PEDRO PERES CAVALCANTE

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS:
Uma análise comparativa dos quadros regulatórios brasileiro e europeu

RECIFE
2018

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO DO RECIFE

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS:
Uma análise comparativa dos quadros regulatórios brasileiro e europeu

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade de Direito do Recife, Centro de Ciências Jurídicas, da Universidade Federal de Pernambuco, como exigência parcial para a obtenção do grau de Bacharel em Direito.

Orientando: Pedro Peres Cavalcante

Orientadora: Profª. Eugênia Cristina Nilsen Ribeiro Barza

RECIFE
2018

AGRADECIMENTOS

A Maria, Sérgio e Tiago, por serem meu chão, o início de tudo, o alicerce mais básico.

A Fernanda, por estar sempre junto, ainda que fisicamente tão distante.

A Camila, pela amizade inestimável, pelas lições compartilhadas e pelo alento da certeza do companheirismo.

A Julia, melhor companhia da juventude irreprimível de Setúbal, por ter aparecido e refrescado os dias.

A professora Eugênia, pela orientação e atenção primorosas.

A Carol, Izídia, Júlio, Marcela, Luana, Paula e Raiana, amigos e companheiros nesta longa jornada, pelos risos, aflições, alegrias e decepções que vivemos juntos. Minha gratidão pela companhia leve e pelas mãos estendidas.

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

Em relação às expressões em língua estrangeira, escolheu-se pela manutenção dos acrônimos originais.

ANDP – Autoridade Nacional de Proteção de Dados

CE – Conselho da Europa

GDPR – General Data Protection Regulation (Regulamento Geral de Proteção de Dados Pessoais)

LGPD – Lei Geral de Proteção de Dados Pessoais

MCI – Marco Civil da Internet

NSA – National Security Agency (Agência de Segurança Nacional)

OCDE - Organização para a Cooperação e Desenvolvimento Econômico

UE - União Europeia

RESUMO

A privacidade comporta diversas interpretações, dependentes das variações provocadas pelo contexto sócio-histórico em que está inserida. Na contemporaneidade, a redefinição da privacidade está estreitamente ligada às novas tecnologias de informação e comunicação, especialmente à Internet. Diante da capacidade sem precedentes de difusão de informações da Internet e a expansão contínua da capacidade de armazenamento informacional, os crescentes tráfegos informacionais concernentes às pessoas impactam diretamente a privacidade, em razão da emergência de situações e problemas inéditos característicos dos contextos digitais. As ameaças à privacidade requerem uma tutela jurídica que seja compatível com os desafios à mostra. É neste sentido que, na era digital, sua proteção está imbricada com a proteção dos chamados dados pessoais, fragmentos informacionais que refletem a identidade das pessoas a que se referem. Esta aproximação confere uma dimensão objetiva à tutela da personalidade humana, revelando-se acertada por uma miríade de razões. Se, por um lado, a proteção aos dados pessoais tem, primevamente, uma forte conexão com a tutela da privacidade, é também verdade que as evoluções neste campo de estudos revelaram sua importância para assegurar outras garantias fundamentais. Big data, inteligência artificial e Internet das Coisas são exemplos de fenômenos atuais que, baseados na coleta e análise intensiva de dados, tensionam a temática da proteção de dados pessoais, pondo em evidência a complexidade da matéria e revelando aspectos novos que ensejam compreensões atualizadas com as constantes evoluções desta seara. A proteção de dados, portanto, revela-se como uma matéria complexa e em constante mudança. Nesta trilha, este trabalho elegeu como objetivo geral a investigação desta complexidade na abordagem regulatória brasileira, representada pela Lei 13.709/18, marco regulatório geral para a proteção de dados pessoais. Como objetivos específicos, têm-se: 1) estudar a relação entre privacidade e dados pessoais; 2) verificar a morfologia das leis de proteção aos dados pessoais e, mais precisamente, a dos quadros regulatórios brasileiro e europeu, representados pela Lei Geral de Proteção de Dados Pessoais e pelo Regulamento Europeu sobre Proteção de Dados Pessoais, o Regulamento (UE) 2016/679; e 3) analisar os principais elementos do emergente sistema brasileiro de proteção aos dados. A metodologia utilizada baseou-se no emprego da pesquisa qualitativa, analítica, realizada por meio do método indutivo, que envolveu análise de legislação e pesquisa doutrinária (revisão bibliográfica). A investigação estabeleceu como ponto de partida a contextualização da privacidade aos tempos atuais. A partir das considerações semânticas feitas sobre a privacidade e a prerrogativa jurídica que lhe é correlata, chegamos à temática da proteção de dados pessoais. Em seguida, estudamos a construção autônoma desta matéria, analisando os elementos típicos dos mecanismos regulatórios legais. Compreendidas estas noções, faz-se uso de uma abordagem comparativa, cotejando-se o quadro regulatório europeu com o brasileiro. Por fim, intenta-se a realização de uma análise prospectiva a respeito do quadro regulatório brasileiro de proteção de dados.

.

PALAVRAS-CHAVE: Privacidade. Proteção de dados pessoais. Dados pessoais. Direito digital. Consentimento. Lei 13.709/2018. Lei Geral de Proteção de Dados Pessoais. Regulamento (UE) 2016/679. LGPD. Regulamento Geral sobre a Proteção de Dados. GDPR. Autoridade Nacional de Proteção de Dados Pessoais.

SUMÁRIO

INTRODUÇÃO.....7
1. PRIVACIDADE E DADOS PESSOAIS.....9
1.1 Privacidade: do que estamos falando? 9
1.2 Construção da identificação do direito à privacidade digital à tutela de dados pessoais.....13
2. REGULANDO A PROTEÇÃO DE DADOS PESSOAIS 23
2.1 A morfologia das leis de proteção de dados pessoais.....23
2.2 O quadro regulatório europeu.....26
2.3 O quadro regulatório brasileiro.....29
2.4 Análise da Lei Geral de Proteção de Dados Pessoais.....36
2.4.1 O conceito de dados pessoais.....36
2.4.2 Dados sensíveis, dados anônimos e anonimizados.....38
2.4.3 Consentimento e autodeterminação informacional.....43
2.5 Vetos à LGPD e a Importância da Autoridade Nacional de Proteção de Dados Pessoais.....48
3. O REGIME BRASILEIRO DE PROTEÇÃO DE DADOS PESSOAIS.....52
3.1 Considerações sobre a Lei Geral de Proteção de Dados Pessoais.....52
3.2 Regulação de risco e corregulação.....53
CONSIDERAÇÕES FINAIS.....57
REFERÊNCIAS.....59

INTRODUÇÃO

É corrente a fala de que a privacidade é um elemento em extinção na vida moderna. Os fenômenos fáticos desencadeados pela Internet e pela era digital são apontados como justificativas para estas declarações, que, com frequência, referenciam obras literárias distópicas - como *1984*, de George Orwell, e *Admirável Mundo Novo*, de Aldous Huxley – e anunciam, de maneira simplista e escatológica, que a privacidade morreu.

De fato, não se pode refutar que o fenômeno da digitalização tem causado desdobramentos que desafiam a proteção da privacidade em múltiplos níveis. Revelações de empreendimentos governamentais na área da vigilância massiva e a divulgação de incidentes de segurança que provocam o vazamento ou utilização indevida de informações pessoais são exemplos de ocorrências graves que contribuíram para a percepção pública de que a privacidade corresponde a um bem deveras fragilizado nos tempos modernos. Ademais, o uso cotidiano das novas tecnologias e suas várias aplicações parece mitigar a proteção da privacidade, que aparenta ter-se tornado uma moeda de troca para a conveniência na vida moderna[1].

Embora estes problemas estejam ligados à privacidade, compreendê-los por meio da semântica da própria privacidade parece ser pouco efetivo, ou ainda, inadequado, dada a vagueza que lhe parece ser intrínseca. Quando se fala em privacidade, apontar uma ocorrência que ocasiona sua violação parece ser mais fácil do que a definir.

Por sua vez, a abordagem dos problemas relacionados à privacidade por meio da proteção de dados pessoais é um recurso útil e prático. De fato, os dados pessoais correspondem a um elemento que confere uma tônica objetiva às discussões sobre privacidade, pois são instrumentos bem-delimitados que compartilham características em comum com o campo semântico da privacidade. A subsunção, porém, não é perfeita: o regime de proteção de dados pessoais não se limita à proteção da privacidade. O estudo dos mecanismos regulatórios da proteção oferecida aos dados pessoais revela uma matéria de alta complexidade, em que se encontram imbricadas, inclusive, outras garantias individuais além do direito à privacidade.

---

1 FRANKEL, Max. Where Did Our 'Inalienable Rights' Go? **The New York Times**, Nova Iorque. 22 jun. 2013. Disponível em: <http://www.nytimes.com/2013/06/23/opinion/sunday/where-did-our-inalienable-rights-go.html?_r=0>. Acesso em: 14/04/2015

Este trabalho dedica-se à investigação do estado da proteção jurídica oferecida à privacidade digital e à proteção dos dados pessoais no contexto brasileiro, analisando-se o quadro regulatório disposto na recém-aprovada Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais. Para o desenvolvimento desta pesquisa, estão incluídos em seu percurso a investigação do estudo da relação entre privacidade e dados pessoais e o estudo da morfologia da tutela e dos mecanismos regulatórios delineados à matéria. Compreendidas estas noções, faz-se uso de uma abordagem comparativa, cotejando-se o Regulamento Europeu sobre Proteção de Dados Pessoais, Regulamento (UE) 2016/679, com as disposições da Lei 13.709/2018. Esta escolha é justificada pela influência exercida pela legislação europeia na edição do marco regulatório brasileiro. O arremate desta investigação se dá com uma avaliação prospectiva a respeito do sistema de proteção de dados pessoais brasileiro.

1. PRIVACIDADE E DADOS PESSOAIS

1.1 Privacidade: do que estamos falando?

A privacidade é um tema frequente nos noticiários atuais. Nos últimos anos, as discussões sobre a temática foram certamente impulsionadas pelo escândalo de vigilância massiva sobre cidadãos e líderes de Estado do mundo inteiro perpetrado pela Agência de Segurança Nacional (NSA) norte-americana, revelado em 2013 pelo ex-agente de segurança governamental Edward Snowden. O episódio, largamente noticiado, promoveu uma guinada nos debates contemporâneos sobre privacidade tanto nas esferas informais como institucionais. As revelações feitas a respeito da NSA constituíram um marco para a popularização de uma nova compreensão pública sobre a privacidade e a necessidade de sua proteção, descortinando ao olho comum a temática da privacidade na era digital. A transposição do valor da privacidade ao contexto digital guarda relação próxima com a proteção de dados pessoais. Para que compreendamos esta proximidade, é necessário que refaçamos o percurso de sua construção, traçando algumas pontuações históricas e epistemológicas acerca da privacidade e do direito da privacidade.

Longe de constituir algo homogêneo, a privacidade é comumente definida de acordo com diferentes conceitos - sempre amplos e abrangentes - a depender do contexto cultural e histórico em que se insere[2]. A noção do que é privado, assim, constitui muito menos uma realidade imanente do que uma construção histórica que espelha uma época. Ainda que se tenha em vista seu caráter mutável e variável, não se torna menos difícil a tarefa de delimitar o que se entende por privacidade. Para Daniel J. Solove, a busca por uma definição tida como tradicional sobre privacidade levou a discussões infindas e infrutíferas. As tentativas de conceituação desenvolvidas para o tema revelam-se ou demasiado amplas ou estreitas demais, o que acaba por impedir que problemas reais ligados à sua violação sejam analisados, prevenidos ou remediados[3].

Danilo Doneda, por sua vez, registra a ausência de um conceito que ancore de maneira firme o que se entende pelo termo, pontuando ser este um problema não restrito

---

2 DONEDA, Danilo Cesar Maganhoto; ALMEIDA, Virgílio Augusto Fernandes de. Privacy Governance in Cyberspace. **IEEE Internet Computing**, [S.l.], v. 19, n. 3, p. 50, maio. 2015. Disponível em: <https://ieeexplore.ieee.org/document/7111890?reload=true>. Acesso em: 28 set. 2018.

3 SOLOVE, Daniel J. I've Got Nothing to Hide and Other Misunderstandings of Privacy. **San Diego Law Review**, San Diego, v. 44, p.759, jan. 2007. Disponível em: <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1159&context=faculty_publications>. acesso em: 28 set. 2018. p. 759

à doutrina brasileira[4]. Nos Estados Unidos, por exemplo, o consolidado termo *privacy* (e a prerrogativa correspondente do *right to privacy*) faz referência a uma variedade de situações que não seriam usualmente atribuídas à temática por um jurista brasileiro (ou outro da tradição do *Civil Law*). Como assevera Doneda, a contraposição entre os sistemas do *Civil Law e do Common Law* não seria suficiente para explicar as diferenças semânticas conferidas ao tema da privacidade, dado que as concepções sobre o *right to privacy* variam consideravelmente mesmo entre os Estados Unidos e o Reino Unido[5]. Como bem pontuado pelo próprio autor:

> Diversos ordenamentos seguiram seus próprios caminhos ao tratar da privacidade, visto que entravam em terreno onde as particularidades de cada sociedade eram determinantes. Daí resultaram diferenças de concepção consideráveis: dentro da etiqueta da privacidade se enfileiraram estruturas voltadas para, por exemplo, garantir a ilicitude da publicação de retratos sem consentimento do retratado; o direito de abortar; a inviolabilidade do domicílio e tantas outras[6].

Se a concepção de uma definição atual ubíqua e plenamente funcional para a privacidade revela-se como tarefa não só árdua como arriscada, o regresso às suas bases históricas pode nos apontar ao fulcro de suas essências. A construção do que se entende pela privacidade hoje se assenta, sobretudo, no trunfo do individualismo consagrado com a ascensão da burguesia, é dizer, na consolidação da distinção entre o componente individual e o social. Contribuíram neste sentido, num primeiro momento, a concepção do Estado-nação, da sociedade civil e das teorias de sua soberania nos séculos XVI e XVII, formando a noção moderna do ente público, e, em segundo lugar, a reação ao absolutismo marcada pela necessidade de uma esfera privada livre do controle deste mesmo ente público, algo experimentado tanto no fim da sociedade feudal, pela emergência da Revolução Industrial[7]. A privacidade torna-se um elemento típico da vida burguesa, marcada por um forte componente individualista[8]. Isto se reflete no elemento da propriedade, tão caro aos ideais liberais relacionados à ascensão da burguesia. Se a disposição das abastadas residências burguesas definia bem o que poderia vir a público e o que deveria ser mantido oculto do olhar externo, as habitações populares de camponeses, operários e classes mais baixas não permitiam o privilégio do resguardo em relação aos

4 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1. Ed. Rio de Janeiro: Renovar, 2006. p. 63
5 Idem. p. 64
6 Idem, ibidem.
7 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1. Ed. Rio de Janeiro: Renovar, 2006. p. 78-9.
8 Idem. p. 79

olhares estranhos, deixando às claras o que se passava em seu interior, e, portanto, privando-lhes de um viver privado[9]. A emergência desta primeva noção liberal acerca da privacidade não dá continuidade a uma tradição anterior, mas, sim, atesta o reconhecimento da individualidade própria da burguesia, que a diferencia do corpo social e é instrumentalizada com um forte componente individualista[10].

Em 1890, Louis Brandeis e Samuel Warren, ex-colegas de classe na Universidade de Harvard, publicam o seminal artigo *The Right to Privacy*, referência indispensável às discussões sobre a temática da privacidade até a presente data. A dupla discorre sobre a ameaça potencial representada à privacidade pelas mudanças tecnológicas da época e como o *Common Law* poderia se desenvolver no sentido de salvaguardar o interesse do que se conhecia à época por "privacidade". Longe de dedicar-se a extensivas considerações conceituais sobre o termo, o artigo define a privacidade retomando a expressão "direito a ser deixado sozinho", balizada pelo juiz Thomas Cooley em 1880 no seu famoso tratado sobre reparação de danos. Neste tratado, o uso da expressão refere-se à ideia de que tentativas de estabelecimento de contato físico ensejam danos que merecem ser reparados; não se intenta de qualquer forma definir o que é privacidade. Não obstante, Brandeis e Warren resgatam a expressão para falar sobre o tema, demonstrando que muitos dos elementos de um direito à privacidade já existiam na lei[11]. Os autores aduzem que o princípio subjacente da privacidade remete ao de "não violar a personalidade", discorrendo que o valor daquela não se assenta na vantagem econômica obtida pela pessoa sobre quem se publica, mas da paz mental ou alívio providos pela ausência de qualquer publicação[12].

A identificação do direito à privacidade como o direito a ser deixado sozinho desenvolvida por Warren e Brandeis contribuiu significativamente para o desenvolvimento das discussões sobre a prerrogativa nos Estados Unidos durante o século XX[13], tendo sido utilizada como parâmetro conceitual pela magistratura norte-americana e sendo largamente citada no meio acadêmico até a presente data. Como pontuado por Daniel Solove, no entanto, esta noção de um direito à privacidade identificado à não interferência na vida alheia é insuficiente:

---

9 PROST, Antoine; VINCENT, Gérard (Org.). **História da vida privada**. 1. Ed. Tradução de Denise Bottmann, Dorothée de Bruchard. São Paulo: Companhia das Letras, 2009. 1 p. v. 5. p. 15

10 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1. Ed. Rio de Janeiro: Renovar, 2006. p. 82

11 Brandeis, L. Warren; S. *apud* SOLOVE, Daniel J. Conceptualizing Privacy. **California Law Review**, California, v. 90, jul. 2002. p. 1100

12 Idem. Ibidem.

13 SOLOVE, Daniel J. Conceptualizing Privacy. California Law Review, v. 90, p. 1100, jul. 2002.

> A formulação da privacidade como o direito a ser deixado a só descreve meramente um atributo da privacidade. Compreender a privacidade como o direito a ser deixado a só falha em oferecer esclarecimentos suficientes acerca de como a privacidade deve ser valorada vis-à-vis outros interesses, como liberdade de expressão, efetiva observância das leis, e outros importantes valores. Ser deixados a sós não nos informa sobre os aspectos em que devemos ser deixados sós[14].

Não obstante as críticas pertinentes a esta concepção restrita do direito à privacidade, a contribuição de Warren e Brandeis para a discussão acerca desta prerrogativa vai muito além de uma formulação conceitual definitiva, sendo importante notar que as considerações feitas partiam de um novo fato social, a emergência de novas tecnologias de informação (no caso, jornal e fotografias) - fenômeno que continua presente na atualidade – e que a conceituação oferecida descortinava uma nova compreensão acerca da privacidade, associando esta à personalidade, em vez do elemento da propriedade[15].

No século XX, assiste-se ao aprofundamento desta noção de privacidade que revolve em torno da personalidade humana, o que, por sua vez, traduz-se em novas concepções jurídicas sobre o direito à privacidade. Isto não significa, contudo, que às novas situações fáticas relacionadas à privacidade corresponde ubiquamente o mesmo tipo de proteção legal nos diferentes ordenamentos jurídicos. Como anteriormente pontuado, definições de privacidade são um produto cultural determinado segundo o contexto sócio-histórico em que se inserem, havendo, deste modo, diferenças na tutela jurídica oferecida por cada ordenamento.

A chegada dos computadores – e, posteriormente, da Internet - revela-se como um importante marco tecnológico responsável pela inauguração do aspecto digital da privacidade, que vai, de maneira paulatina, se descortinando legalmente como a proteção aos dados pessoais. Duas são as questões: como se deu este processo? Como os dados pessoais passaram a constituir o eixo gravitacional da proteção à privacidade no meio digital?

---

14 Tradução nossa de "*The formulation of privacy as the right to be let alone merely describes an attribute of privacy. Understanding privacy as being let alone fails to provide much guidance about how privacy should be valued vis-à-vis other interests, such as free speech, effective law enforcement, and other important values. Being let alone does not inform us about the matters in which we should be let alone".* SOLOVE, Daniel J. Conceptualizing Privacy. **California Law Review**, California, v. 90, p. 1101, jul. 2002.

15 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1. Ed. Rio de Janeiro: Renovar, 2006. p. 85

1.2 Construção da identificação do direito à privacidade digital à tutela de dados pessoais

Se a telefonia e a radiodifusão já haviam impactado significativamente as interações comunicativas nas primeiras décadas do século passado, o período pós-guerra foi marcado por uma profunda transformação na abrangência e intensidade dos fluxos de telecomunicações[16]. Num ritmo praticamente exponencial, o restante do século XX assistiu à contínua sucessão de inovações técnicas que impactaram e reconfiguraram a organização humana em múltiplos níveis. A informação passou a ser transmitida através de meios cada vez mais eficazes – o aprimoramento da tecnologia a cabo, a transmissão via satélite, a utilização da fibra ótica em cabos transatlânticos –, difundida em mais meios de comunicação – a televisão, o telex, a telefonia móvel –, e, também, armazenada em instrumentos cada vez mais potentes - os computadores. Na década de 1990, o acesso à Internet, restrito basicamente a algumas universidades nos anos 1980, teve seu acesso ampliado ao grande público, o que não apenas energizou intensivamente os processos de globalização, como acionou um movimento sem precedentes de impacto nos diversos aspectos da vida humana, cujos efeitos ainda não são de todo conhecidos.

À incessante sucessão de inovações tecnológicas associa-se um quadro evidente de mudanças econômicas experimentado pelos países industrializados. Com a instalação da crise do modelo fordista a partir da década de 1970, torna-se evidente a necessidade de reestruturação do capital. Para instalação dessa reestruturação, Manuel Castells sublinha a importância desempenhada pela revolução técnica-informacional, que, aliada à transformação organizacional pautada na flexibilidade e na adaptabilidade, foi absolutamente crucial para garantir a velocidade e a eficiência da reestruturação[17] .

Delineia-se, assim, uma nova etapa do capitalismo, marcada pela ênfase no processamento de informações. Castells denomina este novo modelo econômico de informacionalista, caracterizando-o pela "ação do conhecimento sobre os próprios conhecimentos como principal fonte de produtividade"[18]. Embora todo modo de desenvolvimento se baseie no domínio de algum tipo de conhecimento e no processamento de informação, o modelo econômico informacionalista distingue-se a partir da peculiaridade de que seu escopo corresponde ao tratamento do conhecimento e da informação numa

16 GIDDDENS, Anthony. **Sociologia**. 4. ed. Tradução: Sandra Regina Netz. Porto Alegre: Artmed, 2005. p. 61.

17 CASTELLS, Manuel. **Sociedade em Rede**: **A era da informação : economia, sociedade e cultura**; v. 1. 6. ed. Tradução de Roneide Venancio Majer. São Paulo: Paz e Terra, 1999. 1 p. 55

18 Idem. p. 53-4.

perspectiva autorreferente: o processamento da informação está focalizado na melhoria da própria tecnologia que processa a informação[19].

Neste sentido, Colin J. Bennett coloca que a informação se tornou um recurso que rapidamente se tornou mais fácil de coletar, armazenar, recuperar e comunicar; da mesma forma como o aço e os combustíveis fósseis foram indispensáveis à transição entre os modelos de sociedade agrícola e industrial, a informação é algo fulcral na passagem para o pós-industrialismo[20]. É neste contexto que emerge a sociedade de informação, novo arranjo socioeconômico em que a informação e o conhecimento são recursos-chaves.

É notório que a informação, elemento de natureza abstrata e imaterial, tenha passado a ocupar tamanha centralidade nos processos de organização humana. Como pontua Norbert Wiener, "informação é informação, não é nem matéria, nem energia"[21]. Ao contrário de substâncias materiais, a informação não existe de maneira significativa sem um sujeito cognoscente capaz de apreendê-la: sem o indivíduo que dela toma conhecimento, suas manifestações não passam de signos desprovidos de sentido[22]. A informação não se sujeita às leis físicas de conservação, e, ao contrário de tecnologias pretéritas, as tecnologias de informação, como reprografia, computação e telecomunicações, multiplicam o poder intelectual, em vez do poder físico. A informação pode transformar-se num recurso de poder, econômico ou político, para quem detém acesso a ela, desde que este acesso não seja possível a um grande número de indivíduos[23]

Cumpre aqui pontuar algumas considerações acerca dos termos informação e dados, tão frequentemente sobrepostos. Ambos denotam a representação de um fato, refletindo um determinado aspecto da realidade. Não obstante, cada um carrega um peso próprio[24]. Dados representam uma noção mais primitiva e fragmentada da informação, à semelhança de uma informação em estado potencial. A informação, por sua vez, encerra uma representação mais elaborada da realidade, situada já no limiar da cognição. A informação pressupõe uma fase inicial de depuração de seu conteúdo, de modo a reduzir o

19 Idem. p. 54

20 BENNETT, Colin J. **Regulating privacy: data protection and public policy in Europe and the United States**. 1. ed. Nova Iorque: Cornell University Press, 1992. 15 p. 15

21 Tradução nossa. "*Information is information not matter or energy*". In WIENER, Norbert, 1961. *apud* DONEDA, Danilo Cesar Maganhoto. Op. cit. 2010. p. 17.

22 SIEGHART, Paul. Computers, information, privacy and the law. Journal of the Royal Society of Arts, v. 125, n. 5252, p. 458, jul. 1977.

23 Idem. p. 457

24 DONEDA, Danilo Cesar Maganhoto. **A proteção de dados pessoais nas relações de consumo: para além das informações creditícias**. Brasília: Secretaria de direito econômico / Departamento de proteção e defesa do consumidor, 2010. p. 19

estado de incerteza sobre aquilo que retrata[25]. A este trabalho interessa a informação pessoal, aquela que mantém uma ligação concreta com um indivíduo, dizendo-lhe respeito:

> O vínculo da informação pessoal com o seu titular deve ser de tal natureza a revelar diretamente algo concreto sobre esta pessoa. Assim, a informação pessoal refere-se às suas características ou ações, atribuíveis à pessoa em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então informações diretamente provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como opiniões que manifesta, e tantas outras[26].

O vínculo direto mantido com a pessoa significa que a informação pessoal reflete emanações imediatas da própria personalidade. A informação pessoal aqui mencionada não corresponde, por exemplo, às opiniões emitidas por outrem acerca de um indivíduo, tampouco à produção intelectual considerada em si deste indivíduo (ainda que sua autoria o seja)[27]. É justamente este elo direto mantido entre a informação pessoal e a pessoa humana que atrai para a matéria a tutela da personalidade, e, por consequência, os próprios direitos da personalidade[28]. No âmbito da personalidade, há uma evidente convergência entre as noções de dado e informação. Uma das primeiras – como também mais influentes - definições oferecidas ao termo dado pessoal é hábil a demonstrar como os termos se imbricam[29]. Há decerto uma confusão no emprego dos termos. Na medida em que o fenômeno computacional se reproduz, o termo correntemente utilizado passa a ser o de dado pessoal, mais apropriado à uma lógica de armazenamento organizado da informação - como trataremos a seguir.

Como visto, na era do informacionalismo, a informação, capaz de transmitir conhecimento, exsurge como recurso econômico fulcral. No que se refere à esfera da individualidade, este fenômeno incide, inicialmente, a partir da coleta de informações sobre as pessoas. Com a computadorização presenciada a partir da década de 1960, torna-se continuamente mais prático o armazenamento de informações pessoais, o que, num primeiro momento, é verificado no âmbito governamental. Stefano Rodotà pontua irretoca-

25 Idem. Ibidem.
26 Idem. p. 20
27 Idem. p. 21
28 Idem. Ibidem.
29 Nas Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, desenvolvidas pela Organização para a Cooperação e Desenvolvimento Econômico (OECD) em 1980, tem-se que: *"'*dado pessoal' significa ***qualquer informação*** relacionada com um indivíduo identificado ou identificável (sujeito dos dados)". Grifos nossos.

velmente ainda em 1973: "a novidade fundamental introduzida pelos computadores é a transformação de informação dispersa em informação organizada"[30].

Embora registros sobre informações pessoais estejam presentes há séculos em diferentes sociedades, apenas em tempos recentes vieram estes a obter contornos suficientemente relevantes à geração de controvérsias. Daniel J. Solove pontua que os avanços técnicos foram essenciais ao desenvolvimento da capacidade governamental de recenseamento nos Estados Unidos na virada entre os séculos XIX e XX[31]. Em 1890, o então funcionário do sistema censitário Herman Hollerite desenvolveu um sistema de cartões perfurados que se tornou responsável por reduzir bruscamente o tempo para contagem e organização das informações coletadas. Hollerite deixaria o funcionalismo público para fundar sua própria companhia de confecção de cartões perfuráveis, a qual, através de sucessivas fusões, viria a tornar-se a IBM (Internet Business Machines), empresa pioneira no ramo da computação. A prosperidade inicial da companhia deu-se, em grande parte, devido à necessidade governamental de coleta informacional, na medida em que agências governamentais passam a computadorizar seus registros. Os identificadores numéricos individuais ligados ao Sistema de Seguridade Social norte-americano, chamados de Números de Seguridade Social, passam a deter relevante papel nas bases informatizadas, de modo que, ainda na década de 1970, já figuravam como um relevante recurso para identificação de pessoas tanto por agências governamentais como pelo setor privado[3233]. Assiste-se, assim, aos progressivos avanços na capacidade de coleta, armazenamento e sistematização das mais variadas informações acerca de indivíduos por agentes externos – entes governamentais e privados – a fim de perseguir fins específicos diversos; no caso governamental, pode-se citar a promoção de políticas públicas, já na esfera privada, o aumento na capacidade de vendas com o *marketing* direcionado. Danilo Doneda aponta que o diferencial promovido pela informatização no tratamento de dados pessoais tem um caráter duplo: é quantitativo, na medida em que mais dados são processados em menos tempo, e qualitativo, em função da aplicação de técnicas sofisticadas ao processamento de maneira a obter resultados mais valiosos[34].

30 RODOTÀ, S., 1999. *apud* DONEDA, Danilo Cesar Maganhoto. Op. Cit. 2010. p. 22

31 SOLOVE, Daniel. **The digital person : technology and privacy in the information age**: : technology and privacy in the information age. 2. ed. Nova Iorque: New York University Press, 2006. p. 14-5.

32 SOLOVE, Daniel. **The digital person : technology and privacy in the information age**: : technology and privacy in the information age. 2. ed. Nova Iorque: New York University Press, 2006. p. 14-5.

33 Relevante o destaque de que até hoje identificadores numéricos individuais ligados a instituições governamentais detêm um importante papel, mesmo com a ascensão de tecnologias como a biometria. No Brasil, o CPF (Cadastro de Pessoas Físicas) é um dos identificadores numéricos institucionais mais relevantes.

34 DONEDA, Danilo Cesar Maganhoto. Op. cit. 2010. p.31

A ascensão desta nova conjuntura informacional provocada pela informática promove implicações no campo da privacidade, atraindo a atenção de acadêmicos, filósofos e do público em geral para o tema. A relação entre informações pessoais e privacidade pode ser eficientemente equacionada da seguinte forma: quanto maior o grau de privacidade, menor a difusão de informações, e vice-versa[35]. Ainda que a fórmula seja redutora da complexidade fática, serve como um bom ponto de partida para que se compreenda como a proteção de informações pessoais passou a ser abarcada pelos ordenamentos jurídicos: como pressuposto da tutela do direito à privacidade[36].

Em 1973, o antigo Departamento de Saúde, Educação e Bem-Estar do governo estadunidense registra as preocupações crescentes tocantes à privacidade no contexto de insurgência de computadores e bancos de dados:

> Houve um tempo em que as informações sobre um indivíduo tendiam a ser compartilhadas em contatos cara a cara, envolvendo confiança pessoal e uma certa simetria, ou equilíbrio, entre o emissor e o receptor. Hoje em dia, um indivíduo vê-se cada vez mais obrigado a compartilhar informações sobre si mesmo com um grande número de instituições sem rosto, para que estas sejam manuseadas e utilizadas por estranhos – desconhecidos, não vistos, e, frequentemente, não-responsivos. Por vezes o indivíduo sequer sabe que uma organização mantém um registro sobre ele. Com frequência ele não chega a vê-lo, e, muito menos, a contestar a precisão deste registro e sua disseminação ou a obstar seu uso por outros[37].

Os pontos levantados neste relatório do início da década de 1970 se fazem presentes até os tempos atuais na medida em que continuam a refletir as preocupações frente à obtenção do que hoje denominamos dados pessoais – ainda que, como nunca antes, ressalve-se, haja avanços legais no tratamento da matéria. A organização da informação introduzida pelos computadores engendra o desenvolvimento de bancos de dados, bases informacionais sistematizadas capazes de eficientemente classificar e organizar informações segundo uma lógica de natureza geralmente utilitarista, isto é, a fim de obter o

---

35 DONEDA, Danilo Cesar Maganhoto. **A proteção de dados pessoais nas relações de consumo: para além das informações creditícias**. Brasília: Secretaria de direito econômico / Departamento de proteção e defesa do consumidor, 2010. p. 24

36 Idem. Ibidem.

37 Tradução nossa: "*There was a time when information about an individual tended to be elicited in face-to-face contacts involving personal trust and a certain symmetry, or balance, between giver and receiver. Nowadays, an individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers —unknown, unseen, and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others"*. Estados Unidos. Departamento de Saúde, Educação e Bem-Estar, 1973. *apud* SOLOVE, Daniel. **The digital person : technology and privacy in the information age**: : technology and privacy in the information age. 2. ed. Nova Iorque: New York University Press, 2006. p. 14-5 1 p. 15

máximo proveito a partir do conjunto informacional de que se dispõe[38]. Como pontuado pelo relatório do então Departamento de Saúde, Educação e Bem-Estar estadunidense, um indivíduo torna-se obrigado a partilhar com um número cada vez maior de instituições aparentemente "despersonalizadas" informações de cunho pessoal, as quais são tratadas e administradas por terceiros desconhecidos. Estes novos fatos atraem a guarida legal, posto que fazem com que "o estatuto jurídico destes dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo"[39].

Nesta trilha, uma das mais tradicionais noções encampadas sobre a privacidade, a da manutenção de reserva, segredo e sigilo de informações em relação ao olhar externo, vai cedendo espaço a uma nova concepção, cujo principal eixo revolve em torno da necessidade de controle do que é feito com os dados pessoais. Assim, emerge uma dimensão mais objetiva no tocante à privacidade e à sua tutela, a qual se alinha com o recurso externo dos dados pessoais.

Durante as décadas de 1970 e 1980, é possível registrar a aprovação de alguns marcos regulatórios sobre o tema. Atribui-se ao Land de Hesse na Alemanha a primeira lei de proteção de dados (*Hessisches Datenschutzgesetz*), em 1970, e à Suécia, a primeira lei nacional de proteção de dados, em 1973.

Viktor Mayer-Scönberger registra diferenças importantes ao traçar uma linha evolutiva dos marcos regulatórios sobre dados pessoais[40]. Segundo o autor, distinguem-se três gerações de leis de proteção de dados pessoais. A primeira geração, da qual fazem parte os marcos legais supracitados, tem como ponto de partida a ameaça potencialmente gerada pela tecnologia - especificamente, os computadores. Estas leis debruçavam-se sobre um cenário em que grandes centros de processamento de dados concentrariam a coleta e gestão de dados pessoais. Seu principal enfoque referia-se à concessão de autorizações para a criação destes bancos e do controle posterior a ser exercido por órgãos públicos[41]. Deve-se ressaltar que aqui os principais destinatários (quando não os únicos) destas normas eram os entes públicos. Esta primeira geração de leis é marcada por uma forte estruturação tecnicista determinada pela informática, e seu escopo não

38 DONEDA, Danilo Cesar Maganhoto. **A proteção de dados pessoais nas relações de consumo: para além das informações creditícias**. Brasília: Secretaria de direito econômico / Departamento de proteção e defesa do consumidor, 2010. p. 22

39 Idem. p. 23

40 MAYER-SCÖNBERGER, Viktor, 2009. *apud* DONEDA, Danilo Cesar Maganhoto. **A proteção de dados pessoais nas relações de consumo: para além das informações creditícias**. Brasília: Secretaria de direito econômico / Departamento de proteção e defesa do consumidor, 2010. p. 41

41 Idem. Ibidem.

correspondia ainda à proteção ao valor da privacidade, mas à regulação sobre o uso de bancos de dados e as modalidades de tratamento destes dados, não se incluindo o indivíduo detentor dos dados nestes processos[42]. Como de costume no tocante ao tratamento jurídico conferido a fenômenos tecnológicos emergentes, as leis pertences a esta primeira geração experimentaram curto período de relevância, o que se deu, sobretudo, em razão da proliferação dos bancos de dados, minando, assim, a possibilidade de um regime de concessão de autorizações.

A segunda geração de leis de proteção de dados caracteriza-se pelo abandono do enfoque no fenômeno computacional, passando-se a equacionar a privacidade e a proteção de dados na tutela oferecida, identificada como uma liberdade negativa, exercida pelo próprio indivíduo. A esta geração pertencem leis como a lei francesa de proteção de dados, denominada *Informatique et Libertées* (Lei 78-17, de 06 de janeiro de 1978), e a lei austríaca de 18 de outubro de 1978, nº 565/1978 (*Datenschutzgesetz*)[43].

A terceira geração de normas para a proteção de dados pessoais continua a promover a inserção do cidadão na matéria, buscando-se ampliar esta participação além da mera decisão a respeito do compartilhamento ou não de seus dados. Leva-se em conta, por exemplo, o contexto em que seus dados são solicitados, definindo-se meios de proteção para ocasiões em que a liberdade de escolha resta prejudicada por condicionantes específicas, promovendo, assim, o efetivo exercício da autodeterminação informativa. Passa-se a reconhecer a complexidade no que concerne ao tratamento de dados pessoais, de modo que seu caráter plurifásico (posteriormente à coleta, sucedem-se operações como armazenamento, tratamento para usos específicos, transmissão) enseja igualmente a inclusão do indivíduo, ao qual se passa a assegurar certas garantias, como o dever de informação – o dever de ter-lhe informado o que é feito com seus dados[44].

Solidifica-se, assim, a noção de um direito à autodeterminação informativa, segundo a qual o próprio indivíduo possui o direito de controlar a obtenção, titularidade, tratamento e transmissão de dados relativos à sua pessoa[45]. Danilo Doneda reúne outras características comuns a estas leis: • difusão de autoridades autônomas responsáveis pela aplicação efetiva das leis, o que se contrapõe à diminuição do poder de barganha do indivíduo para a autorização ao processamento de seus dados; • paradoxalmente, diminuição do poder de escolha do cidadão no exercício de sua autodeterminação informaci-

42 Idem. Ibidem.
43 Idem. Ibidem.
44 DONEDA, Danilo Cesar Maganhoto. **Op. Cit., 2010**. p. 42
45 Assim define a sentença de 15 de dezembro de 1983 do Tribunal Constitucional Federal alemão *in* DONEDA, Danilo Cesar Maganhoto, Op. Cit., **2010**. p. 43.

onal em relação a certos tipos de dados, em razão destes envolverem exigirem *per se* níveis de proteção de mais alto grau[46]; • surgimento de mecanismos normativos anexos na forma, por exemplo, de normas específicas para certos setores de processamento de dados (área de crédito ao consumo ou de saúde, por exemplo)[47]. A esta geração pertencem mecanismos como as Diretivas da União Europeia, responsáveis por uniformizar entre os países integrantes do bloco a proteção das pessoas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Diretiva 95/46/CE), e ainda, a relação entre o tratamento de dados pessoais, a privacidade e as comunicações eletrônicas (Diretiva 2002/58/CE).

A abertura da Internet ao uso individual e pessoal na década de 1990 potencializa exponencialmente os fluxos de informação e comunicação, aí incluídos os processos referentes ao tratamento de dados pessoais. Uma das mais relevantes mudanças diz respeito à potencialização da coleta e do tratamento de dados efetuados por entes do setor privado.

Com o acesso à Internet, o usuário individual passa a compartilhar dados sobre si próprio para ter acesso a serviços específicos, além de deixar, desapercebidamente, rastros informacionais ao navegar pelo ciberespaço. Os processos referentes a dados também passam a ser caracterizados por um forte componente transnacional – dados pessoais são intercambiados com agentes de diferentes nacionalidades, nem sempre coincidindo o local físico de armazenamento destas informações com a origem do detentor dos dados ou com o local da empresa coletora. A Internet, assim, põe em xeque as noções tradicionais de soberania e jurisdição, já que mitiga fronteiras como nenhuma outra tecnologia.

Neste sentido, o *locus* virtual forjado pela chamada rede das redes introduz novas problemáticas a respeito da tutela da privacidade em sua dimensão de proteção de dados pessoais. Como pontuado na introdução deste trabalho, é usual deparar-se com argumentos de que, em tempos digitais, a privacidade não existe. Contudo, por todo o percurso já demonstrado, a proteção aos dados pessoais subsiste como uma dimensão objetiva e pragmática da proteção à privacidade nos ambientes digitais.

É cabal que o acelerado ritmo dos avanços tecnológicos promove mudanças mais frequentes nos processos humanos de organização. Como nunca antes, a coleta e tratamento de dados figura como um processo inevitável e irrefreável. Dados transfor-

46 São os dados sensíveis (ver 2.4.2)
47 DONEDA, Danilo Cesar Maganhoto, Op. Cit., **2010**. p. 43

maram-se num *commodity* essencial para a economia digital, engendrando novas possibilidades de negócios. Tendo-se em conta que os dados pessoais constituem unidades segmentadas que revelam aspectos da vida e da identidade dos indivíduos a que se referem, torna-se facilmente compreensível o interesse no acesso a esses fragmentos identitários. A mudança qualitativa no processamento de dados mencionada anteriormente experimentou (e continua a experimentar) novas evoluções com o desenvolvimento da Internet e a progressividade das evoluções tecnológicas. Ela é viabilizada devido ao uso de novos métodos, algoritmos e técnicas capazes de gerar análises detalhadas a respeito de um indivíduo ou coletividade a partir de dados pessoais[48].

O *profiling*, ou perfilização[49], por exemplo, é uma técnica que se baseia no tratamento de dados para a elaboração de perfis de comportamento de uma pessoa com base nos dados disponibilizados por ela ou recolhidos por algum meio[50]. Através do emprego de métodos estatísticos e técnicas de inteligência artificial, os dados passam por um tratamento que formula uma "meta-informação", que sintetiza os hábitos, preferências e outros vários registros sobre a vida de uma pessoa[51]. A técnica do *profiling*, portanto, pode auxiliar na predição mais acertada de comportamentos, uma vez que antevê tendências com base no histórico comportamental. Suas aplicações são variadas, como expõe Danilo Doneda:

> A técnica pode ter várias aplicações desde, por exemplo, o controle de entrada de pessoas em um determinado país pela alfândega, que selecionaria para um exame acurado as pessoas às quais se atribuísse maior possibilidade de realizar atos contra o interesse nacional; bem como uma finalidade privada, como o envio seletivo de mensagens publicitárias de um produto apenas para seus potenciais compradores (possibilitando, portanto, a publicidade comportamental),dentre inumeráveis outras.[52]

A mineração de dados (ou *data mining)*, por sua vez, é uma técnica caracterizada pelo enfoque em vastas quantidades de dados, que são extensivamente varridas e mineradas a fim da depreensão de informações relevantes. O *data mining* debruça-se sobre quantidades extensas de dados em busca do estabelecimento de "correlações, recorrências, formas, tendências e padrões significativos com o auxílio de instrumentos estatísti-

48 DONEDA, Danilo Cesar Maganhoto, Op. Cit., **2010**. p. 32
49 Trata-se de neologismo.
50 DONEDA, Danilo Cesar Maganhoto, Op. Cit., **2010**. p. 42
51 DONEDA, Danilo Cesar Maganhoto, Op. Cit., 2010. p. 32
52 Idem. Ibidem.

cos e matemáticos"[53]. Esta técnica está associada ao fenômeno do acúmulo de quantidades massivas de dados, o chamado *big data*. Com o aumento da capacidade de armazenamento, tornou-se viável o acúmulo de grandes quantidades de dados, inclusive aqueles que, numa análise prévia, não apresentariam qualquer tipo de relevância. O modelo de negócios baseado no *big data* incentiva a captura e armazenamento de qualquer dado, na medida em que reter informação tornou-se mais barato do que eliminá-la[54].

Registra-se que, hoje, 90% dos dados no mundo foram criados nos últimos dois anos, e que, a cada dois dias, cria-se a mesma quantidade de dados gerada do início dos tempos até o ano de 2013[55]. Com a Internet, a obtenção de dados pessoais se espraia pelas mais diferentes ações do cotidiano: a navegação pela *web*, a utilização de aplicativos nos celulares, o uso das redes sociais, os dispositivos inteligentes que passam despercebidos (a chamada Internet das Coisas). Um grande número de ações e escolhas nos contextos digitais são geradores de dados, que podem ser processados para as mais diversas aplicações. Os propósitos para os quais são utilizados os dados pessoais não podem servir à caracterização do tratamento de dados como bom ou ruim: como com toda tecnologia, é importante a diferenciação entre as técnicas e os usos que delas são feitos. Não se pode interpretar o fenômeno da utilização de dados pessoais – e, portanto, o de sua proteção – de maneira simplista, dada sua patente complexidade.

Uma abordagem regulatória bem-sucedida das novas situações ligadas a dados pessoais exige a inclusão de ferramentas inovadoras para administrar o uso de dados pessoais e garantir o efetivo exercício da autonomia informacional por parte dos cidadãos[56].

---

53 DONEDA, Danilo Cesar Maganhoto, Op. Cit., 2010. p. 36

54 MAYER-SCÖNBERGER, Viktor, 2009. *apud* BENNETT, Colin; RAAB, Charles D. **Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective**. 2018. p. 10 Disponível em: <https://ssrn.com/abstract=2972086> Acesso em: 20/10/2018

55 CitiGroup, 2017, p. 4. *apud* PRIVACY INTERNATIONAL. **The Keys to Data Protection:** a guide for policy engagement on data protection. [S.l.: s.n.], 2018. Disponível em: < https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf> Acesso em: 18/10/18

56 DONEDA, Danilo Cesar Maganhoto; ALMEIDA, Virgílio Augusto Fernandes de. Op. cit. p. 52

2. REGULANDO A PROTEÇÃO DE DADOS PESSOAIS

2.1 A morfologia das leis de proteção de dados pessoais

Como visto, ao lidarem com um objeto de tutela externo à subjetividade individual, os dados pessoais oferecem uma abordagem pragmática à questão da privacidade. Os dados são rastros informacionais refletores da identidade de determinada pessoa; tutelá-los, portanto, implica proteger também a própria personalidade humana. Seu trunfo como meio de tutela da privacidade em tempos atuais dá-se justamente por esta linha objetiva de abordagem.

É indispensável pontuar, contudo, que este reconhecimento geral da relevância da proteção de dados pessoais para tutelar a privacidade em tempos digitais não implica a adoção de um tratamento legal necessariamente uniforme à questão. Colin Bennett observa que fatores como o componente determinista do ponto de vista tecnológico – padrões técnicos adotados por diferentes países tendem a ser semelhantes –, a necessidade de desenvolvimento de padrões e a interoperabilidade para os fluxos internacionais de dados geraram uma demanda por leis que confluíssem quanto ao seu núcleo estrutural, sua principiologia e suas ferramentas de aplicação[57].

Assim, embora de um lado seja possível atestar um movimento de convergência entre as diferentes leis nacionais sobre a matéria - verificável, por exemplo, na adoção de uma mesma principiologia ou no estabelecimento de direitos para o titular dos dados -, ao serem adicionados à equação da proteção legal variantes como a implementação de tecnologias, a adoção de boas práticas pela indústria e a atuação de autoridades nacionais de proteção de dados, é possível inferir que sistemas de proteção bastante distintos podem emergir ainda que com legislações semelhantes[58].

Como usualmente se verifica em matérias referentes à Internet, diferentes atores interessam-se pela regulação da proteção de dados pessoais a partir de pontos de vista distintos. Entre eles, pode-se simplificadamente elencar os governos, interessados em ter acesso a dados para desenvolvimento precípuo de políticas públicas; as empresas privadas, desejosas da exploração de potencialidades econômicas nos fluxos de dados, e a sociedade civil organizada, dedicada, substancialmente, à defesa da garantia do direito à privacidade dos indivíduos, evitando o uso abusivo de dados por parte dos dois outros

57 BENNETT, 1992. *apud* DONEDA, Danilo. Op. cit. 2010 p. 51
58 BAMBERGER, K.A; MULLIGAN, D.K, 2013 *in* DONEDA, Danilo Cesar Maganhoto, Op. Cit., 2015. P. 51.

atores. Tendo em vista que a edição de leis específicas constitui o ponto de partida para a efetiva garantia de direitos, a concepção de um marco legal que equilibre os interesses plurais de um elenco diverso de entes implicados na matéria é, certamente, o primeiro passo para a efetiva proteção de dados.

A evidente assimetria entre, de um lado, o usuário individual e, de outro, os entes públicos e as corporações empresariais reforça a necessidade de que os mecanismos legais e regulatórios implicados sejam idôneos a garantir uma proteção robusta aos dados pessoais, permitindo o efetivo exercício da autonomia informacional. Ainda que dotados de limitações, quadros regulatórios para a proteção de dados pessoais figuram como um ponto de partida importante e fundamental para assegurar salvaguardas de cunho legal e regulatório quanto à tutela de dados pessoais[59].

Como anteriormente mencionado, uma série de fatores contribuiu, historicamente, para o desenvolvimento da estrutura e principiologia comumente encontradas nas leis de proteção de dados. A edição de um marco legal deste tipo costuma contar com elementos como o escopo da lei, definições, princípios para proteção de dados, estabelecimento de obrigações para controladores e operadores[60], os direitos dos usuários de dados e fiscalização e implementação das disposições legais[61]. A consolidação de uma base morfológica para essas leis, especialmente no tocante à sua principiologia e taxonomia de termos relevantes, remete, primeiramente, às discussões instigadas pela possível criação de um banco de dados central acerca dos cidadãos norte-americanos na segunda metade da década de 1960[62]. O projeto acabou sendo abandonado, porém as discussões acerca da matéria seguiram em ascensão nos anos seguintes, levando à criação de um comitê consultivo (*Secretary's Advisory Committee on Automated Personal Data Systems*) ligado ao Departamento de Saúde, Educação e Bem-Estar. Como já mencionado anteriormente, em 1973, este comitê publicou o relatório Registros, computadores e os direitos dos cidadãos*,* no qual, inclusive, são delineadas algumas salvaguardas a respeito da proteção de dados:

> - Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo.

59 PRIVACY INTERNATIONAL. Op. Cit. p. 10

60 Controladores e operadores são os agentes responsáveis pelas diversas operações que envolvem dados pessoais. O controlador é responsável pelas decisões que dirigem o tratamento dos dados, ao passo que o operador realiza o tratamento efetivo, conforme as orientações estabelecidas pelo controlador. Ambas as figuras podem ser pessoas naturais ou jurídicas.

61 PRIVACY INTERNATIONAL. Op. Cit. p. 10

62 Tratava-se do *National Data Center*, banco de dados a ser gerenciado pelo governo federal que reuniria registros informacionais de diversas agências federais, condensando informações censitárias, creditícias, trabalhistas, fiscais e previdenciárias.

> - Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada.
> - Deve existir um meio para um indivíduo evitar que a informação a seu respeito colhida para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento.
> - Deve existir um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito.
> - Toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve tomar as devidas precauções para evitar o mau uso destes dados[63]

O conteúdo destes enunciados, apontados pelo Comitê como salvaguardas essenciais à manutenção de qualquer banco sistematizado de dados, viria a ser cristalizado em princípios bem-definidos, denominados de *Fair Information Practice Principles*. Seu delineamento mais nítido se encontra em documentos regionais importantes, como as Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, da Organização para a Cooperação e Desenvolvimento Econômico (OECD), e a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108), da União Europeia. Ambas iniciativas datam do início da década de 1980, tendo passado por modificações recentes em 2013 (OECD) e 2018 (UE). De maneira resumida, é possível arrolar os seguintes princípios:

> 1 - *Princípio da transparência*, pelo qual o tratamento de dados pessoais não pode ser realizado sem o conhecimento do titular dos dados, que deve ser informado especificamente sobre todas as informações relevantes concernentes a este tratamento.
>
> 2 - *Princípio da qualidade*, pelo qual os dados armazenados devem ser fiéis à realidade, atualizados, completos e relevantes, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade.
>
> 3 - *Princípio da finalidade*, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que pode-se, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).
>
> 4 - *Princípio do livre acesso*, pelo qual o indivíduo deve ter acesso às suas informações armazenadas em um banco de dados, podendo obter cópias destes registros; após este acesso e de acordo com o princípio da qualidade, as informações incorretas poderão ser corrigidas, aquelas registradas indevidamente poderão ser canceladas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos.

63 Estados Unidos. Departamento de Saúde, Educação e Bem-Estar, 1973. *apud* DONEDA, Danilo Cesar Maganhoto, Op. Cit., 2010. p. 44-45.

> 5 - *Princípio da segurança física e lógica*, pelo qual os dados devem ser protegidos por meios técnicos e administrativos adequados contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado[64].

A principiologia acima elencada é considerada básica para a generalidade das leis que tratam da proteção de dados pessoais, que, eventualmente, registram novas adições ao rol de princípios adotados, nunca descartando, contudo, o que já se encontra consolidado sobre a matéria.

Em síntese, as leis de proteção de dados baseiam-se em princípios bem-determinados para conferirem direitos aos indivíduos sobre seus próprios dados, sendo estabelecidas obrigações para os entes que efetuarem o processamento desses dados, de tal modo que meios idôneos ao cumprimento da lei e a compensação de danos causados devem ser acionados sempre que estas obrigações e deveres forem descumpridos[65].

Não se pode deixar de sublinhar que a pressão pela utilização do potencial econômico dos dados impele que os quadros regulatórios não se atenham a salvaguardar os direitos dos sujeitos informacionais, intentando-se, especialmente em legislações mais recentes, a conciliação dos mecanismos de proteção com os interesses econômicos e comerciais adjacentes.

2.2 O quadro regulatório europeu

A União Europeia é hoje a maior referência na matéria de proteção de dados, contando com um sistema legal e institucional avançado, cujo desenvolvimento se processou através de décadas. Ainda em 1981, foi aprovada a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108/CE). A Diretiva 95/46/CE, implementada em 1995, dá continuidade ao aprofundamento do tratamento da matéria, estabelecendo diretrizes à proteção de dados entre os Estados-membros. O preâmbulo da Diretiva evidencia que as diretrizes se baseiam na promoção tanto dos direitos fundamentais dos indivíduos, especialmente o da vida privada, quanto do progresso econômico e social, do desenvolvimento do comércio e do bem-estar[66]. Assim, há um evidente propósito conciliatório entre a promoção das garantias individuais e a exploração econômica destes dados, esta última a serviço, in-

64 RODOTÀ, S., 1999, p. 62. *apud* DONEDA, Danilo Cesar Maganhoto. **Op. Cit., 2010**. P.46
65 PRIVACY INTERNATIONAL. Op. Cit. p. 16
66 Considerando nº 02. Da Diretiva 95/46/CE.

clusive, da livre circulação de dados entre os países integrantes do bloco. À Diretiva 95/46/CE, seguiram-se outras diretivas adjacentes, como a Diretiva 2002/58/CE (única ainda em vigor) e a Diretiva 2006/24/CE, concernentes, em síntese, à proteção de dados no contexto das comunicações eletrônicas.

Os primeiros anos do novo milênio assistiram à continuidade da rápida sucessão tecnológica e o deslinde de novos contornos do fenômeno digital. A matéria de dados pessoais é altamente impactada com a difusão do acesso à Internet, a ascensão das redes sociais e a proliferação do uso de dispositivos portáteis *smart*, encabeçada pelos smartphones e pelos *tablets*. Aliadas à defasagem regulatória, as disparidades na execução e aplicação da Diretiva 95/46 engendraram a necessidade da concepção de uma nova regulação no âmbito europeu. O novo quadro regulatório materializa-se com o Regulamento 2016/679 do Parlamento Europeu e do Conselho, o Regulamento Geral de Proteção de Dados (GDPR). Nas considerações iniciais da GDPR, explicita-se que o regulamento deverá promover a equivalência do nível de proteção de dados entre diferentes países-membros com fins de garantir um nível de proteção coerente e elevado das pessoas singulares, bem como a supressão de obstáculos à livre circulação dos dados na União Europeia, ativando seu potencial econômico[67]. Essencialmente, trata-se da mesma tônica impressa à Diretiva 95/46/CE (revogada pela GDPR, inclusive), conciliando-se direitos e interesses econômicos; contudo, a evolução do fenômeno digital faz com que esta retórica conciliatória adquira nova importância.

As diferenças nas conjunturas socioeconômicas em que se inserem a Diretiva 95/46/CE e a GDPR são latentes. A época da Diretiva 95/46/CE é caracterizada por uma Internet primitiva, acessada por meio de computadores pessoais do tipo *desktop*, recém-aberta ao uso individual e cujos potenciais econômicos são ainda primitivamente explorados através de anúncios indistintos. Por sua vez, a GDPR insere-se num mundo em que os dados tornaram-se centrais, sendo gerados a todo vapor por usuários e seus vários dispositivos de modo a atrair o interesse não só de companhias privadas, como de entes governamentais, ambos interessados em coletar o máximo de informações possível.

É no período que separa as duas regulações que a União Europeia pôde consolidar um complexo sistema de proteção. No âmbito nacional, ascende a atuação das autoridades nacionais de proteção de dados pessoais, agentes relevantes para o cumprimento das disposições legais, ao passo que, no âmbito internacional, o grupo de proteção das

67 Considererações nºs 9 e 10 do Regulamento (UE) 2016/679.

pessoas no que diz respeito ao tratamento de dados pessoais (Article 29 Working Party), instituído pelo artigo 29 da Diretiva 95/46/CE, presta assistência e orientação às autoridades, procedendo à análise de temas relevantes através da emissão de pareceres e recomendações. As cortes europeias também exercem um papel relevante neste regime de proteção de dados. Jovan Kurbalija aponta que, desde a compra do Skype pela Microsoft, a União Europeia não possui nenhuma grande empresa da Internet, fraqueza que, paradoxalmente, pode transformar-se em força no âmbito da governança da Internet[68]. Para o autor, esse *status* desobriga a UE de proteção dos interesses econômicos de gigantes digitais, tornando-a mais livre para promover, no geral, interesses públicos relacionados à Internet – tais quais, direitos do usuário, inclusão e neutralidade de rede. Neste sentido, as decisões judiciais europeias envolvendo gigantes da indústria digital, como Google e Facebook, são tidas como parâmetros relevantes para a comunidade internacional, que se inspira nos julgados para abordar questões semelhantes em suas próprias jurisdições[69]. Talvez o exemplo mais marcante seja o reconhecimento do chamado direito ao esquecimento pelo Tribunal de Justiça da União Europeia na disputa judicial entre o Google e a Agência Espanhola de Proteção de Dados (AEPD).

O status de regulamento da GDPR indica a desnecessidade de transposição das disposições normativas para incorporação ao direito nacional de cada Estado-membro, tratando-se, assim, de uma norma interna do bloco. Trata-se de uma regulação robusta, composta por 11 capítulos, 99 artigos e mais de uma centena de considerações preambulares, que aprofunda o arranjo legal estabelecido na Diretiva 95/46/CE. Proceder a uma análise detida do novo quadro regulatório europeu não constitui o escopo deste trabalho, sendo destacadas aqui apenas algumas de suas previsões – mais à frente, quando da análise da lei brasileira, serão feitas algumas considerações comparativas.

O sistema protetivo da GDPR funda-se, de um lado, na principiologia típica da seara da proteção de dados, frisando a promoção das garantias e prerrogativas individuais implicadas na matéria, e, de outro, em determinações específicas, concretas, regras que visam à cobertura das situações fáticas já verificadas, aptas a manter-se a par do desenvolvimento tecnológico[70]. Uma novidade que tem sido bastante discutida é a aplicação de multas, que podem chegar à vultosa soma de € 20.000.000,00 ou, em se tratando

68 KURBALIJA, Jovan. **Uma introdução à governança da internet** [livro eletrônico] / Jovan Kurbalija. Trad. Carolina Carvalho. São Paulo: Comitê Gestor da Internet no Brasil, 2016. p. **223**

69 Idem. Ibidem.

70 GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais *in*: BRANCO, Sérgio; TEFFÉ, Chiara de Teffé (Org.). **Privacidade em perspectivas**. 1. ed. Rio de Janeiro: Lumen Juris, 2018. cap. 6, p. 94.

de uma empresa, até 4 % do seu volume de negócios anual em nível mundial correspondente ao exercício financeiro anterior[71]. O direito ao esquecimento passa a ser previsto legalmente, sendo assegurado ao titular o apagamento de seus dados numa gama de situações. A situação plasmada no caso apreciado pela corte europeia encontra-se disposta no art. 17(1)(*c*), em que é assegurado o apagamento dos dados pessoais pelo titular que proceder ao direito de oposição (previsto no artigo 21), conquanto não haja "interesses legítimos prevalecentes que justifiquem o tratamento".

O grupo de proteção instituído pelo artigo 29 da Diretiva 95/46/CE deixa de existir, sendo instituído, em seu lugar, o Comitê Europeu para a Proteção de Dados (EDPB), um órgão independente e dotado de personalidade jurídica.

Por fim, cumpre ressaltar a existência de um extenso rol de considerações iniciais hábeis a orientar de maneira mais próxima a interpretação da lei.

2.3 O quadro regulatório brasileiro

A proteção de dados pessoais encontra seu primeiro lastro legal na proteção oferecida à privacidade como direito fundamental.

No rol de garantias fundamentais da nossa Constituição Federal, encontram-se deferências à proteção da privacidade nas seguintes disposições:

> Art. 5º
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal[72]

Não obstante a ausência do termo em si, o inciso X acena à proteção da privacidade ao garantir como invioláveis a intimidade e a vida privada, noções adjacentes à de privacidade. O inciso XII, por sua vez, faz expressa menção ao sigilo de "dados", providência inédita à época da promulgação da Carta na legislação brasileira, indicação clara do reconhecimento do fenômeno informático[73]. Também merece destaque o fato de o Brasil ser signatário de tratados internacionais que igualmente reconhecem a vida priva-

71 Artigo 83. Ponto 5. GDPR
72 BRASIL. Constituição Federal (1988).
73 DONEDA, Danilo Cesar Maganhoto. **Op. Cit., 2010**. p. 54

da como inviolável[74]. Em se tratando do reconhecimento da proteção dos dados pessoais como uma garantia fundamental em si, o Brasil é signatário do documento final da XIII *Cumbre Ibero-Americana* de Chefes de Estado e de Governo, conhecido como Declaração de Santa Cruz de La Sierra e firmado em 15 de novembro de 2003, que em seu item 45 dispõe:

> Estamos também conscientes de que a proteção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Proteção de Dados, aberta a todos os países da nossa Comunidade[75].

Na Constituição Federal, encontra-se ainda a previsão do remédio constitucional *habeas data*, garantidor de acesso dos cidadãos a informações que lhe dizem respeito e armazenadas em bancos de dados públicos, bem como à prerrogativa de retificação destes dados[76]. Note-se que a previsão da ação constitucional se estabelece nos moldes gerais da proteção de dados, especialmente no tocante aos princípios da qualidade e do livre acesso, mencionados no tópico 2.1. A título de curiosidade, no direito comparado, a Constituição da Colômbia prevê o habeas *data* inclusive em relação a entidades priva-

74 Neste sentido, tem-se a **Declaração Universal dos Direitos Humanos, de 1948, que, em seu artigo 12, dispõe:** Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques; e o **Pacto Internacional sobre os Direitos Civis e Políticos, de 1966, cujo artigo 17 dispõe:** Ninguém será objeto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques ilegais à sua honra e reputação. Toda a pessoa tem direito a proteção da lei contra essas ingerências ou esses ataques.

75 Declaração de Santa Cruz de La Sierra. XIII CIMEIRA IBERO-AMERICANA DE CHEFES DE ESTADO e DE GOVERNO. Disponível em: < https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf> Acesso em 27/10/18

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

das[77], ao passo que nas constituições de Portugal[78] (1976) e Espanha[79] (1978) encontram-se previsões que abordam questões emergentes da informática de uma maneira mais específica, havendo, no caso da carta fundamental portuguesa, disposições mais robustas da proteção de dados pessoais.

A nível infraconstitucional, é possível encontrar algumas normas setoriais no ordenamento jurídico brasileiro que chegam a abordar a proteção de dados, ainda que não se dediquem exclusivamente a isso. Destacam-se nesse sentido: o Código de Defesa do Consumidor (Lei 8.078/90), ao dispor sobre bancos de dados e cadastros que contêm informações sobre consumidores (arts. 43 e 44); Lei do Cadastro Positivo (Lei n° 12.414/2011), dispondo sobre bancos de dados que reúnam informações sobre adimplemento para formação de histórico de crédito e a Lei de Acesso à Informação Pública (Lei n° 12.527/2011), que, em seu artigo 31, provê diretrizes para o tratamento de informações pessoais pela administração pública. Não obstante a abordagem dessas leis seja restrita a âmbitos específicos, é possível atestar que, assim como o *habeas data* constitucional, essas normas também remetem à principiologia cristalizada no âmbito da proteção de dados pessoais. Na Lei do Cadastro Positivo, por exemplo, é possível identificar, entre outros princípios: o princípio do livre acesso (art. 5º, I, II e III; art. 6º, I, II e III), o princípio da transparência (art. 5º, IV; art. 6º, IV) e o princípio da finalidade (art. 5º, VII)[80].

77 Ver artigo 15 da Constituição da Colômbia.

78 A Constituição da República Portuguesa (1976) dispõe sobre a utilização da informática em seu artigo 35 nos seguintes termos: 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei; 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente; 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei; 5. É proibida a atribuição de um número nacional único aos cidadãos; 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

79 Ver artigos 18 e 105(b) da Constituição Espanhola (1978).

80 Lei 12.414/2011. Art. 5º São direitos do cadastrado: I - obter o cancelamento do cadastro quando solicitado; II - acessar gratuitamente as informações sobre ele existentes no banco de dados, inclusive o seu histórico, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta para informar as informações de adimplemento; III - solicitar impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 7 (sete) dias, sua correção ou cancelamento e comunicação aos bancos de dados com os quais ele compartilhou a informação; IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial; V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento. Art. 6º8p Fi-

Em 23 de abril de 2014, sanciona-se a lei 12.965/2014, o chamado Marco Civil da Internet (MCI), um marco regulatório civil sobre princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Trata-se de um arranjo normativo eminentemente principiológico. O tema da privacidade é abordado pelo MCI na seguinte tríade de aspectos: 1) princípios e direitos do usuário; 2) retenção de logs e 3) acesso e processamento de dados pessoais[81]. [CITATION DON14 \l 1046]. Destaca-se que, no rol de princípios orientadores do uso da Internet, a privacidade e a proteção de dados pessoais são abordados autonomamente:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> [...]
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei[82]

Esta previsão em separado ecoa as disposições da Carta dos Direitos Fundamentais da União Europeia, em que a privacidade e os dados pessoais são previstos como direitos autônomos[83], apesar de suas semelhanças (a privacidade é mais ampla). Esta previsão em separado provê a proteção de dados de uma autonomia dignificante, indicando, teleologicamente, o reconhecimento de sua importância.

Note-se que a menção à proteção de dados pessoais no inciso III do art. 3º vem acompanhada da expressão "na forma da lei", indicando que a regulação propriamente dedicada à proteção de dados deverá ser objeto de outro marco regulatório (uma lei específica), enquanto as determinações do Marco Civil relacionadas à proteção de dados

---

cam os gestores de bancos de dados obrigados, quando solicitados, a fornecer ao cadastrado: I - todas as informações sobre ele constantes de seus arquivos, no momento da solicitação; II - indicação das fontes relativas às informações de que trata o inciso I, incluindo endereço e telefone para contato; III - indicação dos gestores de bancos de dados com os quais as informações foram compartilhadas; IV - indicação de todos os consulentes que tiveram acesso a qualquer informação sobre ele nos 6 (seis) meses anteriores à solicitação; e V - cópia de texto contendo sumário dos seus direitos, definidos em lei ou em normas infralegais pertinentes à sua relação com bancos de dados, bem como a lista dos órgãos governamentais aos quais poderá ele recorrer, caso considere que esses direitos foram infringidos; VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.

81 DONEDA, Danilo Cesar Maganhoto. Privacy and Data Protection in the Marco Civil da Internet. Disponível em: <http://www.privacylatam.com/?p=239> Acesso em 23/06/14

82 BRASIL. Lei 12.965/2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>

83 UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia** (2000/C 364/01). Artigo 7: Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. Artigo 8: 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

consistem em recortes específicos que levam em conta as características da própria Internet[84].

O artigo 7º do MCI arrola entre os direitos do usuário ao acessar a Internet previsões bastante semelhantes àquelas encontradas nos incisos X e XII do artigo 5º da Constituição:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

Como bem pontuado por Danilo Doneda[85], a aparência redundante destes incisos é afastada pela previsão específica do art. 7º, III, concernente à interpretação do judiciário brasileiro em face dos incisos supramencionados da Constituição Federal, segundo a qual não constitui violação o armazenamento indevido de dados, mas apenas sua comunicação. A lei reconhece o paradoxo, estendendo aos dados armazenados o mesmo nível de proteção oferecido aos dados comunicados.

É importante destacar que o caráter eminentemente principiológico do chamado Marco Civil da Internet não é indicativo de previsões legais redundantes em relação às normas já consolidadas no ordenamento jurídico pátrio, em relação, por exemplo, ao reconhecimento de direitos individuais. Quando da cerimônia da sanção do Marco Civil da Internet, a então presidente Dilma Rousseff asseverou que os mesmos direitos que as pessoas possuem *off-line* devem ser garantidos *online*[86], algo repetido pelo Conselho de Direitos Humanos da ONU na Resolução número A/HRC/28/L.27[87], sobre o direito à privacidade na era digital. As diferenças entre o meio real e o meio virtual exigem que as ferramentas utilizadas para garantir direitos e tratar de outras questões no mundo *online* sejam apropriadas à natureza única do meio digital.

A sanção do MCI representou avanços à matéria de proteção de dados pessoais. A aprovação de uma legislação específica, contudo, seguiu sendo necessária, dada a

84 DONEDA, Danilo Cesar Maganhoto. Privacy and Data Protection in the Marco Civil da Internet. Disponível em: <http://www.privacylatam.com/?p=239> Acesso em 23/06/14
85 Idem. Ibidem.
86 NET MUNDIAL - Discurso Dilma Rousseff. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/15102/NET-MUNDIAL---Discurso-Dilma-Rousseff/> Acesso em: 28/10/18
87 CONSELHO DE DIREITOS HUMANOS DA ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Resolução A/HRC/28/L.27, 24/03/2015. <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G15/061/64/PDF/G1506164.pdf?OpenElement>

complexidade da matéria. As discussões para a aprovação de uma regulação autônoma tiveram início em 2010 a partir de proposta do Poder Executivo, havendo uma posterior profusão de iniciativas.

Destacaram-se três iniciativas legislativas autônomas, advindas do Poder Executivo (PLPDP/EX), da Câmara dos Deputados (PLPDP/CAM) e do Senado Federal (PLDPD/SEN). A linha do tempo aqui delineada baseia-se na reconstituição cronológica traçada por Bruno Bioni[88]. A iniciativa do Poder Executivo, concretizada no projeto de lei 5.276/16, remonta ao ano de 2010, com a abertura, pelo Ministério da Justiça, de uma consulta pública sobre um anteprojeto de lei de proteção de dados pessoais. A consulta, realizada entre 2010 e 2011, foi disponibilizada via plataforma digital[89], sendo possível a quaisquer partes interessadas tecer comentários ao anteprojeto de lei.

Em 2012, o então deputado federal Milton Alimonti propôs o PL 4.060/12. As revelações sobre espionagem e vigilância massiva feitas por Edward Snowden em 2013 motivaram o surgimento de três novos projetos: o PL 330/2013, de autoria do senador Antônio Carlos Valadares; o PL 131/2014, uma das proposições feitas pela Comissão de Inquérito Parlamentar da Espionagem quando de seu encerramento; e o PL 181/2014, do Senador Vital do Rêgo. Em janeiro de 2015, foi aberta outra consulta pública pelo Ministério da Justiça sobre a nova minuta do anteprojeto de lei de proteção de dados pessoais[90]. No mesmo ano, a Comissão de Ciência e Tecnologia/CCT do Senado aprovou substitutivo para os PLS 330/2013, 131/014 e 181/2014, que são fundidos num só projeto de lei. Em maio de 2016, às vésperas do afastamento ocasionado pela abertura do processo de impeachment, a presidenta Dilma Rousseff encaminhou ao Congresso Nacional o texto final do APL de proteção de dados pessoais, transformado no PL 5.276/16. O trâmite deu-se em regime de urgência constitucional a pedido da presidenta, o que foi posteriormente retirado a pedido do novo presidente Michel Temer. Em julho daquele ano, o PL 5.276/16 foi apensado ao PL. 4.060/12. Também em 2016, foi instaurada na Câmara dos Deputados a Comissão de Proteção de Dados Pessoais, cuja composição mista caracterizada por partidos de diferentes orientações ideológicas é tida como

88 BIONI, Bruno Ricardo. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados: Próximas semanas serão decisivas e pode não haver melhor momento para que Brasil deixe para trás seu atraso. **JOTA**, [S.l.], 02 jul. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018>. Acesso em: 28 out. 2018.

89 É possível consultar os debates integrantes da primeira consulta por meio do acesso ao link <http://culturadigital.br/dadospessoais/>

90 É possível consultar os debates integrantes da segunda consulta por meio do acesso ao link <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>

fundamental para a posterior aprovação da matéria com unanimidade na Câmara dos Deputados.

Os trabalhos da comissão aprofundaram o conhecimento da matéria na casa legislativa através das discussões fomentadas pela agenda de audiências públicas, seminários e missões internacionais[91]. O roteiro de trabalho da comissão desenrolou-se do final 2016 a meados de 2018.

Em 28 de maio de 2018, é aprovado o requerimento de urgência para apreciação dos PLs sobre proteção de dados. No dia seguinte, o deputado Orlando Silva apresenta substitutivo global aos projetos de lei 5.276/16 e 4.060/12, que é aprovado por unanimidade em plenário. O PLC 53/2018, fusão dos projetos apensados, tramitou, então, para o Senado Federal. O mês de junho assistiu à publicação de diferentes manifestos multissetoriais pela aprovação do projeto. Em rara ocorrência, entidades do setor empresarial, acadêmico e do terceiro setor manifestaram-se conjuntamente[92] a favor da aprovação do PLC 53/2018, em razão da convergência de interesses representada pelo equilíbrio da referida iniciativa. Em 10 de julho de 2018, a lei foi aprovada por unanimidade no Senado Federal, fazendo com que as iniciativas legislativas do Senado Federal supramencionadas perdessem objeto. Em 14 de agosto de 2018, o presidente Michel Temer sancionou a nova lei, identificada sob o nº 13.709/2018, com o veto a alguns de seus dispositivos.

A Lei Geral de Proteção de Dados Pessoais foi resultado de duradouros trâmites legislativos, aos quais contribuíram diversos atores interessados. Assim como em relação ao Marco Civil da Internet, a LGPD também foi marcada por uma discussão multissetorial e pluriparticipativa. A lei estabelece direitos aos titulares dados e obrigações aos agentes de tratamento responsáveis pelo seu processamento, conciliando a garantia de direitos com a indução de novos modelos de negócios baseados em dados. Procedemos à sua análise.

2.4 Análise da Lei Geral de Proteção de Dados Pessoais

91 BIONI, Bruno Ricardo. Op. Cit. 2018.

92 Registram-se aqui três manifestos autônomos: o manifesto da Coalizão Direitos na Rede, disponível em <https://direitosnarede.org.br/c/pela-aprovacao-imediata-do-plc-53-18/>; o Manifesto Pela Aprovação Da Lei De Proteção De Dados Pessoais, disponível em < https://brasscom.org.br/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais/> e a carta em defesa da Autoridade Independente de Proteção de Dados Pessoais, disponível em: <https://docs.google.com/forms/d/e/1FAIpQLSfsw3Lm4UFkGykGCqgqfahQKUEmGXI2FNPvElLnJj_2qvf-vA/viewform>. Todas acessadas em: 04/11/2018

A Lei Geral de Proteção de Dados estrutura um sistema geral de proteção de dados pessoais ao longo de 65 artigos, dos quais nove foram vetados parcial ou integralmente. Destaca-se que, diferentemente do Marco Civil da Internet, a LGPD corresponde a um regulamento geral para proteção de dados pessoais, independentemente destes passarem por fluxos da Internet ou não. Assim, quaisquer estabelecimentos que coletem dados pessoais - como farmácias, locadoras de carro, postos de gasolina – estão submetidos às disposições legais.

A lei segue uma lógica semelhante à GDPR europeia. Estabelecem-se, inicialmente, princípios bem-reconhecidos sobre a matéria, os quais embasam os direitos dos titulares de dados e as diretrizes a serem observadas nas operações que envolvem o tratamento de dados pessoais pelos controladores e operadores (agentes de tratamento). Há regras específicas atribuídas ao tratamento de dados pelo poder público. Preveem-se sanções administrativas e econômicas em face da inobservância das prescrições legais pelos agentes de tratamento. A responsabilização destes, ressalte-se, não se configura a partir de uma lógica de reparação de danos. Há determinações na lei que indicam o alinhamento a uma abordagem regulatória baseada no risco, o que exploraremos no tópico 3.2.

Pelas limitações impostas a este trabalho, decidiu-se pela análise de dois elementos centrais ao estudo da matéria: os conceitos de dados pessoais e consentimento. De todo modo, ressalta-se, desde já, que as considerações sobre estes elementos não pretendem ser exaustivas, servindo como um delineamento panorâmico indispensável à compreensão necessária destas definições. Primeiro, abordamos estes dois conceitos-chave para, em segundo lugar, desenvolvermos algumas considerações a respeito do sistema de proteção como um todo.

2.4.1 O conceito de dados pessoais

Como assinalado no tópico 1.2, o dado denota uma unidade segmentada detentora de certo valor informacional. A classificação de um dado como pessoal indica características atribuídas a um indivíduo, as quais refletem fragmentos de sua própria identidade. Delimitar esta classificação é uma tarefa semântica fundamental a qualquer lei que pretenda regular a proteção de dados pessoais, posto que, a depender dessas demarcações conceituais, pode-se verificar uma maior ou menor amplitude do alcance da

proteção à própria personalidade humana. Neste sentido, as definições de dados pessoais podem ser consideradas expansionistas ou reducionistas[93].

As definições reducionistas encerram um conceito restritivo, segundo o qual um dado é pessoal quando identifica de maneira individualizante uma pessoa. Assim, o dado pessoal refere-se de maneira certeira a uma pessoa específica (identificada), de modo a não haver dúvidas a respeito da relação entre o dado e o indivíduo ao qual se refere[94]. Opera-se uma clara identificação: o dado pessoal reflete a projeção de uma pessoa una e inequívoca[95]. Fala-se, assim, que o dado pessoal se refere a uma pessoa dita "identificada", posto que o dado a identifica de maneira clara. Assim, identificadores numéricos únicos, como o Cadastro de Pessoas Físicas, o Registro Geral ou o número de passaporte seriam, assim, exemplos de dados pessoais, pois identificam inequivocamente um indivíduo.

Em contraponto, a acepção expansionista alarga o conceito de dado pessoal. Segundo seus ditames, para um dado ser caracterizado como tal, não é imprescindível que sua capacidade de identificação de um indivíduo seja plena e inequívoca. Assim, também é considerada dado pessoal a unidade informacional que pode de maneira indireta chegar a identificar uma pessoa[96]. A concepção expansionista, desta forma, engloba tanto o dado que se refere inequivocamente a uma pessoa, como aquele que, de maneira indireta, também serve à identificação de um indivíduo. Nesta trilha, o dado que identifica uma pessoa por vias indiretas refere-se a uma pessoa identificável, pois detém a possibilidade de identificar um indivíduo ao ser, por exemplo, analisado junto a outros dados da mesma pessoa.

Deve-se destacar que a análise da chamada identificabilidade[97] ou o grau de identificação de um indivíduo deve sempre ser feita contextualmente. Afora dados altamente específicos, como os supracitados identificadores numéricos únicos, aferir o potencial de identificação de um dado com base em elementos intrínsecos à sua própria natureza é desaconselhado. O dado sobre o ano de nascimento de uma criança pode ser útil para distingui-la do restante do seu núcleo familiar, porém pode carecer de utilidade

93 BIONI, Bruno Ricardo. **Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil.** [S.l.: s.n.], 2016. p. 21 Disponível em: <https://www.researchgate.net/publication/328266374_Xeque-Mate_o_tripe_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil>. Acesso em: 17 out. 2018.

94 BIONI, Bruno Ricardo. Op. Cit. 2016. p. 16

95 DINNANT, J-M.POULLET, Y.; 2004, p. 29 *apud* BIONI, Bruno Ricardo. Op. cit. 2016 p. 17

96 BIONI, Bruno Ricardo. Op. Cit. 2016. p. 16

97 Trata-se de neologismo. Do inglês *identificability*. que denota a capacidade de proceder a uma identificação.

se analisado para identificar esta criança entre seus colegas de classe na escola, se existirem um grande número de outras crianças com o mesmo ano de nascimento. Da mesma forma, um sobrenome familiar pode ser dotado de um alto grau de identificabilidade num contexto como o ambiente de trabalho, porém perder este potencial individualizante quando utilizado como critério de distinção na análise da população geral, se se tratar de um sobrenome comum[98].

Apesar da proximidade léxica, as acepções expansionista e reducionista operam em vetores opostos na escala de medição do potencial de identificação de um indivíduo por meio de dados pessoais. A Lei Geral de Proteção de Dados Pessoais brasileira adota uma definição expansionista, conceituando o dado pessoal como a "informação relacionada a pessoa natural identificada ou identificável" em seu art. 5º, I[99]. Esta abordagem ampliativa é definitivamente positiva para a tutela oferecida à proteção da privacidade e pode ser encontrada em vários instrumentos tido como exemplares na regulação mundial sobre a matéria[100].

2.4.2 Dados sensíveis, dados anônimos e anonimizados

A *classificação geral* ampliativa ou restritiva acerca de dados pessoais corresponde apenas a um dos pontos na taxonomia sobre o assunto. Na tipologia sobre a matéria, vale a menção aos conceitos de dados sensíveis e dados anônimos. Como anteriormente asseverado, não se subsume ao escopo deste trabalho uma análise exaustiva e detalhada dessas categorias, assim, as considerações aqui feitas dedicam-se apenas a uma breve exposição panorâmica sobre estas categorias de dados.

98 **Data Protection Commission of Ireland.** Anonymisation and pseudonymisation. Disponível em: <https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm>. Acesso em: 22 out. 2018.

99 BRASIL. Lei n. 13.709, de 14 de ago. de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). -. Brasília, p. 01-02, ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 30 out. 2018.

100 Nas Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, da Organização para a Cooperação e Desenvolvimento Econômico (OECD), tem-se que: *"dado pessoal" significa qualquer informação relacionada com um indivíduo identificado ou identificável (sujeito dos dados)* [parte I, ponto 2]. Já na **Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal** (Convenção 108), da União Europeia, encontra-se que *«dados de carácter pessoal» significa qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação («titular dos dados»)* [artigo 2º, alínea a)]. O Regulamento Geral sobre Dados Pessoais da União Europeia (2016/679), acrescenta um rol exemplificativo e alguns esclarecimentos ao definir dado pessoal como "*informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular"* [art. 4º, inciso 1)].

Os dados sensíveis referem-se a informações pessoais que denotam aspectos que exigem um maior nível de proteção em razão dos riscos envolvidos no seu manejo. São aspectos a respeito de um indivíduo que podem ensejar ações discriminatórias, de diferenciação negativa, se indevidamente processadas; daí porque se diz serem dados sensíveis. Entre os dados deste tipo, pode-se mencionar aqueles que revelam filiações políticas, crenças religiosas, histórico e vida sexual, origem racial ou étnica, aspectos genéticos ou biométricos relacionados a uma pessoa individual. Estes dados experimentam maior proteção pelos quadros regulatórios, evidenciada a partir da exigência de mais camadas de seguranças envolvendo seu tratamento, e, também, do estabelecimento de uma base legal diferenciada, evidenciada, por exemplo, pela exigência expressa de consentimento específico e destacado do titular com o tratamento desses dados para atendimento de finalidades específicas[101].

A elaboração desta categoria distinta, registra Danilo Doneda, não foi concebida sem críticas: argumenta-se que é impossível definir de maneira antecipada os efeitos a serem gerados pelo tratamento de uma informação, seja ela qual for[102]. Nesta trilha, mesmo dados que não se enquadram na classificação de dados sensíveis podem ensejar práticas discriminatórias ao serem tratados. Não obstante o confronto com estas pontuações, a categoria de dados sensíveis e o tratamento específico que lhes é correspondente continua prevalecente em diferentes legislações. A adoção desta classificação distintiva não se traduz na subestimação dos potenciais lesivos do manejo indevido de dados "comuns", mas, sim, no reconhecimento dos maiores riscos que recobrem os dados sensíveis, promovendo-se, assim, o princípio da igualdade material[103].

A LGPD dispõe sobre o tratamento de dados sensíveis em seu artigo 11, colocando como regra principal que apenas o consentimento de forma específica e destacada do titular de dados para finalidades específicas pode autorizar o tratamento de dados sensíveis. São, também, previstas, outras hipóteses que autorizam o tratamento destes dados sem o consentimento do titular, entre as quais se incluem o cumprimento de obrigação legal ou regulatória pelo controlador; tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; realização de estudos por órgão de pesquisa, garantida, sempre que possí-

101 MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. **JOTA**, [S.L.], 14 jul. 2018. Disponível em: < https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>. Acesso em 28 out. 2018

102 DONEDA, Danilo Cesar Maganhoto. **Op. Cit., 2010**. p. 26

103 RODOTÀ, S., 1995, p. 85. *apud* DONEDA, D. C. 2010 Op. Cit., 2010. p. 26

vel, a anonimização dos dados pessoais sensíveis; proteção da vida ou da incolumidade física do titular ou de terceiro. Destaca-se ainda a determinação/ do § 4º, do art. 11, que veda a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde que vise à obtenção de vantagem econômica, salvo se trate de caso de portabilidade de dados consentido pelo titular.

A GDPR aborda o tratamento de dados sensíveis de maneira diferente, proibindo, de maneira expressa, em seu artigo 9(1), o tratamento de "categorias especiais de dados pessoais", é dizer, dados pessoais sensíveis. Assim como na LGPD, são previstas exceções, sendo a primeira delas o consentimento explícito do titular para uma ou mais finalidades específicas, nos termos do artigo 9(2)(*a*)[104]. Comparando as duas legislações, vê-se que é possível estabelecer alguns paralelos entre as ressalvas previstas – há, por exemplo, uma preocupação em comum com os aspectos da saúde e da proteção da vida –, porém as previsões da GDPR não são iguais às da lei brasileira, sendo também bem mais extensas que os enunciados enxutos da LGPD.

Outra distinção importante feita no âmbito dos dados pessoais diz respeito aos dados anônimos e anonimizados. O dado anônimo é caracterizado pela representação contrária ao conceito de dado pessoal: é aquele dado inapto à identificação de um indivíduo. É patente, portanto, que os dados anônimos não são objeto de proteção pelas leis. Os dados anonimizados, por sua vez, dizem respeito a dados que, por meio de técnicas de anonimização, tiveram seu potencial de identificação mitigado. Dilapida-se o vínculo que o dado mantém com seu titular através de técnicas como supressão, generalização, randomização e pseudoanonimização[105].

Há variados motivos para a anonimização de dados; a anonimização pode integrar uma estratégia de minimização de riscos ao serem transmitidos dados entre operadores e controladores, ou ainda, como parte de um protocolo de minimização de dados (*data minimisation*) voltado à própria minimização de riscos na ocorrência de um vazamento desses dados[106]. Um ponto fulcral à tarefa de anonimização diz respeito à inviabi-

104 Artigo 9(1) e (2) GDPR: 1. 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. 2. O disposto no nº 1 não se aplica se se verificar um dos seguintes casos: *a)* Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.o 1 não pode ser anulada pelo titular dos dados;

105 BIONI, Bruno Ricardo. Op. Cit. 2016. p. 25

106 Data Protection Comission of Ireland. **Anonymisation and pseudonymisation**. Disponível em: <https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm>. Acesso em: 22 out. 2018.

lidade da reidentificação do sujeito titular dos dados através da utilização de meios razoáveis para tal. O propósito do processo consiste justamente na perda do elo entre o elemento identificador contido no dado e o sujeito titular; assim, a operação reversa para reconstituição de tal ligação deve ser inviabilizada. Isto pressupõe que a técnica anonimizadora utilizada pelo próprio controlador de dados deve tornar a reidentificação inviável inclusive por ele próprio. Não é o caso da técnica de anonimização empregada garantir de maneira integral a impossibilidade de reidentificação, aliás, a própria noção de que o processo de anonimização pode garantir a impossibilidade total de reidentificar o sujeito de dados não passa de um mito[107]. Não há notícia de técnica existente capaz de suprimir totalmente a identificabilidade de um dado, efetuando, assim, uma operação irreversível. Em lugar desta tarefa impossível, exige-se das operações de anonimização que o resultado final gere dados que não lograriam ser reassociados ao seu titular através do emprego das tecnologias disponíveis à época do tratamento[108]. Neste sentido, o discurso que sustentava outrora a irreversibilidade do processo de anonimização cede espaço a uma abordagem baseada na mitigação dos riscos desta irreversibilidade[109].

A LGPD dispõe em seu artigo 5º, III, que o dado anonimizado corresponde ao *"dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento"*. No caput do artigo 12, encontramos:

> 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.
>
> § 1º 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.
>
> § 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.

Dados anonimizados não são, portanto, protegidos pela guarida legal, a menos que seja possível reverter os processos de anonimização. Note-se que, para que essa reversão seja operada e haja a consideração do dado anonimizado como dado pessoal, a

acesso em 22/10/18

107 NARAYANA & SHMATIKOV, 2010, p. 24 *apud* BIONI, Bruno Ricardo. Op. Cit. 2016. p. 27

108 A Lei 13.709/18 assim dispõe em seu artigo 5º, III: *dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento*.

109 UK Information Commissioner Office, 2012. *apud* BIONI, Bruno Ricardo. Op. Cit. 2016. p. 29

lei adota o parâmetro da razoabilidade, levando em conta as variáveis de custo, tempo e tecnologias correntemente disponíveis. Cumpre aqui destacar que o parágrafo 2º, do artigo 12, constitui um aspecto original da lei brasileira, isto é, inexiste similar disposição na GDPR. Segundo a LGPD, dados anonimizados poderão ser considerados pessoais, caso sejam utilizados para a prática de definição de perfil comportamental de determinada pessoa natural, conquanto seja identificada. Isto evidencia uma abordagem consequencial sobre os dados anonimizados, é dizer, em vez de ater-se à consideração da razoabilidade da reversão do processo de anonimização, a lei leva em conta os possíveis impactos a serem gerados ao livre desenvolvimento da personalidade individual decorrentes do processamento de dados[110].

Nas discussões sobre anonimização, distinguem-se dos dados anonimizados os chamados pseudoanonimizados. Os dados pseudoanonimizados são aqueles que têm atribuídos a si elementos pseudônimos a fim de ter seu conteúdo original "disfarçado". Assim, por exemplo, num banco de dados qualquer, o número de CPF de um indivíduo poderia ter todos os seus números trocados por números ou caracteres aleatórios. A técnica de pseudoanonimização não deve ser considerada como um meio efetivo à promoção da anonimização, mas, sim, como uma medida de elevação de segurança para redução da característica relacional de amostras de dados. A LGPD brasileira não distingue dados anonimizados de dados pseudoanonimizados. Em contraste à GDPR europeia, a legislação brasileira não abranda obrigações legais aos controladores de dados que empregam a técnica de pseudoanonimização.

Utilizada isoladamente, a técnica pseudonimizante não é capaz de conferir um nível satisfatório de desidentificação ao dado, deixando de suprimir as partículas identificadoras de seu titular a que se referem as informações. Algumas situações são hábeis a atestar isso: a reutilização de pseudônimos num mesmo banco de dados, por exemplo, aumenta as chances da soma dos diferentes registros em que os pseudônimos foram utilizados ser capaz de identificar um indivíduo, aumentando, assim, os ricos de identificação[111]. Se empregada junto a outras técnicas, contudo, a pseudonimização pode servir de maneira bem-sucedida à constituição de um dado anonimizado. Os pseudônimos ainda

110 BIONI, Bruno Ricardo; MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira. **GDPR matchup: Brazil's General Data Protection Law**. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/>. Acesso em: 31 out. 2018.

111 Data Protection Comission of Ireland. **Anonymisation and pseudonymisation**. Disponível em: <https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm>. Acesso em: 22 out. 2018.

servem como um retrato indireto detalhado de um indivíduo[112]. A LGPD menciona a pseudonimização brevemente, numa única disposição que indica que os estudos de saúde pública que se valem de bases de dados deverão ser conduzidos sempre que possível com a utilização de técnicas de anonimização e pseudonimização entre suas práticas de segurança adotadas. A pseudonimização chega a ser definida pelo artigo 13, § 4º:

> 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.
> [...]
> § 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[113].

A GDPR aborda a temática de dados anonimizados e pseudonimizados de maneira um pouco diferente. O regulamento não faz menção aos dados anonimizados, no entanto, cuida extensivamente dos dados pseudonimizados.

2.4.3 Consentimento e autodeterminação informacional

O consentimento constitui um elemento-chave no âmbito da proteção de dados pessoais. É por meio dele que o indivíduo expressa, precipuamente, sua concordância com os fluxos de coleta, tratamento e transmissão a serem desdobrados a partir de seus dados. O ato de consentir constitui elemento característico do direito contratual. A manifestação da concordância por parte do titular dos dados com as operações a serem derivadas de suas informações pessoais embasa o próprio exercício da já mencionada autodeterminação informacional. Assim, não é difícil entender por que o consentimento constitui um marco para toda a regulação da matéria.

Nos quadros regulatórios, o consentimento ascendeu como uma espécie de carta coringa regulatória em razão da complexidade no estabelecimento de um sistema robusto, capaz de abarcar autorizações e proibições, que tratasse do tratamento de dados pessoais[114]. Desde já, cumpre ressaltar que consentimento não é a única via possível para o

112 Article 29 Data Protection Working Party, 2013. *apud* BIONI, Bruno Ricardo. Op. Cit. 2016. p. 25
113 BRASIL. Lei n. 13.709, de 14 de ago. de 2018.
114 POLONETSKY, J; O, TENE. 2011. p. 47 *apud* BIONI, Bruno Ricardo. Op. Cit. 2016. p. 43

desdobramento de operações sobre dados pessoais, sendo previstas legalmente hipóteses específicas em que este é preterido.

Existem várias nuances a serem observadas a respeito do consentimento. A LGPD define o consentimento, em seu art. 5º, XII, como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". A dimensão mais básica do consentimento refere-se à da informação. A tomada de decisão a respeito de autorização do tratamento de seus dados pressupõe que o indivíduo tenha tido acesso às informações concernentes a estas operações. Portanto, o consentimento é considerado informado quando houve a apresentação de informações e descrições concernentes às operações envolvendo seus dados ao indivíduo. Em alinhamento com o princípio da transparência, estas informações necessitam ser expostas de maneira clara, precisa e facilmente acessível, mencionando-se a realização do tratamento e os respectivos agentes de tratamento, nos termos do art. 6º, inciso VI, da LGPD. Ademais, cabe destacar que o consentimento será tido como 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 (Art. 9º, § 1º, LGPD).

A manifestação livre refere-se à noção de que ao sujeito titular dos dados cabe a decisão voluntária, feita de maneira desimpedida e não coercitiva, sobre o tratamento de suas informações. Assim, a presença de elementos coercitivos, elementos que não dão real poder de escolha ao titular de dados ou elementos que preveem consequências negativas em caso do não-aceite descaracterizam o consentimento livre. Algumas situações comuns que embaraçam a livre manifestação do consentimento merecem ser destacadas.

O desequilíbrio de poder entre as partes envolvidas constitui um óbice clássico. Embora se possa dizer que este desequilíbrio seja característico entre as partes que transacionam dados, algumas situações configuram um arranjo de tal modo assimétrico que a manifestação do consentimento livre resta prejudicada. Seria o caso, por exemplo, de grande número das transações com autoridades públicas, e, ainda, daquelas processadas no contexto laboral, com o empregador. Neste último tipo, o desequilíbrio é bastante evidente: o empregado - temendo ser rechaçado de inúmeras maneiras, inclusive, em última instância, com a perda de seu trabalho – vê seu poder de escolha mitigado diante de solicitações ou exigências de seu empregador no tocante ao tratamento de seus dados.

A LGPD não prevê disposições específicas voltadas a este problema. Vale a menção de que, no ambiente europeu, o antigo Grupo de Proteção de Dados do Artigo 29 chegou a asseverar em sua análise sobre o consentimento sob o regime da GDPR que, em grande número de situações envolvendo o âmbito laboral, o consentimento dos empregados não constitui a base legal adequada para o processamento de seus dados[115]. No âmbito brasileiro, trata-se de uma temática específica a ser apreciada pela futura Autoridade Nacional de Proteção de Dados.

O Grupo de Proteção de Dados do Artigo 29 ressalta a importância do aspecto da condicionalidade na análise da liberdade de escolha no ato de consentimento. O condicionamento da aceitação do tratamento de dados para a execução de um determinado contrato pode oferecer riscos proeminentes ao consentimento. Atrelar o consentimento à aceitação dos termos e condições do contrato de forma geral, ou condicionar um contrato ou serviço ao consentimento para processamento de dados pessoais que não são necessários à execução deste contrato ou serviço é considerado pelo Grupo de Proteção de Dados do Artigo 29 altamente indesejável[116]. A GDPR perfila, em sua consideração inicial de nº 43, o entendimento de que o consentimento não é presumido livre 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"[117].

A lei brasileira não tece considerações tão específicas a este respeito, mas reconhece a necessidade de destaque:

> Art. 9º
>
> § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Próxima à condicionalidade, encontra-se a granularidade, que consiste na segmentação do consentimento. Por vezes, o processamento e tratamento a ser aplicado so-

115 ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on consent under Regulation 2016/679. p. 7. Disponível em: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>. Acesso em: 30/10/2018

116 Idem. Ibidem.

117 Considerando nº 43, 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.

bre um dado pessoal não é monolítico, é dizer, o ato de consentimento a ser expressado pelo sujeito de dados não irá autorizar apenas um tipo de uso sobre os dados, mas vários. Um exemplo[118]: um revendedor comercial põe ao crivo do consentimento de seu cliente dois fins distintos – um deles se refere ao cadastramento do e-mail pessoal do cliente para recebimento de conteúdo publicitário, o outro, ao compartilhamento do perfil deste consumidor com outras empresas do grupo ao que o revendedor comercial pertence.

Note-se que se trata de dois usos distintos e independentes para os dados do usuário, de maneira que os atrelar de maneira inseparável para obtenção do consentimento corresponde à estratégia que fere à liberdade individual de escolha, e, portanto, eiva de vício o consentimento eventualmente adquirido. Daí advém a dimensão granular do consentimento; é preciso que seja oportunizado ao titular dos dados o consentimento para diferentes usos e operações.

Por fim, também adjetiva o consentimento o aspecto de inequívoco, que denota a necessidade daquele em encontrar sua expressão através de uma manifestação certeira, impassível de ambiguidades. O consentimento, assim, deve tomar forma de maneira tal que não sejam deixadas dúvidas a seu respeito. A LGPD prevê, sucintamente, que o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (Art. 8, *caput*). Prevê-se, ainda, que, caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais (Art. 8º, § 1º).

O Grupo de Proteção de Dados do Artigo 29 assinala algumas pontuações interessantes a respeito do caráter inequívoco do consentimento. Sob a GDPR, é inválida a apresentação ao usuário de caixas de diálogo que já estejam previamente assinaladas em concordância com o que é proposto quando apresentadas ao usuário[119]. Tampouco se considera haver consentimento com o mero aceite dos termos gerais e condições do serviço[120]. Para o Grupo de Proteção de Dados do Artigo 29 , a continuidade da navegação em um *website* pelo titular de dados, mesmo diante de um alerta requerendo consenti-

118 ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on consent under Regulation 2016/679. p. 10 Disponível em: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>. Acesso em: 30/10/2018.
119 ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on consent under Regulation 2016/679. p. 17 Disponível em: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>. Acesso em: 30/10/2018.
120 Idem. Ibidem.

mento do usuário, não indica uma ação inequívoca capaz de promover a configuração de consentimento, em razão desta navegação.

Uma observação interessante refere-se ao fenômeno da "fadiga do consentimento". No contexto digital, muitos serviços necessitam de dados para seu funcionamento regular, de modo que o usuário se depara frequentemente com a necessidade de expressar seu consentimento por meio de cliques e deslizes em telas. Essa frequência pode engendrar a fadiga do usuário e titular dos dados, que acaba deixando de ler os termos de consentimento. Para a GDPR, é obrigação dos controladores de dados desenvolver mecanismos que combatam este tipo de situação[121]. Para que se caracterize, é preciso que haja uma ação afirmativa e distinguível por parte do titular de dados. Cumpre destacar que a manifestação de vontade do titular pode encontrar várias formas para perfazer-se, sendo possível que se concretize, entre outros, pelo meio escrito, oral, ou até mesmo por um movimento físico específico de um *smartphone*.

Como anteriormente delineado, afora o consentimento, há outras bases legais que autorizam o tratamento de dados. Entre estas, o legítimo interesse do controlador de dados merece ser destacado. Na redação do artigo 10 da LGPD, encontra-se que o legítimo interesse autoriza o tratamento de dados pessoais com base em situações concretas, que incluem, mas não se limitam ao apoio e promoção de atividades do controlador, e à proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem.

2.5 Vetos à LGPD e a Importância da Autoridade Nacional de Proteção de Dados Pessoais

A despeito do PLC nº 53 ter sido produto de um longo processo de discussões e maturação de propostas envolvendo atores interessados diversos, nove artigos tiveram suas disposições vetadas parcial ou integralmente quando da sanção da lei pela Presidência. Os vetos realizados referem-se à publicidade sobre o uso compartilhado de dados pessoais entre órgãos e entidades de direito público (art. 28), às sanções administrativas que previam a cessação parcial ou total das atividades de tratamento de dados, assim como o funcionamento do banco de dados associado à infração (art. 52, incisos VII, VIII e IX); a proteção dos dados pessoais de requerentes de acesso à informação (art. 23, II) e à criação da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (arts. 55 ao 59). O veto mais signifi-

121 Idem. p. 10

cativo, e também alvo de duras críticas, corresponde ao da criação da Autoridade Nacional de Proteção de Dados Pessoais.

A Autoridade Nacional de Proteção de Dados Pessoais corresponde à entidade fulcral à observância e devida aplicação da lei, o que se pode atestar pelo fato do projeto de lei aprovado pelo Senado Federal em 10 de julho de 2018 mencionar a autoridade nacional 48 vezes[122] ao longo de seu texto. O projeto de lei dispunha que a autoridade nacional seria entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça. Sua estruturação se daria nos moldes das agências reguladoras e sua composição interna abrangeria dois órgãos: o Conselho Diretor, órgão máximo, e o Conselho Nacional de Proteção de Dados Pessoais. O regime autárquico especial previsto proveria a autoridade nacional de independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes, bem como autonomia financeira. Entre as atribuições previstas no art. 56 (vetado) da LGPD, podemos destacar: a fiscalização e aplicação de sanções em caso de descumprimento das prescrições legais para o tratamento de dados; edição de regulamentos e procedimentos sobre proteção de dados pessoais; atendimento de petições de titular contra controlador e promoção de estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade. Sem uma autoridade independente, é evidente que a implementação da lei e a persecução de seus fins restam vastamente prejudicados.

A criação da autoridade nacional, bem como do Conselho Nacional de Proteção de Dados Pessoais, no entanto, foi vetada pela presidência, sob a justificativa de vício de iniciativa. Baseado na cumulação do artigo 61, § 1º, II, 'e', e do artigo 37, XIX, da Constituição Federal, o veto presidencial justifica a denegatória apontando que, nos termos constitucionais, a criação da autoridade nacional, órgão pertencente à administração pública indireta, caberia apenas à iniciativa legiferante do órgão executivo. Como descrevemos anteriormente, o PL nº 53/2018 surgiu como resultado das discussões na Câmara dos Deputados em apreciação dos projetos do poder Executivo e da Câmara dos Deputados que passaram a tramitar em conjunto – respectivamente, os PLs 5.276/16 e 4.060/12.

Argumenta-se que o veto presidencial alegando vício de iniciativa é insustentável, em razão da participação do poder Executivo por meio do PL 5.276/16, que, já an-

122 BRASIL. Parecer n º129, DE 2018 - Plenário/Senado Federal. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7821097&ts=1538690046263&disposition=inline&ts=1538690046263> Acesso em 28/10/2018

tes de seu apensamento ao PL 4.060/12, previa a criação de um órgão fiscalizador. Esta é a conclusão plasmada em parecer assinado pelo ex-ministro do Superior Tribunal Federal Ilmar Nascimento Galvão, e o professor da Universidade de Brasília Jorge Octávio Lavocat Galvão, acerca da constitucionalidade dos artigos 55 e 56 (referentes à ANPD) da LGPD.

A previsão originalmente contida no PL 5.276 referia-se à criação de um órgão fiscalizador competente que integraria a administração pública direta, porém, após emenda parlamentar decorrente das discussões travadas pelo apensamento ao PL 4.060/12, este órgão passou a ser previsto como uma autarquia em regime especial, vinculada ao Ministério da Justiça, nos moldes já anteriormente delineados.

Os pareceristas aduzem que não há caracterização de inconstitucionalidade formal, haja vista que as alterações promovidas pelo poder legislativo em relação às iniciativas legislativas do poder executivo encontram-se dentro da margem de discricionariedade daquele primeiro poder. Neste sentido, a alteração do órgão competente pertencente à administração direta para uma autarquia autônoma, promovida pelo Parlamento, não incorreria em inovação legislativa, tratando-se, em verdade, de um ajuste julgado adequado em decorrência das discussões parlamentares travadas. Enquanto a autarquia possui personalidade jurídica própria, sendo dotada de maior autonomia, o órgão público circunscreve-se dentro da estrutura estatal, sendo-lhe atribuídas competências bem-definidas. A alteração de um para o outro é plenamente admissível, pelas razões já expostas. O parecer assevera, ainda, que é entendimento plasmado pelo próprio STF que as emendas parlamentares efetuadas às iniciativas legislativas do poder executivo são possíveis desde que não resultem em aumento de despesas. Reproduzimos parte de sua fundamentação:

PARECER

[...]

> 22. No contexto, é importante destacar que a jurisprudência do Pretório Excelso é firme no sentido da possibilidade de emenda parlamentar a projetos de iniciativa do Poder Executivo, desde que não haja aumento de despesas[9].
> 23. É aqui que se encontra a chave da questão. A Constituição Federal de 1988, em seu art. 61, §1º, inciso II, alíneas "a", "bc" e "e", delimita que qualquer alteração estrutural da Administração Pública e do quadro de servidores depende de lei de iniciativa privativa do Presidente de República. Ademais, o art. 63, I, da Carta Magna proíbe que haja aumento de despesas por meio de emenda parlamentar em projetos de iniciativa do Poder Executivo.
> 24. A regência constitucional tem como escopo deixar a decisão sobre a prestação do serviço público ao Chefe do Poder de Executivo. De acordo com o seu plano de governo e com o orçamento disponível, o Presidente da República encaminha ao Congresso Nacional os projetos de lei com criação

> ou modificação da estrutura administrativa pertinentes às políticas públicas que pretende implementar.
> 25. Ao Poder Legislativo cumpre debater se a forma adotada é adequada. Caso entenda necessário modificar algum ponto, poderá fazê-lo, desde que não implique aumento de despesa, visto que a opção de alocação de recursos para determinada política pública é exclusiva do Chefe de Governo. Ou seja, os parlamentares não podem alterar a essência da política pública, mas apenas aprimorá-la, dentro das mesmas balizas orçamentárias, ou rejeitá-la, se entenderem impertinentes.
> 26. Na mesma linha, os parlamentares também não estão autorizados a desvirtuar o projeto do Poder Executivo. É preciso, pois, que as emendas parlamentares guardem estreita relação com a proposta original. Não por outro motivo o Supremo Tribunal Federal assentou a que "*a ausência de pertinência temática de emenda da casa legislativa em projeto de lei de iniciativa exclusiva leva a concluir-se pela inconstitucionalidade formal*"[10].
> 27. No caso em análise, a modificação da natureza jurídica do ente fiscalizador de órgão público para autarquia não implicou aumento de despesa. Também não houve criação de cargos. O que o PLC nº 53/2018 fez foi apenas delimitar como será formado o Conselho Diretor da ANPD, sem indicação da natureza do cargo ou o valor de sua remuneração.
> 28. Em verdade, delegou-se ao Poder Executivo a elaboração do regulamento e da estrutura organizacional da ANPD, conforme §4º do art. 55. Já os cargos públicos deverão ser criados posteriormente por lei ou realocados na forma do art. 84, VI, "a", da Constituição Federal de 1988.
> 29. Dito de outra forma, o fato de haver especificação da composição do Conselho Diretor não implicou aumento de despesas, já que os cargos não foram formalmente criados pelo PLC nº 53/2018[123].

O parecer ainda aduz a inexistência de corrupção à temática do projeto, em razão das competências previstas para a ANDP no PL Nº 53/18 serem similares, senão idênticas àquelas dispostas no art. 53 do projeto 5.276/16, encaminhado pela presidência da República. A adequação promovida pela emenda parlamentar visou, assim, à promoção da estrutura administrativa mais adequada à persecução dos fins atribuídos à entidade. Por todas as considerações feitas, o parecer conclui pela inocorrência de inconstitucionalidade formal.

Quando da sanção da versão final da lei, o presidente da República comunicou não ser contrário à criação da autoridade nacional, devendo proceder ao encaminhamento de um novo projeto de lei até o fim de seu mandato. Especula-se sobre a autoridade a ser responsável pela aplicação e fiscalização da lei, caso uma autoridade autônoma não esteja constituída na entrada em vigor da LGPD, a partir de fevereiro de 2020. Mencionam-se, neste sentido, a Agência Brasileira de Inteligência (Abin), o Ministério Público Federal, e até a Polícia Federal[124]. O prazo oferecido para a adaptação às novas disposi-

123 Ex-ministro diz que não há vício de inconstitucionalidade na criação da ANPD. **JOTA**, Brasília, 21 jul. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018>. Acesso em 29/10/2018

124 RAMIRO, André; TAVARES, Paulo. Sancionada a Lei de Proteção de Dados Pessoais, mas com vetos. O que significam?. **Diario de Pernambuco**, Recife, 17 ago. 2018. Política. Disponível em: <http://www.diariodepernambuco.com.br/app/noticia/politica/2018/08/17/interna_politica,760335/sancio-

ções legais – definida pelo início da vigência início da LGPD para fevereiro de 2020 – não pode ofuscar a dimensão urgente da criação e estruturação da autoridade nacional. Por todas as razões já expostas, sem esta entidade bem-estruturada, a qual é legado extenso rol de atribuições, a lei pode tornar-se inócua, tendo-se em vista o desfalque proeminente entre as previsões legais e a capacidade de controle.

nada-a-lei-de-protecao-de-dados-pessoais-mas-com-vetos-o-que-s.shtml>. Acesso em: 29 out. 2018

3. O REGIME BRASILEIRO DE PROTEÇÃO DE DADOS PESSOAIS

3.1 Considerações sobre a Lei Geral de Proteção de Dados Pessoais

Com a sanção da LGPD, o Brasil finalmente possui uma lei especificamente dedicada à proteção de dados pessoais, juntando-se à lista dos quase 120 países e territórios autônomos[125] que já oferecem um marco regulatório específico voltado ao tema. As discussões no âmbito institucional se estenderam por oito anos, sendo confrontadas perspectivas de diferentes matizes, fazendo da legislação aprovada um esforço multissetorial.

Há uma evidente confluência normativa entre a LGPD e a GDPR. As bases de ambas as legislações são construídas sobre princípios, assoalho normativo hábil a resistir à passagem do tempo e ao intenso ritmo de disrupção tecnológica. A partir da principiologia, apoia-se em definições-chaves dos componentes que perpassam todo o sistema protetivo – conceito de dados pessoais, dados sensíveis, consentimento, controladores e operadores – para erigirem-se sistemas de proteção que regulam as tantas operações que envolvem dados, estabelecendo-se obrigações aos agentes de tratamento e direitos ao titular dos dados. Indispensável a esta arquitetura normativa é a fiscalização do cumprimento das disposições legais, para a qual é imprescindível a presença de uma entidade reguladora, responsável, entre outras atribuições, pelo contato com os entes que recolhem e processam dados e pela aplicação das sanções previstas em lei.

Como anteriormente exposto, a ausência de um órgão independente a ser responsável pela observância e fiscalização da lei apresenta severos riscos à efetividade do quadro regulatório brasileiro. Para a LGPD, a autoridade nacional corresponde propriamente a um "pilar de sustentação, sem o qual todo o arcabouço normativo e principiológico vem a ruir"[126]. Não à toa, entre os cerca de 120 países que já contam com uma norma específica para a matéria, apenas 12 não possuem uma entidade autônoma nos moldes mencionados, como Angola e Nicarágua[127].

---

125 Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2018 (September 4, 2018). Available at SSRN: https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

126 DONEDA, Danilo Cesar Maganhoto; MENDES, Laura Schertel. Lei de proteção de dados não pode morrer na praia: Eventual veto ameaçaria fino equilíbrio alcançado. **Folha de São Paulo**, São Paulo, 10 mar. 2018. Opinião. Disponível em: <https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protecao-de-dados-nao-pode-morrer-na-praia.shtml>. Acesso em: 29 out. 2018

127 Idem.

Cumpre aqui reiterar a atuação pluralista das autoridades nacionais de proteção de dados. Os artigos vetados da LPGD revelam que as incumbências da ANDP vão muito além da fiscalização e da aplicação de sanções. Ressaltam-se aqui algumas delas: atendimento às petições de titulares contra responsáveis pelo tratamento de seus dados; desenvolvimento da Política Nacional de Proteção de Dados Pessoais; promoção de estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; cooperação com autoridades nacionais de outros países; edição de regulamentos e procedimentos sobre a proteção de dados e privacidade, assim como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco para a garantia dos princípios gerais de proteção de dados pessoais, conforme a previsão da LGPD; oitiva dos agentes de tratamento e da sociedade a respeito de assuntos relevantes à matéria.

Nota-se, portanto, que a autoridade reguladora é absolutamente necessária ao fortalecimento de um sistema de proteção de dados, uma vez que contribui para sua estruturação por meio das diversas atividades que desenvolve nas áreas normativa, consultiva, educativa, de mediação, de representação internacional, entre outras.

Os efeitos desta ausência também são colaterais, na medida em que as relações exteriores mantidas com o país são afetadas. O interesse do Brasil em ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), noticiado em abril de 2018, fica prejudicado, uma vez que um dos requisitos exigidos de seus membros-integrantes é a adequada proteção de dados pessoais, para cuja concretização é fundamental um órgão autônomo nos moldes da autoridade nacional. Igualmente obstado figura o livre fluxo de dados com os países integrantes da União Europeia, dado que, para que a transmissão de dados transcorra sem autorizações recorrentes, a GDPR exige que os países terceiros ofereçam um nível adequado de proteção de dados pessoais, o que tem como pré-requisito um controle efetivo e independente desta proteção[128].

3.2 Regulação de risco e corregulação

Um ponto importante a ser observado em ambas as regulações corresponde à abordagem dos riscos envolvendo as operações com dados pessoais**.** O avanço do mode-

128 Art. 45(2)(*b*), da GDPR: 2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos: b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros;

lo econômico centrado em dados e a propagação de fenômenos como a governança algorítmica, *big data*, inteligência artificial e internet das coisas evidencia que a proteção de dados pessoais está relacionada, além da tutela à privacidade, ao exercício de várias liberdades e direitos individuais. Um dos exemplos aptos a demonstrar isto, como já expusemos, é a prática da perfilização, ou seja, a definição de um perfil comportamental para o usuário titular de dados, prática de tratamento de dados em franca expansão cujos desenvolvimentos podem engendrar discriminação e inibição do exercício de liberdades.

Considerando ser esta prática uma tendência geral, vê-se que a proteção de dados está não apenas relacionada à dimensão do indivíduo e sua privacidade, mas, também a valores coletivos de uma maneira mais ampla[129]. É este quadro, caracterizado pelas ameaças potenciais causadas pelo tratamento de dados, que engendra a ascensão da consideração dos riscos na proteção de dados pessoais. A chamada regulação do risco revolve em torno da probabilidade de que um prejuízo venha a se configurar no futuro, de tal modo que as normas desenvolvidas buscam antecipar-se à configuração deste malefício. Ambas as legislações, GDPR e LGPD, reconhecem que as operações envolvendo dados pessoais podem gerar riscos às liberdades civis e aos direitos fundamentais[130] e, para preveni-los, incubem os controladores de dados da elaboração de um documento, o relatório de impacto à privacidade[131]. Neste estudo de impacto à privacidade, devem ser registrados os processos de tratamento de dados que representem ameaça considerável às garantias supramencionadas, bem como apontadas ferramentas hábeis à promoção da segurança através da mitigação destes riscos.

O papel desempenhado pelos agentes de tratamento na mitigação de riscos sinaliza a incorporação de uma dinâmica corregulatória aos quadros legais. Explica-se: os agentes de tratamento, públicos ou privados, são corresponsáveis pela promoção da proteção de dados pessoais através do poder de agência que exercem nas estruturas organi-

---

129 WRIGHT, D.; RAAB, C. 2012, 2014 *apud* BENETT, Colin; RAAB, Charles D. **Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective**. p. 10 2018. Disponível em: <https://ssrn.com/abstract=2972086> Acesso em: 20/10/2018

130 Ver, entre outros, artigos 44, II e 50, da LGPD, e os considerandos de nº 51), 76), 77) e 83) da GDPR.

131 **Artigo 5º, XVII, da LGDP:** XVII - relatório de impacto à proteção de dados pessoais: 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;

Artigo 35(1), da GDPR: Quando um certo tipo de tratamento, em particular que utilize novas tecnologia se tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.

zacionais que integram. Tanto na GDPR[132] quanto na LGPD[133], devem os agentes de tratamento desenvolver medidas apropriadas para a observância das prescrições legais, as quais incluem, entre outros, regras de boas práticas e de governança, códigos de conduta, diretrizes internas para processamento de dados, ações educativas, mecanismos internos de mitigação de riscos.

Segundo Rafael Zanatta, a proteção de dados pessoais baseada num modelo de regulação do risco conta com os seguintes elementos:

> (i) instrumentos de tutela coletiva e participação de entidades civis no diálogo preventivo com autoridades independentes de proteção de dados pessoais, (ii) obrigações e instrumentos de regulação *ex ante* atribuídas aos controladores para identificação de riscos a direitos e liberdades fundamentais, (iii) disseminação e metodologias de "gestão de risco" e calibragem entre riscos gerados pelo tratamento e uso de dados pessoais e imunidades jurídicas construídas pela discussão ética sobre os limites do progresso técnico[134].

Em atenção ao ponto i), é interessante pontuar que tanto a legislação europeia[135] quanto a brasileira[136] preveem a possibilidade de adjudicação de demandas judiciais por organizações coletivas na matéria de proteção de dados pessoais, sinalizando a ascensão de uma perspectiva que prima pelo interesse coletivo da proteção de dados.

Em suma, vê-se que há uma convergência, tanto teleológica quanto estrutural, entre as leis brasileira e europeia de proteção de dados pessoais. Na prática, a União Europeia conta com um sistema de proteção de dados bem-desenvolvido, consolidado pelas evoluções e aperfeiçoamentos experimentados através das décadas. Não é demais relembrar que, ainda em 1981, a matéria era abordada na Convenção 108/CE. Este pioneirismo permitiu o acompanhamento da evolução no tratamento dos dados pessoais, pri-

132 Ver, entre outros, artigos 40, 41 e 42, da GDPR.

133 Art. 50, caput, LGPD: Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

134 ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? p. 10 **I ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET**, novembro de 2017. Disponível em: <http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf>. Acesso em: 10/10/18

135 Artigo 80(1), GDPR: O titular dos dados tem o direito de mandatar um organismo, organização ou associação sem fins lucrativos, que esteja devidamente constituído ao abrigo do direito de um Estado-Membro, cujos objetivos estatutários sejam do interesse público e cuja atividade abranja a defesa dos direitos e liberdades do titular dos dados no que respeita à proteção dos seus dados pessoais, para, em seu nome, apresentar reclamação, exercer os direitos previstos nos artigos 77.o, 78.o e 79.o, e exercer o direito de receber uma indemnização referido no artigo 82.o, se tal estiver previsto no direito do Estado-Membro.

136 Artigo 22, LGPD: Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

mando-se pela sintonia com os novos desafios engendrados pelas inovações tecnológicas que se sucederam. Destaca-se neste sentido a atuação do Grupo de Proteção de Dados do Artigo 29, responsável pela investigação detida e emissão de opiniões e análises sobre situações emergentes.

Para lograr êxito semelhante, o Brasil ainda deverá avançar bastante na matéria de proteção de dados. O desenvolvimento de um sistema nacional bem-sucedido de proteção de dados pessoais passa, por todas as razões já exploradas, pela criação de uma autoridade nacional. Apenas com a superação do impasse gerado por sua ausência, poderá o Brasil enfrentar a pluralidade de situações e questões envolvendo a proteção de dados.

CONSIDERAÇÕES FINAIS

As assunções que apontam a privacidade como um elemento em extinção na atualidade assentam-se em evidências vastas neste sentido. Ainda que vários sejam os fatores que contribuam para a erosão da percepção pública acerca da garantia à privacidade, a convergência semântica entre a proteção da privacidade e o elemento objetivo dos dados pessoais desvela uma abordagem com potencial de reabilitação desta prerrogativa fundamental. É evidente que para tal é necessário que os componentes mais essenciais da matéria de proteção de dados sejam popularizados e se incorporem à percepção pública. A promoção da popularização deste debate é, inclusive, uma das atribuições da vindoura autoridade nacional de proteção de dados pessoais.

Constitui um lugar comum a noção de que o Direito não consegue acompanhar o ritmo da disrupção causada pelo fenômeno tecnológico. As abordagens legais que pretendem regular as situações fáticas geradas pelas inovações tecnológicas correm o risco de tornarem-se obsoletas, se incorrerem em disposições deveras específicas, visto que o ritmo da disrupção é incessante. Tendo-se em conta que os dados pessoais passaram a constituir um *commodity* de alto valor para a era digital, a matéria concernente à sua proteção abarca constantes desafios, decorrentes da insurgência contínua de situações inéditas.

Sabe-se que o escopo fundamental das legislações específicas para a proteção de dados pessoais é a tutela do livre desenvolvimento da personalidade humana. A proteção oferecida aos dados pessoais fundamenta-se, em seus termos mais básicos, a partir do reconhecimento do elo que os dados sobre uma pessoa mantêm com a manifestação de sua própria personalidade. Proteger dados é, intrinsecamente, proteger indivíduos ao garantir-lhes que estas manifestações fragmentadas de sua personalidade não sejam utilizadas para fins danosos que ponham em risco sua segurança, sirvam para discriminá-los ou cerceiem suas liberdades. Tem-se visto que os impactos das decisões tomadas a partir das operações envolvendo dados pessoais não se restringem à esfera individual, podendo-se identificar na proteção de dados interesses de ordem coletiva, alinhados a valores éticos aplicados ao corpo social. Este é, inclusive, um ponto a ser observado nas evoluções futuras da matéria: a ascensão da dimensão ética na proteção de dados pessoais, comprometida com a restauração da dignidade humana, e não apenas com a observância das disposições legais.

É nesta conjuntura que ascende o modelo de proteção de dados assentado na regulação de riscos. Analisar os desdobramentos práticos deste novo perfil de proteção será possível apenas com o tempo – especialmente no Brasil, quando se leva em conta que a requisição dos relatórios de impacto à privacidade é atribuída à autoridade nacional a ser criada. A análise da recém-sancionada Lei Geral de Proteção de Dados Pessoais revela um quadro regulatório bem-elaborado, sintonizado com as discussões mais atuais sobre a matéria de maneira flexível, isto é, sem vinculações estreitas ao atual estado tecnológico. Reúnem-se, assim, as condições favoráveis ao desenvolvimento gradativo de um regime bem-sucedido de proteção de dados pessoais. Para que isto ocorra, dever-se-á contar, evidentemente, com a instalação da autoridade nacional de proteção de dados pessoais, cuja importância já foi explicitada na investigação aqui conduzida. A observância dos agentes de tratamento às disposições previstas em lei, especialmente no tocante aos instrumentos de corregulação, é um dos tópicos cujo desenvolvimento deverá ser observado nos próximos anos.

A ampliação dos contornos dos interesses coletivos na proteção de dados constitui outro tema a ser acompanhado. Pergunta-se que tipo de atuação deverá ser predominante: a do indivíduo titular dos dados a exercer sua autonomia informacional, ou a das organizações e entidades civis interessadas na promoção da proteção de dados e da privacidade por interesses coletivos.

REFERÊNCIAS

LEIS E REGULAMENTAÇÕES NORMATIVAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil:** promulgada em 5 de outubro de 1988. Brasília: Senado Federal, 2016.

_____.. **Lei 12.965/2014.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>

_____. Lei n. 13.709, de 14 de ago. de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). -. Brasília, p. 01-02, ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 30 out. 2018.

_____. Parecer n º129, de 2018 - Plenário/Senado Federal. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7821097&ts=1538690046263&disposition=inline&ts=1538690046263> Acesso em 28/10/2018

Declaração de Santa Cruz de La Sierra. XIII CIMEIRA IBERO-AMERICANA DE CHEFES DE ESTADO e DE GOVERNO. Disponível em: < https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf> Acesso em 27/10/18

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

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

REFERÊNCIAS BIBLIOGRÁFICAS E OUTRAS FONTES

Article 29 Data Protection Working Party. **Guidelines on consent under Regulation 2016/679**. Disponível em: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>. Acesso em: 30/10/2018

Data Protection Commission of Ireland. Anonymisation and pseudonymisation. Disponível em: <https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm>. Acesso em: 22 out. 2018.

BENNETT, Colin J. **Regulating privacy: data protection and public policy in Europe and the United States**. 1. ed. Nova Iorque: Cornell University Press, 1992.

BENNETT, Colin; RAAB, Charles D**. Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective**. 2018. Disponível em: <https://ssrn.com/abstract=2972086> Acesso em: 20/10/2018

BIONI, Bruno Ricardo. **Xeque-mate:** o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. [S.l.: s.n.], 2016. Disponível em: <https://www.researchgate.net/publication/328266374_Xeque-Mate_o_tripe_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil>. Acesso em: 17 out. 2018.

BIONI, Bruno Ricardo. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados: Próximas semanas serão decisivas e pode não haver melhor momento para que Brasil deixe para trás seu atraso. **JOTA**, [S.l.], 02 jul. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018>. Acesso em 28 out. 2018

BIONI, Bruno Ricardo; MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira. **GDPR matchup: Brazil's General Data Protection Law**. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/>. Acesso em: 31 out. 2018.

CASTELLS, Manuel. **Sociedade em Rede**: A era da informação : economia, sociedade e cultura; v. 1. 6. ed. Tradução de Roneide Venancio Majer. São Paulo: Paz e Terra, 1999.

DONEDA, Danilo Cesar Maganhoto. **A proteção de dados pessoais nas relações de consumo: para além das informações creditícias**. Brasília: Secretaria de direito econômico / Departamento de proteção e defesa do consumidor, 2010.

DONEDA, Danilo Cesar Maganhoto; ALMEIDA, Virgílio Augusto Fernandes de. Privacy Governance in Cyberspace. **IEEE Internet Computing**, [S.l.], v. 19, n. 3, p. 50-53, maio. 2015. Disponível em: <https://ieeexplore.ieee.org/document/7111890?reload=true>. Acesso em: 28 set. 2018.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1. Ed. Rio de Janeiro: Renovar,

DONEDA, Danilo Cesar Maganhoto**. Privacy and Data Protection in the Marco Civil da Internet.** Disponível em: <http://www.privacylatam.com/?p=239> Acesso em 23/06/14

DONEDA, Danilo Cesar Maganhoto; MENDES, Laura Schertel. Lei de proteção de dados não pode morrer na praia: Eventual veto ameaçaria fino equilíbrio alcançado. **Folha de São Paulo**, São Paulo, 10 mar. 2018. Opinião, p. 12. Disponível em:

<https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protecao-de-dados-nao-pode-morrer-na-praia.shtml>. Acesso em: 29 out. 2018

Ex-ministro diz que não há vício de inconstitucionalidade na criação da ANPD. **JOTA**, Brasília, 21 jul. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018>. Acesso em 29/10/2018

GIDDDENS,, Anthony. **Sociologia**. 4. ed. Tradução: Sandra Regina Netz. Porto Alegre: Artmed, 2005.

GUIDI, Guilherme Berti de Campos. Modelos Regulatórios para Proteção de Dados Pessoais. in: BRANCO, Sérgio; TEFFÉ, Chiara de Teffé (Org.). **Privacidade em perspectivas**. 1. ed. Rio de Janeiro: Lumen Juris, 2018. cap. 6, p. 85-109.

KURBALIJA, Jovan. **Uma introdução à governança da internet** [livro eletrônico] / Jovan Kurbalija. Trad. Carolina Carvalho. São Paulo: Comitê Gestor da Internet no Brasil, 2016.

MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. JOTA, [S.L.], 14 jul. 2018. Disponível em: < https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>. Acesso em 28 out. 2018

NET MUNDIAL - Discurso Dilma Rousseff. Disponível em: <http://www.defesanet.-com.br/cyberwar/noticia/15102/NET-MUNDIAL---Discurso-Dilma-Rousseff/> Acesso em: 28/10/18

PRIVACY INTERNATIONAL. **The Keys to Data Protection:** a guide for policy engagement on data protection. [S.l.: s.n.], 2018. Disponível em: <https://privacyinternational.org/report/2255/data-protection-guide-complete>. Acesso em: 04 out. 2018.

PROST, Antoine; VINCENT, Gérard (Org.). **História da vida privada**. 1. Ed. Tradução de Denise Bottmann, Dorothée de Bruchard. São Paulo: Companhia das Letras, 2009. v. 5.

RAMIRO, André; TAVARES, Paulo. Sancionada a Lei de Proteção de Dados Pessoais, mas com vetos. O que significam?. Diario de Pernambuco, Recife, 17 ago. 2018. Política. Disponível em: <http://www.diariodepernambuco.com.br/app/noticia/politica/2018/08/17/interna_politica,760335/sancionada-a-lei-de-protecao-de-dados-pessoais-mas-com-vetos-o-que-s.shtml>. Acesso em: 29 out. 2018

SOLOVE, Daniel J. Conceptualizing Privacy. **California Law Review**, v. 90, p. 1088-1156, jul. 2002.

SOLOVE, Daniel J. I've Got Nothing to Hide and Other Misunderstandings of Privacy. **San Diego Law Review**, San Diego, v. 44, p. 745-772, jan. 2007. Disponível em: <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.-

com/&httpsredir=1&article=1159&context=faculty_publications>. Acesso em: 28/09/2018.

SOLOVE, Daniel. **The digital person : technology and privacy in the information age**: : technology and privacy in the information age. 2. ed. Nova Iorque: New York University Press, 2006.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? **I ENCONTRODA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET**, NOVEMBRO DE 2017. Disponível em: <http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf >. Acesso em: 10/10/18