso da agenda de proteção de dados pessoais.

REFERÊNCIAS

ARGENTINA. **Ley de Protección de Los Datos Personales**. 2000. Disponível em: <https://www.oas.org/juridico/pdfs/arg_ley25326.pdf>. Acesso em: 09 ago. 2019.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Advice paper on special categories of data ("sensitive data")**. 2011. Bruxelas, Disponível em: <https://www.pdpjournals.com/docs/88417.pdf>. Acesso em: 09 ago. 2018.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 03/2014 on Personal Data Breach Notification**. 2014. Bruxelas, Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf>. Acesso em: 09 ago. 2018.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 4/2007 on the concept of personal data**. Bruxelas: [s. n.], 2007. Disponível em: <http://ec.europa. eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_ en.pdf>. Acesso em: 10/08/2019.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines On Automated Individual Decision-making And Profiling For The Purposes Of Regulation 2016/679 Adopted**. 2017. Bruxelas, Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>. Acesso em: 09 ago. 2018.

BAIÃO, Kelly Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. **Civilistica.com**. Rio de Janeiro, a. 3, n. 2, jul.-dez./2014. Disponível em: <http://civilistica.com/a-garantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-da-dignidade-da-pessoa-humana/>. Acesso em: 15 ago. 2017.

BAROCAS, Solon. **Data mining and discourse on discrimination.** 2014. Proceedings of the Data Ethics Workshop, Conference on Knowledge Discovery and Data Mining (KDD). Disponível em: <http://www.cs.yale.edu/homes/jf/Barocas-Taxonomy.pdf>. Acesso em: 09 jul. 2018.

BARROSO, Luís Roberto. **Conferência Nacional de Internet 2019**. Brasília: ITS Rio, 2019. Son., color. Disponível em: <https://www.youtube.com/watch?v=BlUsshfPCqM>. Acesso em: 07 maio 2019.

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

BRANCO, Sergio. **Memória e esquecimento na internet**. Porto Alegre: Arquipélago, 2017.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 07 out. 2019.

BRASIL. Decreto nº 10.046, de 09 de outubro de 2019a. Brasília, 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm>. Acesso em: 10 out. 2019.

BRASIL. Lei nº 7.716, de 5 de janeiro de 1989. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L7716.htm>. Acesso em: 09 jul. 2019.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Brasília, 1990b. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 10 jul. 2018.

BRASIL. Lei nº 8.080, de 19 de setembro de 1990. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8080.htm>. Acesso em: 09 jul. 2019.

BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. **Código Civil**. Brasília, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 10 jul. 2018.

BRASIL. Lei nº 12.414, de 09 de junho de 2011a. **Lei do Cadastro Positivo**. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm>. Acesso em: 03 out. 2019.

BRASIL. Lei nº 12527, de 18 de novembro de 2011b. **Lei de Acesso à Informação**. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 09 out. 2017.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 07 jul. 2018.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018a. **Lei Geral de Proteção de Dados Pessoais**. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 10 jul. 2019.

BRASIL. Lei nº 13.853, 08 de julho de 2019b. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2>. Acesso em: 30 jul. 2019.

BRASIL. Medida Provisória nº 869, de 27 de dezembro de 2018b. Altera a Lei nº 13.709, de 14 de agosto de 2018. Brasília, Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm>. Acesso em: 06 fev. 2019.

BRASIL. Projeto de Lei n. 5.276, de 13 de maio de 2016 (da Câmara dos Deputados). Brasília, Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016>. Acesso em: 10 set. 2017.

BRASIL. Proposta de Emenda à Constituição nº 17, de 2019c. Brasília, Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1567535523044&disposition=inline>. Acesso em: 09

ago. 2019.

BRASIL. Superior Tribunal de Justiça. Acórdão nº 1.193.764, Terceira Turma. **Recurso Especial 1.193.764**. Brasília, 08 ago. 2011c.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian**. [S.l.]. 17 mar. 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em: 06 jul. 2018.

CAVOUKIAN, Ann. **Privacy by Design:** The 7 Foundational Principles. 2009. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso em: 09 out. 2018.

CLAVELL, Gemma Galdon. **O que acontece com nossos dados na internet?** 2015. El País. Disponível em: <https://brasil.elpais.com/brasil/2015/06/12/tecnologia/1434103095_932305.html>. Acesso em: 04 mar. 2017.

COHEN, Julie E. Examined Lives: Informational Privacy and the Subject as Object. **Stanford Law Review**, Stanford, v. 52, n. 5, p.1373-1438, 2000.

COMISSÃO EUROPEIA. **Adequacy decisions.** 2019. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em: 09 out. 2019.

COMISSÃO EUROPEIA. **Diretrizes Éticas Para Inteligência Artificial Confiável**. Bruxelas, 2019. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>. Acesso em: 20 maio 2019.

CONSELHO DA EUROPA. **Convention 108 +: Convention For The Protection Of Individuals With Regard To The Processing Of Personal Data**. Strasbourg: Conseil de l'Europe, 2018. Disponível em: <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>. Acesso em: 10 jul. 2019.

CONSELHO DA EUROPA. **Resolution (73) 22 On The Protection Of The Privacy Of Individuals Vis-a-vis Electronic Data Banks In The Private Sector**. Estrasburgo, Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830>. Acesso em: 09 jun. 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico.** Joaçaba, v. 12, n. 2, pp. 91-108, jul/dez 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/download/1315/658>. Acesso em: 01 set. 2017.

DONEDA, Danilo; ALMEIDA, Virgílio A. F. **O que é a governança de algoritmos?** 2016. Disponível em: <https://politics.org.br/edicoes/o-que-é-governança-de-algoritmos>. Acesso em: 20 maio 2019.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo Cesar Maganhoto et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar - Revista de Ciências Jurídicas**, [s.l.], v. 23, n. 04, p.1-17, 2018. Fundacao Edson Queiroz. http://dx.doi.org/10.5020/2317-2150.2018.8257. Disponível em: <https://periodicos.unifor.br/rpen/article/view/8257/pdf>. Acesso em: 09 jun. 2019.

DONEDA, Danilo; MONTEIRO, Marília. **Acesso à informação e privacidade no caso da Universidade Federal de Santa Maria.** 2015. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/acesso-a-informacao-e-privacidade-no-caso-da-universidade-federal-de-santa-maria-02072015>. Acesso em: 08 mar. 2019.

ESTADOS UNIDOS. **COPPA - Children's Online Privacy Protection Act**. 1998. Washington, Disponível em: <http://www.coppa.org/coppa.htm>. Acesso em: 09 out. 2018.
ESTADOS UNIDOS. **Fourth Amendment**. 1789. Disponível em: <https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv>. Acesso em: 09 out. 2018.

FERES, Marcos Vinício Chein; OLIVEIRA, Jordan Vinicius de. Dos Códigos Legais aos Códigos do Ciberespaço: reflexões sobre Direito e Deep Web. **Revista de Propriedade Intelectual, Direito Contemporâneo e Constituição**, Aracaju, v. 11, n. 2, p.234-253, jun. 2017. Disponível em: <http://www.pidcc.com.br/artigos/11022017/09.pdf>. Acesso em: 06 out. 2019.

FLORIDI, Luciano; TADDEO, Mariarosaria. What is data ethics? **Philosophical Transactions Of The Royal Society A**: Mathematical, Physical and Engineering Sciences, [s.l.], v. 374, n. 2083, pp. 1-8, 28 dez. 2016. The Royal Society.

FRAZÃO, Ana. Apresentação da obra. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Brasil, 2019a. pp. 5-6.

FRAZÃO, Ana. **Nova LGPD: a importância do consentimento para o tratamento dos dados pessoais.** 2018a. Jota. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018>. Acesso em: 01 jul. 2019.

FRAZÃO, Ana. **Controvérsias sobre direito à explicação e à oposição diante de decisões automatizadas.** 2018b. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/controversias-sobre-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-automatizadas-12122018>. Acesso em: 07 jun. 2019.

FRAZÃO, Ana. **Nova LGPD: o tratamento dos dados pessoais sensíveis.** 2018c. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018>. Acesso em: 04 dez. 2018.

FRAZÃO, Ana. **Nova LGPD: tratamento dos dados de crianças e adolescentes.** 2018d. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-

mercado/nova-lgpd-tratamento-dos-dados-de-criancas-e-adolescentes-03102018>. Acesso em: 04 dez. 2018.

FRAZÃO, Ana. **O direito à explicação e à oposição diante de decisões totalmente automatizada.** 2018e. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018>. Acesso em: 07 jun. 2019.

FRAZÃO, Ana. **Quais devem ser os parâmetros éticos e jurídicos para a utilização da IA?** 2019b. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/quais-devem-ser-os-parametros-eticos-e-juridicos-para-a-utilizacao-da-ia-24042019>. Acesso em: 20 jun. 2019.

GAVIOLI, Allan. **Falha no sistema do Detran-RN causa vazamento de dados de 70 milhões de brasileiros.** 2019. Disponível em: <https://www.infomoney.com.br/minhas-financas/falha-no-sistema-do-detran-rn-causa-vazamento-de-dados-de-70-milhoes-de-brasileiros/>. Acesso em: 08 out. 2019.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

GOVERNO FEDERAL. Relações Exteriores. **Declaração de Osaka dos Líderes do G20**. 2019. Disponível em: <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/20562-declaracao-de-osaka-dos-lideres-do-g20 >. Acesso em: 20 jul. 2019.

HAO, Karen. **This is how AI bias really happens - and why it's so hard to fix.** 2019. MIT Technology Review. Disponível em: <https://www.technologyreview.com/s/612876/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/>. Acesso em: 22 abr. 2019.

HESSE, Konrad. **A Força Normativa da Constituição** *(Die normativa Kraft der Verfassung)*. Porto Alegre: Sergio Antonio Fabris Editor, 1991. Tradução de Gilmar Mendes.

IDENTITY THEFT RESOURCE CENTER. 2017 Annual Data Breach Year-end Review. [S. l.], 2018. Disponível em: <www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf>. Acesso em: 06 jan. 2019.

INTERNATIONAL BUSINESS MACHINES (IBM). **Extracting business value from the 4 V's of big data.** 2018a. Disponível em: <https://www.ibmbigdatahub.com/infographic/extracting-business-value-4-vs-big-data>. Acesso em: 08 jul. 2018.

INTERNATIONAL BUSINESS MACHINES (IBM). **The Four V's of Big Data.** 2018b. Disponível em: <https://ibm.co/18nYiuo>. Acesso em: 08 jul. 2018.

JIMENE, Camilla do Vale. Reflexões sobre privacy by design e privacy by default: da identificação à positivação. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). **Comentários ao GDPR**: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Ed. RT, 2018.

KNIGHT, Will. **The Dark Secret at the Heart of AI.** 2017. MIT Technology Review. Disponível em: <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/>. Acesso em: 04 abr. 2019.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Brasil, 2019. p. 445-463.

KONDER, Carlos Nelson. Vulnerabilidade patrimonial e vulnerabilidade existencial: por um sistema diferenciador. **Revista de Direito do Consumidor**, v. 99, pp. 107, 2015.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private Traits and Attributes Are Predictable from Digital Records of Human Behavior. **Proceedings Of The National Academy Of Sciences**, Berkeley, v. 110, n. 15, p.5802-5805, 09 abr. 2013. Disponível em: <https://www.pnas.org/content/pnas/110/15/5802.full.pdf>. Acesso em: 09 jul. 2019.

LARSON, Christina. **Who needs democracy when you have data?** 2018. MIT Technology Review. Disponível em: <https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/>. Acesso em: 04 mar. 2019.

LEMOS, Ronaldo et al. **As mudanças finais da Lei Geral de Proteção de Dados Pessoais.** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/as-mudancas-finais-da-lei-geral-de-protecao-de-dados-pessoais-10072019>. Acesso em: 10 jul. 2019.

LESSIG, Lawrence. **Code**: version 2.0. Nova York: Basic Books, 2006.

LESSIG, Lawrence. The Architecture of Privacy. **Vanderbilt Entertainment Law And Practice**, Nashville, v. 1, n. 1, p. 56-65, jan. 1999.

LUCA, Cristina de. **Decreto de Bolsonaro aproxima uso de nossos dados a países como China.** 2019. Disponível em: <https://porta23.blogosfera.uol.com.br/2019/10/13/governo-tem-nossos-dados-mas-nao-deve-trata-los-como-se-fosse-o-dono-deles/>. Acesso em: 14 out. 2019.

MACHADO, Joana de Souza; NEGRI, Sergio Marcos Carvalho de Ávila. Direito, dignidade humana e o lugar da justiça: uma análise da utopia realista de Ha- bermas. **Revista Brasileira de Estudos Políticos**, Belo Horizonte, v. 1, n. 103, p.103-203, jul./dez. 2011.

MACHADO, Joana; NEGRI, Sergio. Ensaio sobre a promessa jurídica do esquecimento: uma análise a partir da perspectiva do poder simbólico de Bourdieu. **Revista Brasileira de Políticas Públicas**, v. 7, p. 368-383, 2018.

MACHADO, Leandro; MAGENTA, Matheus. **Governo expôs detalhes da vida de 1,3 mil adolescentes entre mais de 30 mil dependentes químicos por 3 anos.** 2019. Disponível em: <https://g1.globo.com/ciencia-e-saude/noticia/2019/07/02/governo-expos-detalhes-da-vida-de-13-mil-adolescentes-entre-mais-de-30-mil-dependentes-quimicos-por-3-anos.ghtml>. Acesso em: 10 ago. 2019.

MADRIGAL, Alexis C. **Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days.** 2012. The Atlantic. Disponível em: <https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/>. Acesso em: 02 jun. 2019.

MAGRANI, Eduardo. **A Internet das Coisas**. 1. ed. Rio de Janeiro: Editora FGV, 2018. v. 1.

MAGRANI, Eduardo. **Entre dados e robôs:** Ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago, 2019.

MARTINS, Gilberto de Andrade; THEÓPHILO, Carlos Renato. **Metodologia da Investigação Científica para Ciências Sociais Aplicadas**. 3. ed. São Paulo: Atlas, 2016.

MARTINS, Pedro. Categorizando Dados em um Contexto de Big Data: Em defesa de uma abordagem funcional. **XXIII Congresso Ibero-Americano de Direito e Informática**, 2019, no prelo.

McCARTHY, J. **A proposal for the Dartmouth summer research project on Artificial Intelligence**, 1956. Disponível em: <http://raysolomonoff.com/dartmouth/boxa/dart564props.pdf>. Acesso em: 16 jun. 2018.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva Educação, 2014. (Série IDP: linha de pesquisa acadêmica).

MITTELSTADT, Brent Daniel et al. The ethics of algorithms: Mapping the debate. **Big Data & Society**, [s.l.], v. 3, n. 2, pp.1-21, dez. 2016. SAGE Publications.

MONTEIRO, Renato. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**. 2018 Disponível em: <https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>. Acesso em: 04 abr. 2019.

MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada.** 2018. Jota. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>. Acesso em: 09 set. 2018.

MORAES, Maria Celina Bodin de. Ampliando os direitos de personalidade. In: VIEIRA, José Ribas. **20 anos da constituição cidadã de 1988:** efetivação de impasse constitucional. Rio de Janeiro: Forense, 2008. pp. 369-388.

MORAES, Maria Celina Bodin de. **Danos à pessoa humana, uma leitura civil-constitucional dos danos morais**, Rio de Janeiro: Renovar, 2003.

MORAES, Maria Celina Bodin de. **Na medida da Pessoa Humana:** estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010.

MORAES, Maria Celina Bodin de. O conceito de dignidade humana: substrato axiológico e conteúdo normativo. In: SARLET, Ingo Wolfgang. **Constituição, direitos fundamentais e**

Direito Privado. 2. ed. Porto Alegre: Livraria do Advogado, 2006.

MORAES, Maria Celina Bodin de. Por um ensino humanista do direito civil. Rio de Janeiro, a. 1, n. 2. **Civilistica.com**: Revista Eletrônica de Direito Civil, [s. l.], v. 2, n. 1, pp.1-16, dez. 2012. Disponível em: <http://civilistica.com/wp-content/uploads/2015/02/Bodin-de-Moraes-civilistica.com-a.1.n.2.2012.pdf>. Acesso em: 09 set. 2017.

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**, v. 19, p. 159-180, 2018.

MULHOLLAND, Caitlin. O Direito de não saber como decorrência do direito à intimidade – Comentário ao REsp 1.195.995. **Civilistica.com**. Rio de Janeiro, a. 1, n. 1, jul.-set./2012. Disponível em: <http://civilistica.com/direito-de-nao-saber/>. Acesso em: 08 mar. 2019.

NEGRI, Sérgio Marcos Carvalho de Ávila. As razões da pessoa jurídica e a expropriação da subjetividade. **Civilistica.com**. Rio de Janeiro, a. 5, n. 2, 2016. Disponível em: <http://civilistica.com/as- razoes-da-pessoa-juridica/>. Acesso em: 08 set. 2017.

NEGRI, Sergio Marcos Carvalho de Ávila; FERNANDES, Elora Raad; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A Proteção Integral de Crianças e Adolescentes: desafios jurídicos de uma sociedade hiperconectada. In: Fabiana de Menezes Soares; Thaís de Bessa Gontijo de Oliveira; Paula Carolina de Oliveira Azevedo da Mata. (Org.). **Ciência, Tecnologia e Inovação: Políticas & Leis**. 305ed. Florianópolis: Tribo da Ilha, 2019, v. 1, p. 283-304.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. 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**, Goiânia, v. 5, n. 1, p. 63-85, jan./jun. 2019a. Disponível em: <https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf>. Acesso em: 09 out. 2019.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. Variações do direito ao esquecimento no Superior Tribunal de Justiça: um estudo de caso do Recurso Especial n. 1.660.168/RJ. **Revista Brasileira de Direito Civil em Perspectiva**, Goiânia, v. 5, n. 1, p. 59-82, jan./jun. 2019b. Disponível em: <https://indexlaw.org/index.php/direitocivil/article/view/5476/pdf>. Acesso em: 23 out. 2019.

NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

O'NEIL, Cathy. **Weapons of math destruction**: how Big Data increases inequality and threatens democracy. New York: Broadway Books, 2017.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Recommendation of the Council on Artificial Intelligence**. 2019. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 10 jun. 2019.

PARISER, Eli. **O filtro invisível:** o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012. 287 p.

PASCUAL, Manuel G. **Quem vigia os algoritmos para que não sejam racistas ou sexistas?** 2019. Disponível em: <https://brasil.elpais.com/brasil/2019/03/18/tecnologia/1552863873_720561.html>. Acesso em: 12 jun. 2019.

PASQUALE, Frank. **The Black Box Society:** The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015.

PERLINGIERI, Pietro. **La persona e i suoi diritti**. Napoli: Edizioni Scientifiche Italiane, 2005.

PERLINGIERI, Pietro. Normas constitucionais nas relações privadas. **Civilistica.com**. Rio de Janeiro, a. 8, n. 1, 2019. Disponível em: <http://civilistica.com/wp-content/uploads/2019/04/Perlingieri-civilistica.com-a.8.n.1.2019.pdf>. Acesso em: 01 jun. 2019.

PERLINGIERI, Pietro. **O Direito Civil na Legalidade Constitucional**. Rio de Janeiro: Renovar: 2008. Tradução: Maria Cristina De Cicco.

PERLINGIERI, Pietro. **Perfis do direito civil**. 3. Ed., rev. e ampl. Rio de Janeiro: Renovar, 2002. Tradução: Maria Cristina De Cicco.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais:** comentários à Lei n. 13.709/2018. São Paulo: Saraiva Educação, 2018.

PORTUGAL. **Lei da Protecção de Dados Pessoais**. 1998. Disponível em: <https://www.cnpd.pt/bin/legis/nacional/lei_6798.htm>. Acesso em: 09 jul. 2019.

POWLES, Julia; NISSENBAUM, Helen. **The Seductive Diversion of 'Solving' Bias in Artificial Intelligence**. 2018. Disponível em: <https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53>. Acesso em: 05 jun. 2019.

POZZI, Sandro. **EUA multam Facebook em 5 bilhões de dólares por violar privacidade dos usuários.** 2019. El País. Disponível em: <https://brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html>. Acesso em: 07 ago. 2019.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. **Law, Innovation and Technology**, v. 10, n. 1, p. 48-53, 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância.** A privacidade hoje. Rio de Janeiro: Renovar, 2008. Tradução: Danilo Doneda e Luciana Cabral Doneda.

RODOTÀ, Stefano. Entrevista à RTDC. **Revista Trimestral de Direito Civil**, Rio de Janeiro, v. 3, n. 11, jul.-set. 2002, pp. 225–308. Entrevista concedida a Danilo Doneda.

RODOTÀ, Stefano. **Il diritto di avere diritti**. 8. Ed. Bari: Laterza, 2012.

RODOTÀ, Stefano. **Il mondo nella rete**: Quali i diritti, quali i vincoli. Roma: Laterza & Figli – Gruppo Editoriale L'Espresso, 2019.

RODOTÀ, Stefano. **La dignità della persona**. Scuola di Cultura Costituzionale, 14 gennaio 2011. Disponível em: < https://www.unipd.it/scuolacostituzionale/documenti/2011/La%20dignita%20della%20persona%20-%20Rodota.pdf> Acesso em: 10 jun. 2018.

RODOTÀ, Stefano. **La rivoluzione della dignità.** Napoli: La Scuola di Pitagora Editrice, 2013.

RODOTÀ, Stefano. Persona, libertà, tecnologia. **Diritto & Questione Pubbliche**. n. 5, 2005. Disponível em: <http://www.dirittoequestionipubbliche.org/page/2005_n5/mono_S_Rodota.pdf>. Acesso em: 28 jul. 2018.

RODOTÀ, Stefano. Por que é necessária uma Carta de Direitos da Internet?. Trad. Bernardo Diniz Accioli de Vasconcellos e Chiara Spadaccini de Teffé. **Civilistica.com**. Rio de Janeiro, a. 4, n. 2, jul.-dez./2015. Disponível em: <http://civilistica.com/por-que-e-necessaria-uma-carta-de-direitos-da-internet/>. Acesso em: 01 set. 2017.

RODOTÀ, Stefano. Transformações do corpo. **Revista Trimestral de Direito Civil**, v. 19, pp. 91-107, 2004.

ROUVROY, Antoinette. "'Of Data and Men'. Fundamental Rights and Freedoms in a World of Big Data." **Council of Europe, Directorate General of Human Rights and Rule of Law.** vol. T- PD-BUR (2015) 09REV, 2016, p. 1-37.

SALLES, Raquel Bellini de Oliveira. **A cláusula geral de responsabilidade civil objetiva.** Rio de Janeiro: Lumen Juris, 2011. 226 p.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. **Civilistica.com**. Rio de Janeiro, a. 8, n. 1, 2019. Disponível em: <http://civilistica.com/o-consentimento-informado-e-a-protecao/>. Acesso em: 09 abr. 2019.

SARLET, Ingo Wolfgang. Neoconstitucionalismo e influência dos direitos fundamentais no direito privado: algumas notas sobre a evolução brasileira. **Civilistica.com**. Rio de Janeiro, a. 1, n. 1, jul.- set./2012. Disponível em: <http://civilistica.com/neoconstitucionalismo/>. Acesso em: 09 set. 2017.

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

SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil.** 6. Ed. – São Paulo: Atlas, 2015.

SCHREIBER, Anderson. **PEC 17/19: Uma Análise Crítica.** 2019. Disponível em: <http://www.cartaforense.com.br/conteudo/colunas/pec-1719-uma-analise-critica/18345>. Acesso em: 18 jul. 2019.

SCHULMAN, Gabriel. www.privacidade-em-tempos-de-internet.com: o espaço virtual e os

impactos reais à privacidade das pessoas. In TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (coords.). **O direito civil entre o sujeito e a pessoa:** estudos em homenagem ao professor Stefano Rodotà. Belo Horizonte: Fórum, 2016, pp. 330-360.

SCHWAB, Klaus. **A Quarta Revolução Industrial.** São Paulo: Edipro, 2016.

SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, [s.l.], v. 7, n. 4, pp. 233-242, 1 nov. 2017. Oxford University Press (OUP). http://dx.doi.org/10.1093/idpl/ipx022.

SIMITIS, Spiros. Privacy—An Endless Debate? **California Law Review**, Berkeley, v. 98, n. 6, p.1989-2005, dez. 2010.

SOUZA, Carlos Affonso Pereira de. **Por que é um risco um cadastro com rosto, RG e até nosso modo de andar.** 2019a. Disponível em: <https://tecfront.blogosfera.uol.com.br/2019/10/11/governo-cria-base-de-dados-unificada-que-liga-cpf-rosto-e-forma-de-andar/>. Acesso em: 14 out. 2019.

SOUZA, Carlos Affonso Pereira de. Segurança e Sigilo dos Dados Pessoais: primeiras impressões 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, 2019b. pp. 417-441.

SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Direitos do titular de dados pessoais na Lei 13.709/2018: uma abordagem sistemática. 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. pp. 243-286.

STEEL, Emily et al. **How much is your personal data worth?** 2013. Financial Times. Disponível em: <https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz2W6ziE25g>. Acesso em: 09 mar. 2018.

STRUCHINER, Noel; HANNIKAINEN, Ivar. A insustentável leveza do ser: sobre arremesso de anões e o significado do conceito de dignidade da pessoa humana a partir de uma perspectiva experimental. **Civilistica.com**. Rio de Janeiro, a. 5, n. 1, 2016. Disponível em: <http://civilistica.com/a- insustentavel-leveza-do-ser/>. Acesso em: 08 set. 2017.

TAYLOR, Charles. **As fontes do self**: a construção da identidade moderna. 4. ed. São Paulo: Edições Loyola, 2013. Tradução: Adail Ubirajara Sobral e Dinah de Abreu Azevedo.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil Análise a partir do Marco Civil da Internet. **Pensar: Revista de Ciências Jurídicas**, Fortaleza, v. 22, n. 1, p.108-146, jan./ abr. 2017. Disponível em: <https://periodicos.unifor.br/rpen/article/view/6272>. Acesso em: 07 ago. 2017.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. In: **Temas de Direito Civil.** Rio de Janeiro: Renovar, 2004, pp. 23-58.

TEPEDINO, Gustavo. Normas constitucionais e direito civil na construção unitária do ordenamento. In: **Temas de Direito Civil**, t. III, Rio de Janeiro: Renovar, 2009, pp. 03-19.

TEPEDINO, Gustavo. O papel atual da doutrina do direito civil entre o sujeito e a pessoa. In: TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (Coords.). **O direito civil entre o sujeito e a pessoa:** estudos em homenagem ao professor Stefano Rodotá. Belo Horizonte: Fórum, 2016, pp. 17-35.

TEPEDINO, Gustavo; OLIVA, Milena Donato. Personalidade e capacidade na legalidade constitucional. In: **Pessoa e mercado sob a metodologia do direito civil-constitucional.** Santa Cruz do Sul: Essere nel Mondo, vol. 1, 2016, pp. 227-248.

TEPEDINO, Gustavo; TEFFÉ, Chiata 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.** São Paulo: Thomson Reuters Brasil, 2019. p. 287-322.

THE ECONOMIST (Ed.). The world's most valuable resource is no longer oil, but data. **The Economist**. [S.l.]. 6 maio 2017. Disponível em: <https://econ.st/2Gtfztg>. Acesso em: 20 jul. 2019.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Nice, 2000. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/CARTAFUNDAMENTAL.pdf>. Acesso em: 09 out. 2017.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho:** General Regulation Data Protection (Regulamento Geral sobre a Proteção de Dados). Bruxelas, 27 abr. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em: 08 ago. 2018.

UNIÃO EUROPEIA. **Resolução do Parlamento Europeu que contém Recomendações à Comissão Sobre Disposições de Direito Civil Sobre Robótica (2015/2103(INL))**. Estrasburgo, 16 fev. 2017. Disponível em: <http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html?redirect>. Acesso em: 08 abr. 2018.

VENTURA, Felipe. **CPFs de 120 milhões de brasileiros ficaram expostos na internet por meses.** Disponível em: <https://tecnoblog.net/271493/cpf-exposto-internet-servidor-apache/>. Acesso em: 09 jul. 2019.

VERONESE, Alexandre. Os direitos de explicação e oposição frente às decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Brasil, 2019. pp. 385-415.

VIOLA, Mario et al. Entre a privacidade e a liberdade de informação e expressão: existe um direito ao esquecimento no Brasil? In TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (coords.). **O direito civil entre o sujeito e a pessoa:** estudos em homenagem ao professor Stefano Rodotá. Belo Horizonte: Fórum, 2016, pp. 361-380.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, [s.l.], v. 7, n. 2, pp. 76-99, maio 2017. Oxford University Press (OUP). http://dx.doi.org/10.1093/idpl/ipx005.

WARREN, Samuel; BRANDEIS, Louis. **The Right to Privacy.** Harvard Law Review, Boston, v. 4, n. 5, 15 dez. 1890.

ZANATTA, Rafael F.; DONEDA, Danilo. **O que há de novo no debate "credit score" no Brasil?** 2017. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-que-ha-de-novo-no-debate-credit-score-no-brasil-09022017>. Acesso em: 20 nov. 2018.

ZARSKY, Tal Z.. Incompatible: The GDPR in the Age of Big Data. **Selton Hall Law Review**, Nova Jersey, v. 47, p.995-1020, 2017.