UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE DIREITO "PROF. JACY DE ASSIS"

ANA PAULA BOUGLEUX ANDRADE RESENDE

PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO: O TRATAMENTO DE DADOS COMO INSTRUMENTO DE TUTELA DA PRIVACIDADE

UBERLÂNDIA

2019

ANA PAULA BOUGLEUX ANDRADE RESENDE

PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO: O TRATAMENTO DE DADOS COMO INSTRUMENTO DE TUTELA DA PRIVACIDADE

Trabalho de conclusão de curso apresentado à Faculdade de Direito "Professor Jacy de Assis", instituto vinculado à Universidade Federal de Uberlândia, como requisito de aprovação parcial no curso de Bacharelado em Direito.

Orientadora: Profª. Drª. Keila Pacheco Ferreira.

UBERLÂNDIA

2019

ANA PAULA BOUGLEUX ANDRADE RESENDE

PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO: O TRATAMENTO DE DADOS COMO INSTRUMENTO DE TUTELA DA PRIVACIDADE

Trabalho de conclusão de curso apresentado à Faculdade de Direito "Professor Jacy de Assis", instituto vinculado à Universidade Federal de Uberlândia, como requisito de aprovação parcial no curso de Bacharelado em Direito.

Uberlândia, 06 de dezembro de 2019.

_____
Profª. Drª. Keila Pacheco Ferreira – Orientadora

_____
Examinador (a)

_____
Examinador (a)

Dedico este trabalho a quem me acompanhou nessa trajetória desde o início, aos que fizeram parte dela, mas seguiram outros caminhos, e a quem me encontrou no meio da rota e comigo seguiu o itinerário. Dedico àqueles que foram apoio e aconchego nos momentos difíceis e àqueles que tornaram os dias mais leves e prazerosos. Dedico também àqueles que me ensinaram o que é a justiça e qual deve ser o meu propósito entre tantas normativas, vertentes e ideais divergentes.

RESUMO

O presente trabalho objetiva analisar a concepção de privacidade nas últimas décadas, bem como seus reflexos nas sociedades, buscando compreender a importância da temática na atualidade e como se dá a tutela da privacidade no ordenamento jurídico brasileiro. Uma vez imersos nessa temática, observa-se crescente relevância da chamada privacidade de dados pessoais. Nesse sentido, inicia-se um estudo mais aprofundado sobre o conceito dos dados pessoais e suas particularidades, além da aplicação de dados no cotidiano e os riscos da utilização indevida. Superadas as questões iniciais, observa-se que a privacidade de dados tem sido considerada um direito da personalidade, atribuindo-se equivalente importância ao direito à intimidade, por exemplo. Dada a importância da matéria, fica evidente a necessidade de regulamentação, oportunidade em que se estuda os diplomas legais que subsidiaram a proteção de dados pessoais no ordenamento jurídico brasileiro, traçando uma linha cronológica que culmina na recém criada Lei Geral de Proteção de Dados (LGPD). Outrossim, importa destacar quais diplomas legais influenciaram a criação da Nova Lei, dando destaque especial para o Regulamento Geral sobre a Proteção de Dados (GDPR). Superadas essas questões, parte-se para uma análise mais aprofundada da nova lei de proteção de dados pessoais, dando enfoque especial ao tratamento de dados e à autonomia do titular de dados. A LGPD, apesar de ainda não ter entrado em vigor, gera uma série de expectativas aos estudiosos da área, bem como discussões acerca da sua aplicação.

Palavras-chave: Privacidade. Dados pessoais. Consentimento. Direitos da personalidade. Lei Geral de Proteção de Dados.

ABSTRACT

The present work aims to analyze the conception of privacy in the last decades, as well as its reflexes in the societies, intending to understand the value of the subject in the present time and how the protection of the privacy in the Brazilian legal system occurs. Once immersed in this theme, people can note the growing relevance of the privacy of personal data. In this sense, a deeper study is started on the concept of personal data and its particularities, as well as the application of data in daily life and the risks of misuse. Overcoming the initial issues, it is observed that data privacy has been considered a personality right, giving equal importance to the right to privacy, for example. Given the importance of the subject, it is evident the necesity for regulation, occasion when it takes advantage to study the legal acts that subsidized the protection of personal data in the Brazilian legal system, drawing a timeline that culminates in the recently created General Data Protection Act (LGPD). Furthermore, it is important to highlight which legal acts influenced the creation of the New Law, with special emphasis on the General Data Protection Regulation (GDPR). Overcoming these issues, we move on to further analysis of the new personal data protection law, with a special focus on data processing and data subject autonomy. The LGPD, although not yet in force, generates a number of expectations for scholars in the area, as well as discussions about its application.

Key-words: Privacy. Personal data. Consent. Personality rights. General Data Protection Act.

SUMÁRIO

1 INTRODUÇÃO

Os dados pessoais são definidos como informação relativa a uma pessoa singular identificada ou identificável[1], o titular de dados. Assim, os dados pessoais podem ser exemplificados por nome, número de identificação, dados de localização, endereço, identificadores por via eletrônica, origem racial ou étnica, opinião política, dados genéticos e relacionados à saúde.

É certo que os dados dificilmente possuem valor quando analisados de forma individualizada, mas sim quando examinados diante de determinado contexto, diante da finalidade a que se presta, ou associado a demais informações, sendo nesse sentido que os bancos de dados fundamentam-se, os quais constituem um conjunto de informações estruturado conforme determinada lógica, geralmente utilitarista.

Ao tempo que a formação de bancos de dados se dava de forma manual, era inviável e nem sequer havia justificativa para compilação de grandes volumes de informação. No entanto, o surgimento dos bancos de dados automatizados possibilitou a sistematização de grande quantidade de informações, gerando consequências que que vão da influência do mercado de consumo até mesmo à influência de decisões individuais, sendo verdadeiro redistribuidor de poder na era da informação.

Nesse contexto, a atenção é voltada à proteção que os denominados dados pessoais recebem, bem como ao poder de controle e à autonomia oferecida aos titulares desses dados.

Importante destacar as mutações do conceito de privacidade no âmbito jurídico, a qual surge como o "direito a ficar só", manifestado por meio de uma liberdade negativa e de um sujeito passivo que evoca a sua intimidade para manter sua inviolabilidade de direitos, à autodeterminação informativa, enquanto liberdade positiva de um sujeito ativo que possui autonomia para estabelecer os limites entre sua esfera pública e privada. Assim, compreender-se-á a relevância da privacidade, bem como a repercussão das suas diferentes concepções.

Ainda, este trabalho analisará a tutela de dados pessoais como objeto derivado do direito à privacidade, mas que diferencia-se desse em diversos aspectos. Também é objeto de análise a historicidade da proteção de dados, bem como a evolução da sua tutela no que diz respeito aos direitos de controle e livre acesso. Nesse sentido, destaca-se formas diversas de tratamento de dados, estabelecendo que a sua utilização inadequada ou a inexistência de

[1] Definição dada pelo Regulamento Geral de Proteção de Dados (Regulamento UE 2016/679 do Parlamento Europeu e do Conselho).

parâmetros mínimos para a utilização ética desse mecanismos são capazes de gerar manipulação ou até mesmo discriminação do titular de dados.

Os riscos da utilização inadequada dos dados pessoais são majorados diante do crescimento exponencial do uso de tecnologias da informação pela população mundial. Assim, constata-se uma grande desproporção entre a denominada "terceira onda", a qual expressa uma revolução cultural e tecnológica, e a ausência de instituições jurídicas capazes de acompanhar e tutelar as transformações do meio social.

Nesse contexto, analisa-se a tutela de dados pessoais no ordenamento jurídico brasileiro, a qual durante muito tempo foi relegada.

Destaca-se, portanto, a Constituição Federal, que assume papel inaugural na proteção de dados pessoais ao assegurar a inviolabilidade da intimidade e da vida privada[2], o *habeas data*, que funciona como garantia constitucional de acesso às informações pessoais que estejam em posse do poder público, o Código de Defesa do Consumidor, que garante o direito de acesso aos cadastros de consumidores, bem como a atualização e pertinência dos dados cadastrais e, por fim, a Lei nº 12.965/14, comumente denominada Marco Civil da Internet, sendo importante marco na regulamentação das relações virtuais.

No entanto, nenhum dos diplomas legais citados foram capazes de proteger os dados pessoais de forma direta e específica, havendo verdadeira carência nesse sentido.

Nessa conjuntura foi sancionada a Lei nº. 13.709/18, a qual dispõe exclusivamente sobre a proteção de dados pessoais. A Lei Geral de Proteção de Dados Pessoais (LGPD) finalmente assegura, de forma clara e expressa, a proteção de dados pessoais no ordenamento jurídico brasileiro. No entanto, alguns desafios quanto à aplicação do diploma legal podem ser vislumbrados, os quais serão mencionados.

O presente trabalho objetiva analisar a proteção de dados pessoais como um desdobramento do direito à privacidade e suas diversas facetas de controle. Procura-se também demonstrar as peculiaridades da tutela dos dados pessoais e a primordialidade de se estabelecer que o controle não seja atribuído tão somente ao poder público, mas também aos próprios titulares de dados e às autoridades fiscalizadoras. Ademais, são objetivos evidenciar possíveis consequências decorrentes da violação da privacidade de dados, bem como analisar a tutela da privacidade de dados no ordenamento jurídico brasileiro, estabelecendo uma linhagem cronológica.

[2] Conforme consignado no artigo 5º, inciso X da Constituição Federal de 1988.

O trabalho tem o propósito de desenvolver pesquisa exploratória, a fim de explicitar a temática tanto para os pesquisadores do tema, quanto para a comunidade acadêmica em geral. O procedimento de pesquisa utilizado será a revisão bibliográfica, sendo necessária uma vasta pesquisa a doutrinas, leis, artigos e jurisprudências, nacionais e internacionais, que dizem respeito ao direito à privacidade e à proteção de dados pessoais, além de ter como referência primordial a Lei Geral de Proteção de Dados Pessoais. A pesquisa será desenvolvida com base no método hipotético dedutivo e através de análise qualitativa dos resultados.

2 PERSPECTIVAS DO DIREITO À PRIVACIDADE

A privacidade, inicialmente, aparenta ter dificultosa conceituação, uma vez que inexistem definições exatas sobre ela na Constituição Federal, nem tampouco no Código Civil. Marcel Leonardi aponta a carência de definição clara e bem delimitada em diversos ordenamentos jurídicos, sendo certo que essa vagueza de significado ocasiona dificuldade na tutela de direitos relacionados à privacidade[3].

O próprio Tribunal Europeu de Direitos Humanos outrora afirmou "não considerar possível, nem necessário, procurar uma definição exaustiva para a noção de vida privada"[4]. Nesse sentido, o que se observa é a dificuldade em delimitar um conceito unitário para esse direito, sendo o mesmo variável conforme a ocasião.

> Dependendo do doutrinador consultado, encontram-se conceitos abrangentes ou restritivos de privacidade. Assuntos como liberdade de pensamento, controle sobre o próprio corpo, quietude do lar, recato, controle sobre informações pessoais, proteção da reputação, proteção contra buscas e investigações, desenvolvimento da personalidade, autodeterminação informativa, entre outros, são excluídos ou incluídos, de acordo com a definição adotada[5].

Em 1973, Karl Mannheim aponta a interiorização como, ao menos a priori, um privilégio de poucos. Exercida inicialmente por monges, no mundo medieval, o isolamento total e parcial combinado com trabalho, orações e exercícios psicológicos seriam capazes de levar a um estado mental inalcançável no mundo dos negócios, sendo certo que contemplação, espiritualização, sublimação e êxtase religiosa transformaram-se em uma arte e propriedade privilegiada. Nesse contexto, surge o que o autor denomina "ufania da interiorização", no sentido de que propositadamente uma elite do isolamento fora criada[6].

Para além disso, a privaticidade e o isolamento, entendidos como "o desejo do indivíduo subtrair certas experiências íntimas ao controle do mundo exterior e reivindicá-las para si próprio", são tidas como virtudes para o desenvolvimento de uma personalidade independente. Assim, Mannheim destaca a importância da reclusão e do isolamento parcial na interiorização das experiências e construção de uma personalidade diferente de nossos semelhantes, a fim de que o indivíduo não resulte em uma "pilha de ajustamento

---

[3] LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Editora Saraiva, 2011, p. 47.
[4] UNIÃO EUROPEIA. Tribunal Europeu de Direitos Humanos. **Niemietz v. Alemanha**, 72/1991/324/396, seção 29, julgado em 16 de dezembro de 1992.
[5] LEONARDI, op. cit., p. 48.
[6] MANNHEIM, Karl. **Diagnóstico de nosso tempo**. 3. ed. Rio de Janeiro: Zahar Editores, 1973, p. 191.

descoordenados", por fim, afirma que "esse processo de socializar nossas experiências é salutar, desde que seja equilibrado por uma esfera de privaticidade"[7].

Percorrendo-se a história da humanidade é correto afirmar que o homem como ser social individual é um princípio sustentado pela sociedade burguesa, a qual tomou força na Idade Contemporânea, após a queda dos Estados absolutistas que tinham como cerne a supremacia de força e de vontade sobre a sociedade[8], e consequente ascensão de um liberalismo econômico impulsionado pela primeira revolução industrial.

> Talvez não haja exagero em dizer que as origens de nosso desejo moderno de privaticidade devem ser encontrados no aparecimento gradativo da burguesia. Foi no mundo da indústria e do comércio que pela primeira vez a oficina e o escritório se separam do lar, e à medida que os mercadores foram enriquecendo tornou-se possível para os membros da família terem quartos separados, instaurando assim a estrutura externa para a diferenciação de nossas atitudes e sentimentos privados e públicos[9].

Nesse sentido, a contemporaneidade é marcada pelo liberalismo jurídico, em que as liberdades individuais revelavam-se praticamente ilimitadas e a autonomia do homem permite a sua própria tutela de vontades, sem que haja intervenção direta do Estado. Como consequência, é possível vislumbrar evidente abuso de direitos legitimado pela autonomia da vontade e exercício livre das liberdades individuais.

> O direito liberal mantinha o Estado longe das relações entre particulares. Enquanto isso, premidos por necessidades fundamentais, os trabalhadores egressos do campo sujeitavam-se a condições aviltantes de moradia e trabalho. No exercício da sua preciosa "liberdade", assinavam contratos "concordando" em se submeter a jornadas de trabalho extenuantes, salários vergonhosos e habitações insalubres. Tudo com a chancela da ordem jurídica, que entendia que os contratos, como frutos do livre acordo de vontades, eram "justos" por definição[10].

Nesse contexto, diante de uma desigualdade social e econômica, os mais fracos acabavam por ceder toda sua liberdade individual aos mais fortes, em nome de uma suposta autossuficiência. Com o tempo, percebeu-se a insuficiência de apenas proteger o homem contra a dominação estatal, sendo necessário reivindicar que o liberalismo jurídico não permitisse a cessão de direitos essenciais dos homens por ânsias imediatas.

Assim, passou-se a defender a criação de uma nova categoria que fosse capaz de assegurar, no campo do próprio direito privado, a proteção daqueles direitos imprescindíveis ao ser humano, direitos que não se limitavam a uma liberdade ilusória e vazia, direitos superiores

---

[7] MANNHEIM, 1973, p.189-190.
[8] Thomas Hobbes em sua obra mais difundida, O Leviatã, associa o Estado a um monstro bíblico, poderoso e invencível, cuja presença se faz necessária para controlar a natural tendência dos homens ao conflito.
[9] MANNHEIM, op. cit., p. 190.
[10] SCHREIBER, Anderson. **Direitos da personalidade**. 2. ed. São Paulo: Atlas, 2013, p. 3-4.

à própria liberdade, direitos a salvo da vontade do seu titular, direitos indisponíveis, direitos inalienáveis, direitos inatos[11].

A luta pelos direitos da personalidade entra em pauta na segunda metade do século XIX, no entanto, havia muita divergência na definição de quais direitos estariam englobados nesse âmbito, bem como resistência quanto à sua aplicação, tendo em vista um ambiente jurídico ainda marcado pelo pensamento liberal.

A tutela jurídica da privacidade, por sua vez, reflete traços do contexto individualista do qual é originária e, estando ambientado em um ordenamento prioritariamente de cunho patrimonialista, reserva-se a um pequeno extrato da sociedade; a tutela da privacidade surge como um direito pertencente a um grupo restrito e privilegiado.

> Não havia realmente lugar para a tutela jurídica da privacidade em sociedades que confiavam a sua regulação a outros mecanismos – fossem estes a rigidez da hierarquia social ou então a própria arquitetura dos espaços públicos e privados; ou porque as eventuais pretensões a respeito da privacidade fossem neutralizadas por um ordenamento jurídico de cunho corporativo e patrimonialista; ou então porque em sociedades para os quais a privacidade representasse não mais do que um sentimento subjetivo, ela não fosse digna de tutela. O despertar do direito para a privacidade ocorreu justamente num período em que mudou a percepção da pessoa humana pelo ordenamento, do qual ela passou a ocupar papel central e ao qual se seguiu a juridificação de vários aspectos do seu cotidiano[12].

O direito à privacidade, nesse contexto, é invocado pelas primeiras vezes nos tribunais com a finalidade de atender pretensões de uma elite, a qual Doneda denomina "um elenco de celebridades de cada época"[13].

Um dos primeiros julgados que se tem notícia diz respeito ao reconhecimento do direito de propriedade sobre correspondências privadas trocadas entre Alexander Pope e Jonathan Swift, as quais foram publicadas por um editor sem autorização, em 1741, na Inglaterra[14]. No mesmo país, em 1848, o Príncipe Albert teria tido objetos de uma coleção privada reproduzidos graficamente e vendidos, sem sua autorização; nesse caso, também fora reconhecido o direito de propriedade e proibida a reprodução[15].

Na França, o Tribunal Civil do Sena decidiu em 1858 que a publicação de retratos de uma atriz no seu leito de morte seria capaz de desrespeitar a família; a demanda foi proposta pela irmã da falecida, tendo sido determinado a apreensão do desenho e de suas provas fotográficas, levando-se em conta que por mais que o sujeito retratado fosse uma artista, sua

---

[11] SCHREIBER, 2013, p. 4.
[12] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 8.
[13] Ibidem, p. 11
[14] Pope v. Curl, 1741 apud DONEDA, op. cit., p. 11.
[15] Prince Albert v. Stange, 1848 apud DONEDA, op. cit., p. 11.

vida privada deveria ser considerada distinta da pública[16]. Na Itália, por fim, o caso que marca o início do reconhecimento do *diritto alla riservatezza* foi julgado em 1953, pelo Tribunal de Roma, no qual a divulgação de aspectos da vida pessoal de Enrico Caruso foram considerados exposição inadequada[17]; no mesmo ano também houve o julgamento de questões relacionadas à privacidade da vida amorosa de Clara Petacci e Benito Mussolini e seu tratamento pela imprensa[18].

Nesse sentido, a primeira abordagem significativa do direito à privacidade na doutrina, enquanto componente dos direitos à personalidade, deu-se em 1890, com a publicação de um artigo escrito por Samuel D. Warren e Louis D. Brandeis[19], intitulado *"The right to privacy"*, o qual tem relevância até mesmo nos tempos hodiernos. A elaboração da obra evidencia as mudanças sociais, políticas e econômicas vividas na época.

Os autores, nesse sentido, afirmam que as fotografias instantâneas e a indústria dos jornais invadiram o recinto privado e a vida doméstica, colocando em xeque alguns elementos da vida privada das pessoas[20], entendendo-se, inclusive, que a privacidade poderia sofrer ataques capazes de gerar desgastes e dores maiores que uma lesão corporal. Partindo desse pressuposto, são analisadas diversas decisões de tribunais ingleses e americanos, deduzindo então a existência de um princípio geral na *common law*, denominado *right to privacy*[21], expresso pela sentença "the right to be let alone", o qual expressa um dever de abstenção.

O direito a ser deixado só, nesse sentido, revela-se extremamente individualista e mesmo egoísta, expresso por uma ausência de interação, comunicação ou percepção dentro de contextos em que tais atos seriam viáveis[22]. Assim, constitui uma conceituação inaugural do direito à privacidade, sendo certo que invocar o isolamento ou a tranquilidade não é o suficiente para tutelar todas as situações em que haja possível violação da privacidade.

---

[16] COSTA JÚNIOR, Paulo José da. **O direito a estar só: tutela penal da intimidade**. 4. ed. São Paulo: Editora Revista dos Tribunais, 2007, p. 11.

[17] DE CUPIS, Adriano. ***Il diritto alla riservatezza existe***. Foro Italiano, IV, 1954, p. 90-97 apud DONEDA, 2006, p. 11.

[18] AULETTA, Tommaso Amedeo. ***Riservatezza e tutela della personalità***. Milano: Giuffrè, 1978, p. 63-64 apud DONEDA, 2006, p. 11.

[19] WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy*. ***Harvard Law Review***. Cambridge, v. 4, n. 5. p. 193-220, dec. 15, 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 22 nov. 2019.

[20] ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do *right of privacy* nos Estados Unidos**. Revista Brasileira de Direito Civil**. Rio de Janeiro, v. 3, p. 8-27, jan./mar. 2015, p. 10. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/107/103. Acesso em: 22 nov. 2019.

[21] Ibidem, p. 11.

[22] SHILLS, Edward. ***Privacy***: its constitution and vicissitudes, law and contemporary problems. Durham: N.C. School of Law, Duke University, 1966, p. 281-306. Disponível em: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3109&context=lcp. Acesso em: 22 nov. 2019.

Nesse sentido, é possível definir o direito à privacidade como "resguardo contra influências alheias"[23], o qual propõe caráter dúplice ao assegurar o direito a estar só e o direito de não ser molestado, exprimindo-se no "direito de o indivíduo ser deixado em paz para viver sua própria vida com o grau mínimo de interferência"[24].

No mesmo sentido, o Supremo Tribunal Federal definiu o direito à intimidade como a "expressiva prerrogativa de ordem jurídica que consiste em reconhecer, em favor da pessoa, a existência de um espaço indevassável destinado a protegê-la contra indevidas interferências de terceiros na esfera de sua vida privada"[25].

Aponta-se, entretanto, que a imprecisão em conceituar a privacidade como "refúgio contra intervenções externas" consiste em não delimitar em qual nível determinada interferência seria considerada razoável ou não, sendo certo que nem todas as interferências são consideradas afrontas à privacidade em igual intensidade.

É correto, ainda, afirmar que o segredo e o sigilo constituem formas de resguardar-se de interferências alheias, todavia, sob uma perspectiva mais restritiva, vez que envolve uma via de acesso individual, tratando-se da ocultação de fatos pessoais[26], de modo a impedir a revelação de informações secretas. Para além disso, o sigilo pode conotar mais do que a privacidade, como ocorre nos casos de sigilo profissional, em que por vezes significa garantia de ordem pública, e nos casos do sigilo bancário, o qual representa um interesse patrimonial, para além da privacidade.

Também é preciso destacar que a maioria dos hábitos de um indivíduo – os livros que lê, os produtos que compra e as pessoas a quem se associa – de modo geral não são segredos, mas ainda assim são considerados assuntos privados[27].

Nesse contexto, a própria Constituição Federal assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem em seu artigo 5º, inciso X; bem como a inviolabilidade do sigilo de correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, resguardadas exceções, conforme o inciso XII do mesmo dispositivo citado. No entanto, é certo que simplesmente o direito de não ser incomodado e os reconhecidos direitos de inviolabilidade, por si só, não são capazes de tutelar a privacidade em todas as

---

[23] LEONARDI, 2011, p. 55.
[24] Ibidem, p. 55.
[25] BRASIL. Supremo Tribunal Federal (2. Turma). **Mandado de Segurança 23.669- DF**. Ministro Celso de Mello. Decisão liminar proferida em 12 de abril de 2000.
[26] LEONARDI, op. cit., p. 62.
[27] LEONARDI, op. cit., p. 66.

situações, uma vez que partem do pressuposto de um sujeito cuja conduta é passiva, no exercício de uma liberdade negativa.

Importa, nesse sentido, estabelecer critérios de proteção à privacidade quando da atuação ativa do sujeito, de modo a exercer sua liberdade positiva ao estabelecer os limites da sua própria esfera privada. Nesse sentido, são estipuladas quatro tendências referentes à noção de privacidade[28], as quais constituem a transição do "direito a estar só" para o direito de manter controle sobre informações próprias; da privacidade ao direito à autodeterminação informativa; da privacidade à não-discriminação; e, por fim, do sigilo ao controle.

Assim, as definições funcionais da privacidade dizem respeito à possibilidade que o sujeito tem de tomar conhecimento, supervisionar, e findar o fluxo de informações a ele relacionadas. O sujeito, nesse contexto, passa a ter papel ativo ao exercer direito de controle sobre suas próprias informações, ao passo que a privacidade deixa de ser simples ausência de conhecimento alheio sobre fatos da vida privada do indivíduo, passando a significar o controle exercido sobre essas informações e dados pessoais[29].

Observa-se, portanto, um enriquecimento da noção técnica e uma ampliação progressiva na denominação de esfera privada. Primeiro, importa destacar que a mera mudança de perspectiva sobre a privacidade, a qual deixa de representar meramente o direito a estar só e passa a ser o direito de controlar informações pessoais, causa forte alargamento no âmbito de proteção jurídica específica, de modo a ampliar o âmbito de situações juridicamente relevantes.

Além disso, a esfera privada não mais limita-se à identificação de um sujeito e o seu âmbito doméstico, mas passa a ser o seu conjunto de ações, comportamentos, opiniões, preferências e informações pessoais. Assim, a noção clássica de privacidade, na qual o sujeito de direitos invocava a sua intimidade a fim de interromper o fluxo de informações e isolar-se, foi substituído pelo controle de circulação de informações, de modo que "privado" tenha deixado de conotar necessariamente o que é secreto, passando a significar o que é pessoal. Nesse sentido, a privacidade passa a ser identificada como "a tutela das escolhas de vida contra toda forma de controle público e estigmatização social"[30].

Para além disso, os desdobramentos de um modelo de estado liberal e a mudança da relação entre o estado e o cidadão já mencionados neste trabalho fizeram com que as informações passassem a ter maior valor, observando-se certo incremento do interesse social

[28] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 97.
[29] LEONARDI, 2011, p. 68.
[30] RODOTÀ, op. cit., p. 92.

na tutela do âmbito privado. Assim, o que inicialmente era tido como interesse exclusivo da classe burguesa, passou a interessar camadas cada vez mais amplas da população. Ao mesmo tempo que o fluxo de informações crescia, os dados pessoais passavam a ocupar posicionamento importante no âmbito da tutela da privacidade.

A utilização de informações pessoais, pelo Estado e por entes privados, quase sempre justificou-se por dois fatores: controle e eficiência[31]. Assim, havia a necessidade de conhecimento da população para fins de eficiência da administração pública, a qual leva à realização de censos e pesquisas, bem como a cessão compulsória de dados da população ao Estado; além da obtenção de dados para fins de controle estatal[32]. Já no tocante aos entes privados, importante frisar a inicial dificuldade na aplicação funcional dos dados, tendo em vista os altos custos do tratamento[33], bem como a dificuldade na coleta. A utilização dos dados fazia-se conveniente para o Estado tendo em vista o seu poder econômico, interesses específicos e a maior escala[34].

O desenvolvimento das tecnologias de informação permitiram, por sua vez, que o tratamento dos dados se desse com menor custo, oferecendo uma nova gama de possibilidades de utilização destas informações. Nesse sentido, Doneda afirma que "a importância da informação aumenta na medida em que a tecnologia passa a fornecer meios para torna-la útil a um custo razoável"[35].

A mudança de perspectiva do sigilo ao controle de informações, bem como o progresso de tecnologias capazes de fomentar o tratamento de dados, colocam em questão um novo e importante componente da tutela da privacidade, o consentimento. Partindo de uma postura ativa do indivíduo, passa a ter grande relevância a sua concordância com a forma de administração de seus dados.

Importa destacar, nesse contexto, a relevância do consentimento informado, o qual evidencia o dever de comunicar de forma clara e em linguagem acessível sobre a forma de tratamento de dados dos usuários em determinada plataforma, em contraposição ao

---

[31] DONEDA, 2006, p. 13.

[32] Não é por acaso que após o 11 de setembro os Estados Unidos da América passaram a compilar dados de pessoas nacionais e estrangeiras de forma massiva; nesse sentido: "One shocking aspect of the increasing convergence of databases since 9/11 is the U.S. government's aggressive acquisition of foreign and domestic databases", conforme a obra: WEBB, Maureen. **Illusions of security**: global surveillance and democracy in the post-11/9 word. City Lights: San Francisco, 2007, p. 86.

[33] Tratamento de dados pode ser definido como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, nos termos do art. 5º, X, da Lei nº 13.709/2018.

[34] DONEDA, 2006, p. 15.

[35] Ibidem, p. 15.

consentimento presumido, que muitas vezes expressa-se pela simples publicação de uma política de privacidade, completamente ineficaz. Assim, nos termos do artigo 4º, 11, do Regulamento Geral de Proteção de Dados[36], consentimento pode ser definido como "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".

O consentimento, nesse âmbito, consiste no exercício da autonomia da vontade, como forma de manifestação livre da vontade individual, para fins de autorizar determinada modificação da sua própria esfera jurídica. Assim, importante destacar que, a depender da índole do sistema em que se insere, os efeitos do consentimento serão distintos. Nesse sentido, Doneda destaca que em um sistema de índole patrimonialista, o consentimento tem condão de lançar os dados pessoais no mercado e oportunizar "a chamada *commodification* dos dados pessoais – sua transformação em uma *commodity*"; já em um sistema em que se confia ao indivíduo a autodeterminação de sua esfera privada, o consentimento é o instrumento por excelência do exercício deste poder[37].

Partindo do pressuposto da autonomia da vontade de cada cidadão, seria admissível que cada pessoa estabelecesse o seu próprio âmbito público e privado. No entanto, deve-se dar especial atenção para a disparidade de poder entre os titulares de dados e seus detentores, trata-se do que Danilo Doneda denomina "assimetria informacional".

O consentimento opera como elemento acessório, sempre ligado a uma situação que o vincula, seja o estabelecimento de um contrato, uma pesquisa ou a inscrição em um processo seletivo. Nesse sentido, a negativa de fornecimento dos dados pessoais, no exercício da autodeterminação, ocasiona a supressão do acesso àquele determinado bem ou serviço, para o qual o fornecimento de dados pessoais consiste aspecto essencial. Além disso, o próprio consentimento ocasiona uma série efeitos desconhecidos pelo titular de dados[38]. Os dois apontamentos aqui feitos suscitam o mito do consentimento[39], no sentido de que geram uma falsa sensação de segurança.

Assim, é correto afirmar que o consentimento consiste no exercício da autonomia da vontade enquanto declaração de vontade válida entre particulares, entretanto, o consentimento ao tratamento de dados pessoais não deve ser conjecturado da mesma forma que

---

[36] UNIÃO EUROPEIA. Parlamento Europeu e Conselho. **Regulamento (UE) 2016/679, de 27 de abril de 2016**. Disponível em: http://data.europa.eu/eli/reg/2016/679/oj. Acesso em: 19 set. 2018.
[37] DONEDA, 2006, p. 372.
[38] Ibidem, p. 373-374.
[39] RODOTÀ, Stefano. **Elaboratori elettronici e controllo sociale**. Bologna: Il mulino, 1973, p. 45-51.

o consentimento negocial se dá. Caso contrário, "o Estado assim teria um falso álibi para não intervir em uma situação na qual sua obrigação seria de agir positivamente na defesa de direitos fundamentais"[40].

Sendo certo que as regras de circulação das informações estão destinadas a incidir sobre a distribuição de poder na sociedade[41], vislumbra-se a necessidade de estabelecer limites ao consentimento individual, tendo em vista a hipossuficiência do titular de dados gerada pelos desníveis de poder nas relações de mercado.

Surge a necessidade de criação de paradigmas mínimos de proteção à privacidade e para a proteção efetiva dos direitos fundamentais, o que será tratado mais adiante.

2.1 Os paradoxos da privacidade

O surgimento das tecnologias da informação levou alguns a crerem que a limitação de determinados contatos sociais cotidianos ocasionaria a redução do controle que a própria sociedade e os meios de vigilância exercem sob o cidadão. Isso ocorreria, por exemplo, em se tratando do teletrabalho, das videoconferências, das compras à distância e das transações bancárias. Nesse sentido chegou-se a afirmar, inclusive que "estas tecnologias servem também para proteger o indivíduo da forma de controle social, que, no passado serviram para vigiar seus comportamentos e para exercer pressões com vistas à adoção de condutas de tipo conformista"[42].

Assim, o surgimento de uma nova esfera privada aliada ao estabelecimento cada vez maior de pessoas nas cidades seria capaz de minimizar os mecanismos de controle exercido face à sociedade. No entanto, o que se observa é o surgimento de uma falsa sensação de proteção, uma vez que novos e primorosos mecanismos de controle foram criados. Nesse sentido, Rodotà afirma: "deterioram-se as tradicionais formas de controle social, cujo lugar é assumido, no entanto, por controles mais penetrantes e globais, tornados possíveis pelo tratamento eletrônico das informações"[43].

É certo que a tecnologia deixou de ser uma situação de fato para ser um vetor condicionante da sociedade e, por consequência, do direito; além disso, estabelece-se que não

---

[40] RODOTÀ, Stefano. **Tecnologie e diritti**. Bologna: Il mulino, 1995, p. 35.
[41] Idem. **A vida na sociedade da vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008, p. 45.
[42] KATZ, J. M. *Public Policy Origins of Telecommunications Privacy and the Emerging Issues, in Information Age*, 10 (1988), p. 173 apud RODOTÀ, 2008, p. 94.
[43] RODOTÀ, 2008, p. 95.

levar em conta essas variáveis significa subtrair o direito do seu próprio tempo[44]. Assim, a tecnologia assume caráter instrumental e utilitarista, como um meio a atingir um fim a ela exterior.

No entanto, alguns autores afirmam a existência de uma falsa sensação de neutralidade da tecnologia, no sentido de que ela pode parecer isenta em primeira análise, mas, uma vez utilizada em favor dos interesses de "usuários privilegiados", deixa de sê-lo. Nesse sentido afirma-se: "(...)a possibilidade de ter, a priori, uma transparência completa do consumidor, através de sistema de cookies e de cibervínculos invisíveis é boa e bem presente e demonstra, claramente, que a tecnologia não é neutra"[45].

Os denominados usuário privilegiados constituem órgãos públicos e grandes empresas privadas, detentores de considerada reserva de infraestrutura informativa, a qual Rodotà julga tratar-se de uma condição permanente inerente ao novo sistema.

Os órgãos públicos, uma vez que evocam para si a titularidade de serviços essenciais ao pleno desenvolvimento da pessoa humana, como a seguridade social, a saúde e educação públicas, e até mesmo o serviço de correios, passam a ter acesso privilegiado a uma série de dados pessoais intrinsecamente ligados à personalidade do indivíduo, principalmente ao que se denomina dados sensíveis. Já as grandes empresas, apesar de nem sempre serem titulares de serviços essenciais, possuem um grande público utilizador do serviço fornecido, o que lhe dá acesso a uma gama enorme de dados, tendo em vista a grande quantidade de pessoas que utilizam o serviço oferecido.

Infere-se que as tecnologias da informação são capazes de trazer maior comodidade e praticidade à vida cotidiana, inclusive, criando uma esfera privada mais abrangente. No entanto, os meios de controle passam a basear-se nos registros e nas informações deixadas no meio virtual, de modo a fragilizar a esfera privada.

Assim, a criação de mecanismos para fomentar o isolamento e a própria privacidade, por meio da tecnologia, são capazes de torná-la frágil e exposta a ameaças. O momento em que a privacidade entra em contradição consigo mesma e/ou produz consequências inesperadas é denominado "o primeiro paradoxo da privacidade"[46]. Nesse sentido, necessária a criação de um aparato jurídico de proteção à privacidade, do qual trataremos mais adiante.

---

[44] DONEDA, 2006, p. 25.
[45] POULLET, Yves apud DRUMMOND, Victor. **Internet, privacidade e dados pessoais**. Rio de Janeiro: Editora Lumen Juris, 2003, p. 07.
[46] RODOTÀ, 2008, p. 95.

É certo que a progressiva relevância dada ao controle de dados significou muito no âmbito de tutela da informação pessoal. No entanto, conforme explanado anteriormente, é preciso destacar que o sigilo e o direito de não ser perturbado não são meramente substituídos, mas complementares aos direitos de controle, acesso e informação dos dados pessoais.

Nesse âmbito é necessário diferenciar uma categoria especial de dados, a qual se denomina dados sensíveis. Nos termos da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), dados sensíveis dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Assim, são tratados como o "núcleo duro" dos dados pessoais, uma vez que recebem atenção especial por dizerem respeito a questões de foro íntimo.

A grande polêmica relacionada aos dados sensíveis diz respeito à possibilidade de, quando postos em circulação, serem utilizados como mecanismo de discriminação, causando danos aos próprios titulares de dados. Assim, o que se percebe é que parte dos dados sensíveis são formados por informações que refletem a tradicional necessidade de sigilo, como é o caso de dados relacionados à saúde, à vida sexual e à determinadas convicções pessoais.

Em contrapartida, a despeito de qualquer aparato jurídico oferecido por um Estado, nada impede que os dados sensíveis sejam divulgados em âmbito público pelos seus próprios titulares. Para além disso, determinados dados sensíveis são naturalmente ligados à vida pública e ao exercício da cidadania em estados democráticos, como é o caso da opinião política e da filiação sindical.

Nesse sentido, visando que a própria esfera pública não seja afetada negativamente, ou ainda, que os dados não sejam utilizados em desfavor dos seus titulares, as informações sensíveis passam a receber forte estatuto de "privado", para que sejam estabelecidos critérios rígidos de circulação e tratamento, os quais se manifestam principalmente pela proibição de coleta por determinados sujeitos (empregadores, por exemplo) e pela exclusão de legitimidade de certas formas de coleta e circulação. À referida ambivalência entre o público e o privado, denomina-se "o segundo paradoxo da privacidade"[47].

O terceiro e último paradoxo da privacidade[48], por sua vez, diz respeito ao acompanhamento das informações pessoais, ainda quando cedidas à terceiros. A "presença de riscos conexos ao uso das informações coletadas", em adversidade à "natural vocação ao sigilo de certos dados pessoais" enseja o direito de manter o controle sobre as próprias informações,

[47] RODOTÀ, 2008, p. 96.
[48] Ibidem, p. 97.

mesmo quando colocadas em circulação, no âmbito de terceiros, bem como de determinar as modalidades de construção da própria esfera privada.

Nesse contexto, a ótica proprietária dos dados pessoais, da qual falaremos mais detalhadamente adiante, é superada pelo direito de "autodeterminação informativa", o qual permite que os titulares de dados tenham controle e acesso sobre suas informações em quaisquer condições, ainda quando sob o poder de terceiros, fortalecendo o direito individual à privacidade e tornando mais transparentes e controláveis os denominados gestores de dados.

2.2 A privacidade enquanto um direito fundamental

Em se tratando da privacidade no âmbito dos direito fundamentais, importa destacar sua exteriorização em diversas declarações internacionais de direitos, após a Segunda Guerra Mundial. A Declaração Universal dos Direitos do Homem, aprovada em 1948 pela Assembleia Geral das Nações Unidas, estabelece que "ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação"[49]. A Convenção Europeia dos Direitos do Homem, de 1950, e a Carta dos Direitos Fundamentais da União Europeia, de 2000, por sua vez, asseguram o "direito ao respeito pela vida privada e familiar".

É bastante claro que as referidas declarações, apesar de consagrarem o direito à privacidade, não especificam o como deve se dar a sua tutela. Assim, superada a tese de que o direito à privacidade limita-se ao "direito de estar só", bem como o critério formal da posse das informações, no sentido de que o sujeito possui autonomia para controlar seus dados ainda que no âmbito de tutela de terceiros, passa-se à análise material da privacidade enquanto um direito fundamental.

Nessa nova ótica, a mudança de perspectiva sobre o titular de dados, que deixa seu posicionamento passivo para assumir postura ativa no que diz respeito à tutela da sua privacidade, faz com que ele assuma posição de vigilante daqueles que detêm os seus dados, tomando grande relevância o seu consentimento informado.

No entanto, por mais minucioso que seja um ordenamento jurídico acerca da privacidade de dados e por mais rigorosa que seja a exigência de consentimento informado por parte do titular desses dados, impossível seria que um sujeito detivesse o monopólio sobre sua

[49] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos do Homem**. [S. l.]: ONU, 1948. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 09 nov. 2019.

própria imagem construída diante da sociedade, em nome de uma suposta tutela de direitos da personalidade.

Apesar da importância da tutela dos dados pessoais, inconveniente seria exigir que toda a sociedade tivesse a mesma percepção de determinada pessoa, a perspectiva que mais lhe agradasse. Isso interferiria em outras liberdades individuais, como a liberdade de pensamento e interpretação de cada sujeito, além de estabelecer uma espécie de censura na mente dos indivíduos[50].

Para além disso, quanto ao âmbito de abrangência, a sociedade da informação, especificada enquanto "sociedade dos serviços", torna cada vez mais frequentes as padronizações e os vínculos internacionais. Assim, duas consequências podem ser observadas: quanto mais serviços tecnologicamente sofisticados são disponibilizados à sociedade, maior a quantidade de informações pessoais relevantes cedidas ao fornecedor de serviços; e, quanto maior a rede de serviços, maior a possibilidade de interconexão entre bancos de dados e de disseminação internacional das informações coletadas.

Atentando-se aos riscos oferecidos pelas novas tecnologias da informação, houveram ocasiões em que cogitou-se limitar a utilização dessa tecnologias, pois eram vistas como uma ameaça não só aos direitos civis, mas também às características gerais do sistema democrático. Nesse sentido a Assembleia Geral da ONU, na resolução 2.450 (XXIII)[51], de 19 de dezembro de 1968 assinalava: "os usos da eletrônica que possam incidir sobre os direitos do cidadão e os limites que deveriam ser previstos para tais usos em uma sociedade democrática".

No entanto, é bastante evidente que qualquer tentativa de limitação às tecnologias da informação restaram frustradas. Nesse sentido, o que se impõe é o estabelecimento de regras de comunicação na chamada sociedade da informação, as quais deverão limitar o tratamento de dados, bem como determinar o poder de controle que o titular exerce sobre eles, além de estipular os casos excepcionais.

A autodeterminação informativa, nesse contexto, constitui justamente o poder de controle do titular de dados, no sentido de proporcionar ao interessado a tutela de sua própria esfera privada, através dos direitos de informação e acesso aos dados pessoais, de transparência das informações, comunicações e regras associadas ao exercício de direitos, de retificação e

---

[50] RODOTÀ, 2008, p. 99.

[51] ORGANISATION MONDIALE DE LA SANTÉ. **Droits de l'homme et progrès de la science et de la technique**. [S. l.]: Organisation Mondiale da la Santé, 1969. Disponível em: https://apps.who.int/iris/bitstream/handle/10665/186511/WHA22_PB-9_fre.pdf;jsessionid=D0A9D21B1684C8D2CAF32855F803FF2B?sequence=1. Acesso em: 22 out. 2019.

apagamento, de oposição e de decisões individuais automatizadas, e, por fim, de limitações[52]. Assim, surge a necessidade do estabelecimento de meios de garantia e proteção contra utilizações indesejáveis das tecnologias da informação.

Fica estabelecida, portanto, a ilegitimidade do tratamento de informações em algumas situações; dentre ela pode-se citar as informações colhidas sem prévio e explícito consentimento do interessado, bem como a solicitação de dados sensíveis por determinados sujeitos, como é o caso de empregadores que solicitam informações referentes à opinião política e sindical do empregado, ou empresas seguradoras que solicitam informações genéticas dos segurados.

A autodeterminação informativa também possui forte relação com o princípio da finalidade, segundo o qual o tratamento de dados deve dar-se com propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com os propósitos previamente estabelecidos[53]. Assim, as informações de um determinado sujeito não devem circular além do âmbito de atuação do órgão que efetuou a coleta dos dados, nem tampouco circular dentro de sua própria estrutura administrativa de forma não esclarecida ao titular nem autorizada por ele.

A violação ao princípio da finalidade, nesse sentido, pode gerar a circulação e o compartilhamento de dados não autorizados; para além disso, a combinação de dados diversos é capaz de elaborar perfis, o que se denomina operações de *matching*, os quais podem gerar formas de discriminação daqueles que não se identificarem com a maioria, de modo a levar à estigmatização dos comportamentos desviantes e a penalização das minorias[54], ou até mesmo de taxativo controle. Nesse sentido Rodotà afirma:

> Ao se privilegiar os comportamentos "conformes" aos perfis predominantes, torna-se mais difícil a criação de novas identidades coletivas, com riscos para a própria dinâmica social e para a organização democrática. Diante disso, deve ser rigorosamente assegurado o "direito de deixar rastros" sem receber por isso nenhuma penalidade[55].

O estabelecimento de meios e garantias de proteção dos dados vem acompanhado de uma série de exceções, como o tratamento de dados sensíveis que, apesar de receber tratamento diferenciado com relação aos demais dados, engloba exceções como, por exemplo,

---

[52] Rol de direitos estabelecidos pelo Regulamento Geral de Proteção de Dados (Regulamento UE 2016/679).
[53] Conceito de princípio da finalidade estabelecido pelo artigo 6º, I, da Lei nº 13.709/2018.
[54] RODOTÀ, 2008, p. 105.
[55] Ibidem, p. 105.

nos casos de relevante interesse público, fomento de pesquisas e a fim de proteger interesses vitais do titular de dados[56].

Assim, tendo em vista a problemática da utilização inadequada de dados pessoais somada às exceções, as quais podem tornar-se forte obstáculo à efetivação dos direitos atinentes à proteção de dados, urge tratar o direito da autodeterminação informativa, no âmbito do direito à privacidade, como direito fundamental.

Nesse sentido, tratando de conflitos entre direitos, a limitação do direito à privacidade será possível somente em se tratando de outro direito fundamental, por meio da regra do sopesamento estabelecida por Robert Alexy. Nesse âmbito de direitos fundamentais estão incluídos relevantes direitos individuais e coletivos (como o direito à informação, a liberdade de imprensa, bem como o direito à saúde), mas também relevantes interesses do Estado (como a justiça e a segurança interna e internacional)[57].

O direito à privacidade enquanto um direito fundamental torna-se relevante em especial quando do tratamento de dados sensíveis, como na solicitação de determinadas informações do empregador ao empregado ou da seguradora ao segurado, conforme mencionado anteriormente, os quais podem ocasionar a dispensa ou não admissão do empregado, bem como recusa à contratação de seguro ou até mesmo o estabelecimento de prêmio excessivamente oneroso ao segurado.

É nesse sentido que o Tribunal Superior do Trabalho editou a súmula nº 443, a fim de reintegrar o empregado dispensado por mera discriminação, em casos de ser portador do vírus HIV ou de doença grave que suscite estigma ou preconceito.

> *Súmula nº 443 do TST* - DISPENSA DISCRIMINATÓRIA. PRESUNÇÃO. EMPREGADO PORTADOR DE DOENÇA GRAVE. ESTIGMA OU PRECONCEITO. DIREITO À REINTEGRAÇÃO - Res. 185/2012, DEJT divulgado em 25, 26 e 27.09.2012. Presume-se discriminatória a despedida de empregado portador do vírus HIV ou de outra doença grave que suscite estigma ou preconceito. Inválido o ato, o empregado tem direito à reintegração no emprego.

Também é nesse sentido que questiona-se a constitucionalidade da Lei nº. 12.654/2012[58], que estabelece a obrigatoriedade da identificação do perfil genético de pessoas

---

[56] Conforme estipulado no artigo 9º, 2 do Regulamento Geral de Proteção de Dados (Regulamento UE 2016/679) e no artigo 11, II da Lei Geral de Proteção de Dados (Lei nº 13.709/18).

[57] Marcel Leonardi estabelece elementos de valoração da privacidade, com a finalidade de auxiliar suposta colisão de direitos fundamentais envolvendo o direito à privacidade. Assim, constituem elementos de valoração positiva do direito à privacidade: a promoção do bem-estar, a criação de espaços para relações de intimidade, o livre desenvolvimento da personalidade, a manutenção do Estado democrático de direito; por outro lado, são elemento de valoração negativa do direito fundamental à privacidade: o isolamento social, a proteção do indivíduo em detrimento da sociedade; a dificultação do controle social; o embaraçamento das relações sociais e comerciais; e, por fim, a interferência na livre circulação de informações. Disponível em: LEONARDI, 2011, p. 113 et. seq.

[58] A lei altera as Leis nº 12.037/2009 (Lei de Identificação Criminal) e nº 7.210/1984 (Lei de Execução Penal), para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências.

condenadas em crimes dolosos praticados mediante violência de natureza grave contra pessoa e em crimes hediondos. O Recurso Extraordinário 973.837, que teve repercussão geral reconhecida por unanimidade, mas ainda não tem decisão meritória, questiona a constitucionalidade da coleta compulsória de dados genéticos de condenados criminalmente para integrar banco de dados de perfis genéticos, invocando o princípio constitucional da não autoincriminação e o artigo 5º, inciso II, da Constituição Federal.

Em consonância com o alegado em sede de Recurso Extraordinário, a doutrina estabelece que as informações genéticas constituem a parte mais dura do "núcleo duro" da privacidade, pois têm caráter estrutural e permanente, fornecendo o perfil mais definido do sujeito, sendo, portanto, a base da ações discriminatórias[59]. Nesse sentido, é certo que a tutela da privacidade está muito além da construção da esfera privada; ela é capaz de influir na construção de vulnerabilidades.

Por outro lado, existem situações nas quais o titular de dados assume o dever de comunicar informações que outrora poderiam ser utilizadas com cunho discriminatório. É o caso, por exemplo, de portadores de doenças sexualmente transmissíveis, que têm o dever de comunicar o fato aos seus parceiros; também é o caso da comunicação de informações genéticas em procedimentos cirúrgicos e hospitalares. Nessas situações, questiona-se, ainda, se poderia o médico ou enfermeiro quebrar o sigilo profissional quando da inércia do titular de dados e ameaça de direitos à terceiros.

Outrossim, discute-se o "direito de não saber" como instrumento de delimitação da esfera privada, mas também como fator de livre construção da personalidade. É nesse sentido que se interpreta a autonomia que um indivíduo tem de não tomar conhecimento de algum traço genético ou de alguma doença grave.

Finalmente, importa destacar o direito ao esquecimento, o qual se exprime pelo "direito de não ser lembrado contra sua vontade"[60] e consiste do apagamento de dados pessoais quando deixarem de ser necessários para a finalidade que motivou a sua recolha ou tratamento, ou quando da retirada de consentimento, da oposição ao tratamento, do tratamento de forma ilícita, e, por fim, do cumprimento de ordem jurídica[61]. O direito mencionado, apesar de não possuir previsão clara e expressa no ordenamento jurídico brasileiro, está incluído no âmbito dos direitos fundamentais, como forma de tutela ao direito à privacidade. Nesse sentido, o

[59] RODOTÀ, 2008, p. 107.
[60] Definição de direito ao esquecimento dado pelo Superior Tribunal de Justiça em 2013, em julgamento do REsp 1.334.097/RJ, referente ao célebre casa do Chacina da Calanderlária.
[61] Conforme artigo 17, 1 do Regulamento Geral de Proteção de Dados (Regulamento UE 2016/679).

enunciado 531 da VI Jornada de Direito Civil do Conselho de Justiça Federal dispõe: "a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento".

O direito à privacidade, nesse sentido, está além do controle sobre as próprias informações e da estipulação de abrangência da própria esfera privada; o direito à privacidade constitui instrumento de tutela da personalidade, sendo certo que o objeto deste direito pode ser identificado no “patrimônio informativo atual ou potencial” de um sujeito.

3 A TUTELA DE DADOS PESSOAIS

Inicialmente, as soluções aos problemas relacionados à proteção de dados concentravam-se em uma esfera individual, relacionada aos problemas de violação da intimidade. Nesse âmbito, os dados são vistos sob uma ótica proprietária bastante simplista, em que a cessão de informação constitui meramente a troca por algum produto ou serviço.

> [...] a motivação ordinária, e consequentemente a estrutura fundamental, da primeira geração de leis sobre a proteção de dados é justamente a sua finalidade de responder às preocupações sobre as violações da intimidade individual que a tecnologia dos computadores poderia determinar[62].

Nesse sentido, a *deregulation* surge como uma opção do Estado, enquanto forma de política pública e no exercício da sua soberania, em proporcionar ao mercado a regulação de uma determinada atividade[63]. Assim, a *deregulation* encontra respaldo naqueles que afirmam que o aparato legislativo sobre proteção de dados constitui um repasse de gastos à iniciativa privada, os quais são tidos como desnecessários, principalmente em tempos de crises econômicas, considerando que os mecanismos de proteção de dados seriam factíveis apenas em momentos de estabilidade social.

Também suportam a *deregulation* aqueles que afirmam que "disciplinas demasiadamente rígidas de circulação transnacional das informações podem causar dificuldades à produção e ao comércio internacional"[64]. Nesse sentido, sugere-se que exista uma capacidade de auto ordenação das novas tecnologias e que a privacidade seja regulada em conformidade com as forças do mercado.

Referido posicionamento teve respaldo principalmente nos Estados Unidos da América, em que a *Federal Communications Commission*, em 1982, sugeriu ao governo "que confiasse a proteção da privacidade apenas ao jogo das regras do mercado"[65]. Destarte, observa-se a proteção da privacidade sob uma ótica estritamente proprietária, na qual a crescente dependência entre fornecimento de informações e uso de serviços, determinada pela difusão da mídia interativa, tornava cada vez mais inviável o direito à privacidade, não havendo o que se falar em proteção de acordo com as leis do mercado.

Assim, é certo afirmar que a disparidade de poder entre o consumidor de serviços informáticos e telemáticos e os seus fornecedores torna completamente descabido invocar o consentimento livre e esclarecido, já tratado anteriormente, para transações que dizem respeito

---

[62] RODOTÀ, 2008, p. 49.
[63] DONEDA, 2006, p. 391.
[64] RODOTÀ, op. cit., p. 51.
[65] RODOTÀ, op. cit., p. 52.

à privacidade, uma vez que "as regras de circulação das informações determinam também, ou sobretudo, formas de redistribuição do poder"[66].

Desse modo, tratar a proteção de dados sob uma ótica puramente mercadológica parece restringir, em muito, o debate; uma vez que o direito à proteção de dados se vê continuamente desgastado ou simplesmente desconsiderado em detrimento da prevalência de uma lógica de mercado.

Em análise aos pontos elencados pelos defensores da *deregulation*, pode-se afirmar que a arguição de que o aparato legislativo acerca da proteção de dados aumenta os custos para as empresas e para a administração pública sugere que alguns direitos fundamentais sejam tratados com prioridade em relação a outros. Nesse sentido, indaga-se se existiria algum direito fundamental de menor magnitude que outros.

É certo que uma demanda para a proteção de dados pessoais não é sentida de forma uniforme por uma sociedade de perfil heterogêneo, isso porque o interesse em sua tutela desenvolve-se somente depois que uma série de outras necessidades básicas sejam satisfeitas. Nesse sentido, a necessidade de estabelecimento de mecanismos de proteção de dados pessoais varia conforme o padrão médio de consumo da população, bem como outros padrões como sua educação e a penetração da tecnologia no cotidiano.

No entanto, ainda que uma parcela carente da população não tivesse interesse direto na tutela de dados pessoais, isso não seria capaz de abolir a importância da tutela dos dados pessoais no âmbito do desenvolvimento dos direitos da personalidade, uma vez que é capaz de atingir a população de forma indireta, enquanto consumidores e trabalhadores, por exemplo.

Tanto a iniciativa privada quanto a administração pública, ao desempenharem suas funções, sujeitam-se a normativas que dizem respeito a proteção e segurança dos trabalhadores, respaldam os interesses dos consumidores e impõe exigências sobre uma conduta ambiental correta. Assim, questiona-se se a negativa de tutela aos dados pessoais não seria trata-los como menos relevantes.

Para além disso, o pretexto de que a regulamentação dos dados seria mais viável em momentos de estabilidade social, econômica e política propõe um aparato frágil de regulação. São nos momentos de crise e instabilidade social que os governos invocam para si a necessidade de maior controle e vigilância sobre a população, assim, seria completamente descabido que nesses momentos os mecanismos de proteção de dados desaparecessem; trata-se

[66] RODOTÀ, 2008, p. 90.

de um aparato de garantia de direitos, o qual não pode ser utilizado de maneira arbitrária pelos governantes.

Em contraposição à *deregulation*, a *regulation* surge como resposta a alguns problemas insurgentes na antiga lógica de mercado[67]; a *regulation,* nesse sentido, consiste na promulgação de um conjunto normativo e de um mecanismo que zela pela sua aplicação. Além disso, a nova lógica possui uma faceta cuja finalidade é corrigir defeitos internos do mercado, e outra que busca corrigir distorções exteriores, os quais decorrem da atividade do mercado, podendo ser citados os interesses dos consumidores, a tutela do meio-ambiente, a saúde pública ou a segurança dos trabalhadores[68].

Assim, surge a necessidade de criar instituições e regulamentos adequadas à nova situação. O tratamento da questão como problemas de violação da intimidade fortalece o âmbito das defesas individuais, no entanto, o posicionamento passivo mostra-se insuficiente diante da gama de abusos que o titular de dados fica sujeito.

A força expansiva da proteção de dados pessoais leva-a a ser vista como uma "continuação por outros meios" da proteção da privacidade, sendo nesse sentido que Carta dos Direitos Fundamentais da União Europeia dedica um artigo à proteção da vida privada e familiar (art. 7º) e outro à proteção de dados pessoais (art. 8º), a fim de estabelecer controle direto dos dados pessoais, possibilitando conduta ativa do titular de dados.

> De sua tradicional definição como "direito a ser deixado só" passa-se, justamente pela influência da tecnologia dos computadores, àquela que constituirá um constante ponto de referência na discussão: "direito a controlar o uso que os outros façam das informações que me digam respeito". Em fase mais recente surge um outro tipo de definição, segundo a qual a privacidade se consubstancia no "direito do indivíduo de escolher aquilo que está disposto a revelar aos outros[69].

Nesse sentido, importa ressaltar que a proteção de dados pessoais se particulariza em relação aos direitos da privacidade. A proteção de dados pessoais, em suma, propõe o tema da privacidade, porém modifica seus elementos; aprofunda seus postulados e toca nos pontos centrais dos interesses em questão.[70]

Conforme mencionado anteriormente, diversas declarações de direitos internacionais consagraram o direito à privacidade enquanto um direito fundamental, sendo as primeiras delas datadas de 1948. No entanto, a proteção de dados pessoais se deu pela primeira vez em 1970, através do Ato de Proteção de Dados do Hesse (Hessiches Datenschutzgesetz).

---

[67] Podem ser citados: falta de concorrência, distribuição de bens públicos, ocorrência de "externalities", mercados incompletos, defeitos de informação, desemprego, inflação e crescimento desiquilibrado, conforme a obra: LA SPINA, Antonio; MAJONE, Giandomenico. ***Lo stato regolatore*** apud DONEDA, 2006, p. 391.

[68] DONEDA, op. cit., p. 392.

[69] RODOTÀ, 2008, p. 75.

[70] DONEDA, op. cit., p. 205.

Para além disso, o constitucionalismo jovem europeu inclui o direito à privacidade de dados dentre os seus direitos assegurados, como é possível observar nas constituições portuguesa, de 1976, e espanhola, de 1978, as quais preveem a utilização da informática, e, no caso da Constituição Portuguesa, uma referência direta à proteção de dados.

Já as recomendações da Organização para Cooperação e Desenvolvimento Econômico de 1980 (também conhecido como *guidelines* da OECD) e a Convenção 108 do Conselho da Europa de 1981 (também conhecida como Convenção de Estrasburgo), constituem documentos de relevância internacional que cuidam da proteção de dados, estabelecendo princípios para o seu tratamento, como correção, exatidão, finalidade, publicidade, acesso individual e segurança, de modo a fomentar a transição do direito à privacidade enquanto a reação à uma violação, para um controle direto do âmbito privado.

Nesse sentido, a União Europeia a fim de assegurar a livre circulação de dados no seu âmbito aprovou a Diretiva 95/46/CE, em 1995, que uniformiza o tratamento de dados entre os países-membro e cuida da proteção de indivíduos em relação ao tratamento de dados pessoais. A legislação também prestou-se ao fomento do comércio interno do bloco econômico, através da redução dos custos das transações de dados.

Já em 2016, foi aprovada a *General Data Protection Regulation* (denominada GDPR; em português, Regulamento Geral de Proteção de Dados), em substituição à diretiva mencionada, passando a vigorar em 2018. A GDPR apresenta avanços em relação à diretiva substituída, no sentido de ampliar direitos dos usuários, bem como na responsabilização das organizações e empresas que realizam o tratamento de dados pessoais, buscando garantir aos titulares um maior controle sobre os dados que lhes dizem respeito.

Aqui cabe ressaltar a diferenciação entre legislações europeias, modelos em proteção de dados enquanto direitos fundamentais, e a legislação norte americana, a qual privilegia o livre fluxo de informações, consagrando o direito à liberdade em detrimento da privacidade de dados, através do que se denomina auto regulação ou auto vigilância (*self-surveillance*)[71].

> Enquanto há quase três décadas o modelo europeu começava a se delinear e logo procurou estruturar o problema em torno dos direitos fundamentais, o enforque norte-americano sempre levou em alta conta a promoção do fluxo de dados, encarando a tutela da privacidade na área como um sistema de ajustes e vedações de práticas abusivas, a serem verificadas quase sempre em concreto, a posteriori[72].

[71] DRUMMOND, 2003, p. 58.
[72] DONEDA, 2006, p. 318.

Em discrepância ao ordenamento europeu, nos Estados Unidos da América o individualismo somado às tradições do *commom law*, sustentado pela técnica de solução de casos pelos precedentes, explicitam a dificuldade de aproximação entre o *"right of privacy"* aos direitos da personalidade[73/74]. Nesse sentido, a proteção de dados pessoais é desenvolvida por meio de uma legislação fragmentada, bastante particularizada, e por vezes distante dos padrões de qualidade estabelecidos nas demais partes do mundo.

Nesse contexto, a legislação europeia, em especial a Convenção 108, de 1981, a Diretiva 95/46 e, mais recentemente, a GDPR, tornaram-se grandes influenciadoras da proteção de dados pessoais em diversos países do globo.

Destaca-se, nesse seguimento, a Argentina e o Uruguai, países latino americanos que possuem legislação específica e de alta complexidade para a tutela de dados pessoais, em níveis de proteção adequados, nos termos estabelecidos pela União Europeia[75]. A Argentina teve sua legislação aprovada em 2000, a qual prevê os direitos dos titulares de dados, bem como estabelece princípios como a finalidade, a legalidade e a exatidão, além da responsabilização pelo tratamento de dados, sanções e medidas de proteção. O Uruguai, por sua vez, teve sua legislação aprovada em 2011, aproximando-se em muito da legislação argentina.

Em contrapartida, por muito tempo a temática foi negligenciada pelo ordenamento jurídico brasileiro, inexistindo regulamentação específica. Somente em 2018 foi sancionado o primeiro diploma legal que trata com exclusividade a proteção de dados no Brasil, porém ainda não se encontra em vigência e vislumbra alguns desafios para a sua aplicação, os quais serão tratado mais adiante.

> No ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada[76].

---

[73] ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do *right of privacy* nos Estados Unidos**. Revista Brasileira de Direito Civil**. Rio de Janeiro, v. 3, p. 8-27, jan./mar. 2015, p. 10. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/107/103. Acesso em: 22 nov. 2019.

[74] Apesar de haver uma identidade linguística entre o *"right of privacy"* e o "direito à privacidade", ambos não podem ser tidos como equivalentes, uma vez que o *privacy* norte-americano evoca uma constelação de situações: "a tranquilidade do próprio lar, o controle sobre informações pessoais, o controle sobre o próprio corpo, a liberdade de pensamento, o controle sobre a vigilância, a proteção da reputação, a proteção contra averiguações e interrogatórios abusivos, o planejamento familiar, a educação dos próprios filhos, o aborto, a eutanásia, entre outros", conforme esclarecido em DONEDA, 2006, p. 264.

[75] Trata-se da análise do nível de proteção oferecido por cada regulamento; mais adiante será debatida a referida chancela dada pela União Europeia.

[76] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010, p. 49.

Assim, tendo em vista a crescente importância dos dados pessoais, expressa pela comissária europeia do consumo, Meglena Kuneva, como "o novo óleo da internet e a nova moeda do mundo digital"[77], e partindo da ótica europeia influenciadora do ordenamento jurídico brasileiro de que a tutela de dados pessoais insere-se dentre os direitos fundamentais, importa pormenorizar como o controle de dados pessoais se desenvolveu ao longo do tempo, como se dá o livre acesso e a liberdade informacional diante de um aparato restritivo de tratamento, bem como as formas de tratamento de dados pessoais e quais são os riscos ligados à sua utilização inadequada.

3.1 O desenvolvimento do controle de dados pessoais

Na atual sociedade da informação, em que a produção de dados supera, em muito, tudo o que a população é humanamente capaz consumir, os poderosos são os detentores de tecnologia e ciência digital. Nesse sentido, tendo em vista que grande parte do que se faz em rede deixa rastros, os quais dizem muito a respeito de cada indivíduo (gostos pessoais, áreas de interesse, convicções religiosas, opiniões políticas, dentre outros), tomam relevância discussões acerca do controle exercido sobre os dados pessoais. Importa, nesse sentido, estabelecer critérios para diferenciação das esferas pública e privada de cada sujeito, bem como assegurar sua autonomia para definir tais limites.

Em que pese a existência de legislações regulamentadoras da privacidade de dados pessoais, mencionadas anteriormente, constata-se certa desproporção entre a "terceira onda" e a falta de instituições jurídicas adequadas para acompanhar as transformações[78]. Assim, é vislumbrada a necessidade de remédios institucionais.

> [...] a nova angústia nasce da consciência da forte defasagem entre a rapidez do progresso técnico-científico e a lentidão com que amadurece a capacidade de controle dos processos sociais que acompanham tal progresso[79].

A obra denominada Grande Irmão, de George Orwell, ilustra uma sociedade onde o aparato de repressão toma conta da sociedade, inexistindo vida privada. É o que se pode observar nos tempos atuais diante de câmeras de vigilância, reconhecimento facial a metros de distância, cadastros cada vez mais complexos nos sistemas de inteligência dos países.

> Assediados por computadores, espiados por olhos furtivos, filmados por telecâmeras invisíveis. Os cidadãos da sociedade da informação correm o risco de parecer homens

[77] Discurso proferido na mesa redonda sobre coleta de dados, direcionamento e perfilação, em Bruxelas, 31 de março de 2009.
[78] RODOTÀ, 2008, p. 57.
[79] Ibidem, p. 42.

> de vidro: uma sociedade que a informática e a telemática estão tornando totalmente transparente. [80]

Nesse sentido, urge que o cidadão não seja mais visto como mero fornecedor de dados, devendo exercer controle sobre eles. Acerca do exercício de controle de dados, cumpre destacar que a proposta de um poder autônomo de controle, expresso por um direito de acesso individual, foi o que mais recebeu respaldo inicialmente.

No entanto, Rodotà afirma ser inviável pensar em uma via de controle individual, a qual se restrinja apenas e tão somente em assegurar ao cidadão a exatidão e o uso correto das informações, uma vez que o fornecedor de dados constitui parte hipossuficiente, incapaz de impedir determinados abusos do poder público ou até mesmo das grandes corporações. Nesse sentido, para que o controle funcione como mecanismo de equilíbrio dessa nova estrutura de poder, é necessário que a atenção seja deslocada dos meios de reação social para instrumentos de controle social.

Outra razão para que o controle de dados não se concentre apenas a esfera individual de cada sujeito é o fato das informações pessoais ocuparem uma posição que vai além de um "recurso" informativo, ou um atributo do sujeito. É inegável que as tecnologias interativas sejam capazes de associar dados pessoais a fim de criar uma nova mercadoria. As informações, uma vez utilizadas em conjunto, exprimem opiniões e preferências pessoais, funcionando como mercadoria para as grandes empresas e órgãos públicos.

> E é significativo que justamente neste ponto se encontrem, cada vez mais, normas relacionadas às sondagens de opinião, que constituem hoje a fronteira mais controvertida e sensível no que diz respeito à expressão das preferências dos cidadãos. E já que essa preferências também podem abranger escolhas significativas para a organização social e política, uma vez mais a disciplina da coleta e do tratamento das informações demonstra que não pode ser reduzida somente ao seu valor individual[81].

Assim, determina-se que o controle de dados seja realizado não somente da perspectiva individual, mas que seja um controle de mão dupla, pelo qual o controlado torna-se o controlador. O simples direito de acesso aos bancos de dados (públicos e privados) é capaz de fazer com que o responsável tenha uma conduta mais transparente e correta com relação aos dados que armazena.

Nesse sentido, o direito de acesso, retificação, atualização e até mesmo esquecimento dos dados significam uma forma de o indivíduo fiscalizar e autotutelar o tratamento dos seus dados pessoais.

> A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser

[80] RODOTÀ, 2008, p. 08.
[81] Ibidem, p. 46.

> administrado com procedimentos que permitam a este indivíduo ter o direito de participar na decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contidas. Qualquer registro, divulgação e utilização de informações fora destes procedimentos não devem ser permitidas, por consistirem em uma prática desleal, a não ser que tal registro, utilização ou divulgação sejam autorizadas por lei. [82]

O direito ao controle de dados, nesse sentido, não deve ser visto como "inimigo da sociedade aberta"[83], nem como elemento hostil à ação pública, mas como o exercício regular do direito de autodeterminação informativa do indivíduo, para que ele seja capaz de determinar quais dados pessoais serão disponibilizados a terceiros e em qual proporção, para qual fim, sob quais condições.

Para além da faceta de controle individual, a qual exige que haja consentimento informado para a coleta e tratamento de informações, faz-se necessária a existência de uma autoridade fiscalizadora capaz de zelar pelo cumprimento da legislação de proteção de dados, a qual se deve atribuir poder geral de vigilância.

Importa destacar, assim, a necessidade de que tal instituição administrativa seja independente do poder público. Primeiramente porque o próprio poder público é detentor de uma vasta gama de dados, assim, a função de vigilância implica a intervenção no âmbito de bancos de dados do próprio governo. Faz-se essencial que esta entidade de vigilância encontre-se fora das estruturas administrativas e burocráticas tradicionais do Estado e funcione de maneira diversa dos entes controlados, uma vez que a própria burocracia é fomentadora da coleta de dados. E, em segundo lugar, para que a atuação da própria entidade seja dotada de imparcialidade e credibilidade. Nesse sentido, a independência visa afastar ao máximo a atuação dos entes reguladores da influência de poderes estatais já constituídos[84].

Nessa perspectiva, são estabelecidos preceitos com a finalidade de assegurar a independência e isenção da autoridade fiscalizadora, dentre os quais podem ser citados: a necessidade de mecanismos de nomeação de seus membros, de modo a limitar a discricionariedade (estabelecendo, por exemplo, determinada formação ou atuação profissional), determinar a incompatibilidade de sua atuação com outras atividades (atuais ou mesmo pregressas), e, por fim, limitar o cargo temporalmente; bem como estabelecer a ausência de ingerência sobre os atos da autoridade, através da instauração desses órgãos fora de uma posição hierárquica em relação ao governo[85].

---

[82] EUA, *Records, computers and the rights of citizens*. Report of the Secretary's Advisory Comitee on Automated Personal Data Systems, 1973 apud DONEDA, 2006, p. 214.
[83] POPPER, Karl. ***La società aperta e i suoi nemici***, vol. 2, Roma, 1973-74 apud RODOTÀ, 2008, p. 48.
[84] DONEDA, 2006, p. 393.
[85] Ibidem, p. 393-394.

Assim, enquanto os defensores da ideia de vigilância através da lógica de mercado negam a importância de um órgão público controlador, os oponentes sugerem que esta instituição exerça controle geral e continuado, desempenhando funções como a de fiscalização do controle, tratamento e circulação de dados, de órgão consultivo, de resolução e atenuante de conflitos, e, por fim, de poder normativo autônomo; ao passo que sujeitos individuais ou coletivos, em sede de controle difuso, exerçam vigilância eventual e fragmentada.

Ainda assim, uma vez reconhecida a necessidade de controle de dados, faz-se necessário definir se haverá tratamento diverso para dados eletrônicos e manuais, se existirá diferenciação entre o tratamento de dados da pessoa física e da pessoa jurídica, se, a depender do sujeito controlador, as regras serão mais ou menos rígidas, bem como a forma como funcionará a circulação transnacional de dados.

No que diz respeito à diferenciação no controle de dados automatizados ou manuais, é certo que constitui medida capaz de gerar certa preferência aos que pretendem esquivar-se das exigências positivadas; assim, muito mais importante do que o critério de tratamento, automático ou não, é a finalidade da coleta, sendo, portanto, irrelevante a diferenciação entre dado automatizado ou manual para que seja submetido ao controle.

Quanto ao titular de dados, tem-se que seria injusto estabelecer qualquer distinção na tutela dos interesses da pessoa física para a pessoa jurídica, além de gerar uma certa discriminação. Assim, irrelevante qualquer diferenciação nesse sentido.

Já a criação de exceções à regra a que estão submetidos os bancos de dados, devem ser analisadas de maneira mais crítica. As exceções são abertas em se tratando de alguns sujeitos específicos (como a polícia, os serviços secretos, ou a magistratura), assim, necessário que haja "uma efetiva e estreita relação entre informações coletadas e a necessidade de manutenção do sigilo"[86]. Para além disso, importante frisar que os referidos órgãos não estão submetidos a uma excepcionalidade absoluta; é preciso que haja razoabilidade nessa análise, principalmente a fim de se buscar o "controle de mão dupla" já mencionado, bem como evitar um sentimento de frustração diante de exceções absolutas no tratamento de dados, sejam eles sensíveis ou não.

Quanto à circulação transnacional de dados, importa destacar que as legislações individuais de cada Estado não devem ser examinadas de forma isolada, uma vez o estabelecimento de relações entre países diversos, sejam essas relações negociais ou não, implicam na circulação de dados. Nesse sentido, partindo do pressuposto de que nem todos os sistemas legais consideram a proteção de dados um direito fundamental, exige-se uma

[86] RODOTÀ, 2008, p. 65.

responsabilidade especial por parte daqueles que o fazem. É comum, nesse sentido, que um país cuja tutela de dados seja menos rigorosa comprometa o ordenamento de países com os quais se relaciona, em especial países que se propõe a estabelecer tutela rígida de dados pessoais.

É nessa perspectiva que fala-se em "paraísos de dados", analogamente aos paraísos fiscais, os quais consistem em territórios onde a tutela específica de dados é enfraquecida ou até mesmo inexistente, assim, prestam-se para realização de operações que são consideradas ilícitas no local de origem das informações.

Tendo em vista a relevância da tutela de dados já explicitada neste trabalho, bem como ser inimaginável que os países e organizações internacionais relacionem-se sem que ocorra circulação de dados, alguns autores são convictos ao afirmarem que a convergência dos modelos de proteção de dados pessoais seja um caminho certo e natural no desenvolvimento da temática[87]. Nesse sentido, a transferência internacional de dados pessoais seria possível desde que presentes adequação dos diversos ordenamentos jurídicos, consentimento do titular de dados, e cláusulas-padrão de circulação.

A questão ora suscitada foi pacificada no âmbito da União Europeia, uma vez que o Regulamento Geral de Proteção de Dados estabelece que todos os países membros deverão manter nível de proteção de dados equivalente entre si, para que seja garantida a livre circulação de dados[88], além disso, os Estados membros possuem autonomia para legislar acerca das formas de tratamento ou até mesmo dos dados sensíveis, desde que não contrariem o Regulamento.

Além disso, em se tratando de circulação de dados para países terceiros e organizações internacionais, exige-se a garantia de que o nível de proteção exigido pelo referido regulamento seja mantida; nesse sentido dispõe a consideração preliminar nº 101:

> A circulação de dados pessoais, com origem e destino quer a países não pertencentes à União quer a organizações internacionais, é necessária ao desenvolvimento do comércio e da cooperação internacionais. O aumento dessa circulação criou novos desafios e novas preocupações em relação à proteção dos dados pessoais. Todavia, quando os dados pessoais são transferidos da União para responsáveis pelo tratamento, para subcontratantes ou para outros destinatários em países terceiros ou para organizações internacionais, o nível de proteção das pessoas singulares assegurado na União pelo presente regulamento deverá continuar a ser garantido, inclusive nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional em causa para responsáveis pelo tratamento, subcontratantes desse país terceiro ou de outro, ou para uma organização internacional. [...]

Baseando-se no trecho acima citado, o artigo 44 do Regulamento estabelece o princípio geral das transferências, prezando pelo "nível de proteção das pessoas singulares", e o artigo 45 estabelece os critérios avaliadores do nível de proteção de países terceiros e

[87] DONEDA, 2006, p. 312.
[88] Consideração preliminar nº 10, do Regulamento (UE) 2016/679.

organizações internacionais, prevendo que um ato de execução assegure a adequação do país ou organização analisada, sendo certo o estabelecimento de reavaliações periódicas.

Nesse sentido, questiona-se se a imposição de critérios para circulação de dados ao exterior não seria uma forma indireta de obter eficácia extraterritorial da própria normativa europeia, ou até mesmo se não se trata de uma interferência na soberania de países terceiros[89].

Destaca-se, no entanto, que a "decisão de adequação" referida acima não é requisito absoluto para a circulação transnacional de dados, uma vez que existem causas derrogantes, previstas no artigo 49 do Regulamento[90], entre elas o consentimento explícito do titular de dados à transferência prevista; a finalidade de satisfazer celebração ou execução de um contrato, celebrado no interesse do titular dos dados, entre o responsável pelo seu tratamento e outra pessoa singular ou coletiva; por importantes razões de interesse público; quando for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial; para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento; dentre outros.

Por fim, faz-se urgente compreender que a noção de proteção de dados extrapola problemas ligados à tutela da intimidade individual, sendo necessário construir uma noção mais completa, de modo a estabelecer "critério de base para a legalidade da ação pública"[91], uma vez que o poder público evoca para si a responsabilidade de editar leis e criar um aparato de proteção de dados pessoais.

Ocorre, assim, uma união entre as esferas pessoais e políticas, uma vez que a proteção de dados não diz respeito apenas e tão somente à tutela da intimidade das pessoas, mas passa a ter grande valia para os chamados usuários privilegiados. Partindo do pressuposto de que o controle de dados deve se dar em uma via de mão dupla, necessário discutir como se dá esse controle e como ocorre a instrumentalização da liberdade informacional.

3.2 Direito de acesso aos dados pessoais e liberdade informacional

O livre acesso aos dados constitui um princípio no âmbito da proteção de dados pessoais, pelo qual o indivíduo deve ter acesso às suas informações armazenadas em um banco de dados, podendo obter cópias destes registros[92].

---

[89] DONEDA, 2006, p.314/315.
[90] Regulamento (UE) 2016/679.
[91] RODOTÀ, 2008, p. 44.
[92] Fair Information Principles. Department of Homeland Security, 2008 apud DONEDA, 2010, p. 46.

Assim, após este acesso e de acordo com o princípio da qualidade, pelo qual os dados armazenados devem ser fieis à realidade, atualizados, completos e relevantes, 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[93].

O livre acesso, nesse sentido, constitui muito mais do que o direito a ser informado, trata-se do direito de ter acesso a informações públicas e privadas, significando a negação da ideia de intangibilidade dos bancos de dados, bem como a materialização de um controle difuso exercido diretamente pelos interessados.

Nesse sentido, encontra-se diretamente relacionado à transparência da atividade de serviços públicos e privados, sendo capaz de coibir as empresas e a administração pública a cumprirem a legislação de forma espontânea, procedendo-se de modo a concretizar o controle por via de mão dupla.

Assim, é correta a afirmação de que o princípio do livre acesso possibilita o alcance de dados pessoais e anônimos, mas também aumenta a transparência global da ação pública. Ademais, permite a verificação do grau de desenvolvimento de um processo decisório, bem como a participação nesse processo, e, por fim, a intervenção na gestão de determinados sistemas. Nesse sentido, aumenta-se a possibilidade de exercício do controle difuso por parte dos cidadãos, em especial nas questões de âmbito público, bem como a capacidade de intervenção nos processos decisórios e de gestão, principalmente em âmbito local.

Para além disso, o próprio direito de acesso encontra alguns empecilhos para alcançar efetividade, dentre os quais podem ser citados a falta de informação, os custos do acesso e a disparidade de poder existente entre o titular de dados e seu gestor, seja ele público ou privado. Nesse sentido, sugere-se que o direito de acesso individual seja "'integrado' pela presença de um sujeito coletivo"[94], podendo ser sindicatos, associações civis e associações de tutela dos consumidores, por exemplo.

> O direito de acesso torna-se desta forma a face dinâmica de um direito à informação que pode se concretizar eficazmente através da iniciativa direta de indivíduos ou grupos. Logo, estamos diante de um instrumento capaz de determinar formas de redistribuição de poder[95].

Importa destacar, nesse contexto, que o surgimento das legislações que dispõe acerca da proteção de dados é concomitante ao surgimento das "leis de acesso à informação",

[93] DONEDA, 2010, p. 46.
[94] RODOTÀ, 2008, p. 68.
[95] Ibidem, p. 73.

segundo as quais o poder público fica obrigado a prestar informações por ele produzidas ou custodiadas a qualquer pessoa, física ou jurídica, sem necessidade de motivação e de forma gratuita.

É certo que existe limitação na divulgação dessas informações, como a divulgação de dados pessoais em titularidade de entes públicos e a divulgação de informações consideradas sigilosas por autoridades ou por força de lei, no entanto, tais leis prestam-se à transparência ativa das entidades públicas. Assim, é bastante claro que o direito de livre acesso não diz respeito somente à tutela de interesses individuais.

3.3 Formas de tratamento de dados e sua utilização inadequada

Anteriormente já foram apontados inconsistências no tratamento dos dados pessoais como mera mercadoria. Neste tópico demonstrar-se-á como o tratamento reducionista dessa questão pode gerar consequências negativas.

> [...] a disciplina da circulação das informações pessoais tem sido considerada unicamente em sua dimensão proprietária, tratando-se tais informações como propriedade exclusiva do interessado, que pode livremente negociar sua cessão. Assim, abandona-se totalmente a outra dimensão, ligada à consequências sociais e às consequências para o próprio interessado, da circulação de determinadas categorias de informações pessoais e de informações coletadas para finalidades específicas: problema este que deve ser enfrentado considerando-se valores e interesses diversos daqueles puramente proprietários[96].

Nesse contexto, Rodotà afirma que as novas mídias constituem canais para o fornecimento de bens e serviços, baseados em uma troca de informações cada vez mais consistente. Assim, nessa nova configuração, as tecnologias interativas são capazes de criar novos e significativos contextos. O que outrora era tratado apenas como "recurso" ou "bem" fundamental da sociedade, uma vez associado a novas informações, passa a ser uma "mercadoria", tendo em vista que o mercado é capaz de associar dados diversos sobre uma mesma pessoa a fim de traçar o perfil do indivíduo.

Inicialmente, importa frisar que o advento da informática possibilitou mudanças significativas na própria forma de tratamento dos dados. A primeira mudança, mensurada quantitativamente, diz respeito ao incremento da quantidade de informação que poderia ser processada, ou seja, o poder de processar mais dados em menos tempo. Outra mudança, de âmbito qualitativo, diz respeito à aplicação de novos métodos no tratamento de dados, como os algoritmos, a fim de tornar as informação mais valiosas e delas extrair utilidade diversas[97].

---

[96] RODOTÀ, 2008, p. 76.
[97] DONEDA, 2006, p. 172.

Nesse sentido, à medida que a tecnologia desenvolve-se, que a produção e o processamento de dados multiplicam-se, e que o tratamento se dá com análise qualitativa de dados, mais dificultoso é invocar o direito de privacidade.

> Graças ao desenvolvimento dos meios de armazenamento e processamento de dados, cresceria exponencialmente o custo para se manter uma informação em segredo; a privacidade ficaria mais custosa, à medida que a utilização de dados pessoais se torna mais econômica e acessível[98]

Assim, no que diz respeito ao tratamento qualitativo de dados, importa expor algumas da técnicas utilizadas, bem como os seus efeitos.

A primeira delas, nomeada *profiling*, consiste na análise de dados de indivíduos ou de grupos com o auxílio de métodos estatísticos e técnicas de inteligência artificial, com o fim de obter uma "metainformação", que consiste em uma síntese de hábitos, preferências pessoais e outros registros da vida da pessoa analisada. Nesse sentido, o resultado pode ser utilizado para traçar tendências comportamentos e decisões futuras[99].

A técnica pode ter diversas aplicações, seja em âmbito público, no 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, ou em âmbito privado, com o envio seletivo de mensagens publicitárias de um produto apenas para seus potenciais consumidores[100].

Importa destacar que quando da utilização desta técnica, o perfil virtual de determinada pessoa passa a confundir-se com a realidade material, de modo que o perfil eletrônico passe a ser a única personalidade visível a outras pessoas. Assim, as técnicas de previsão de padrões de comportamento tendem a levar a uma diminuição da esfera de liberdade do indivíduo, uma vez que pautam-se em uma personalidade virtualmente construída e, por consequência, não considera eventuais mudanças de opinião, de modo a reduzir a liberdade de escolha do sujeito.

Outra técnica de tratamento de dados pode ser denominada *data mining*, a qual "consiste na busca de correlações, recorrências, forma, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxílio de instrumentos estatísticos e matemáticos"[101]. Dessa forma, extrai-se valor de uma gama enorme de dados em estado inalterado e não classificado. Nesse sentido quanto maior a quantidade de informações em

---

[98] PARDOLESI, Roberto. ***Dalla rizervatezza alla protezione dei dati personali****: uma storia di evoluzione e discontinuità* apud DONEDA, 2006, p. 173.
[99] DONEDA, op. cit., p. 173.
[100] DONEDA, op. cit., p.173-174.
[101] BOURCIER, Daniele. ***De l'intelligence artificielle à la personne virtuelle****: émergence d'une entité juridique?*, p. 75 apud DONEDA, op. cit., p.176.

"estado bruto", maior a possibilidade de obter informações relevantes a partir da aplicação dessa técnica.

Assim, por óbvio, a aplicação do *data mining* depende de uma grande capacidade de armazenamento de dados e, tendo em vista a redução dos custos de armazenamento, conclui-se que a técnica mencionada ocasiona uma devastadora compilação de dados por tempo indeterminado, ainda que seja de informações que, a priori, não possuem carga valorativa. Nesse sentido, passa-se do paradigma do esquecimento para o paradigma da memória[102].

> Hoje, com episódios de nosso passado sendo cada vez mais armazenados em arquivos de computadores, a possibilidade de 'começar de novo' está se tornando sempre mais difícil. A noção cristã de redenção é incompreensível para o computador[103]

Nesse sentido, aponta-se a utilização do anonimato e de pseudônimos como a fruição das liberdades fundamentais, como forma de relacionar-se sem sofrer as consequências das pressões sociais e o risco de preconceito.

Destaca-se, ainda, que as técnicas mencionadas "podem provocar um distanciamento entre a informação conscientemente fornecida pela pessoa e a utilidade na qual ela é transformada"[104]. Assim, cumpre destacar a diferenciação entre "informação de base", que provem diretamente de uma pessoa, e "informação resultado", a qual consiste no resultado da aplicação de um método de tratamento à informação de base, em busca de alguma utilidade; nesse sentido, o processo de transformação da informação base em informação resultado denomina-se secundarização da informação.

Nesse contexto, estipula-se que os dados pessoais passam a ser os intermediários entre a pessoa e a sociedade, sendo "justamente isto que terá como efeito a perda de controle da pessoa sobre o que se sabe em relação a si mesma – o que, em última análise, representa uma diminuição na sua própria liberdade"[105].

Diante do exposto, é certo que nenhuma informação tem valor por si mesma, mas somente se analisada diante de determinado contexto, diante da finalidade a se presta, ou tendo em vista as demais informações às quais se associa.

> As inovações contidas em lei e códigos de auto-regulamentação derivam sobretudo do fato de que os meios interativos modificam a capacidade de coleta das informações, instituindo uma comunicação eletrônica contínua e direta entre os gestores dos novos serviços e seus usuários. Assim se torna possível não só um controle mais direto do comportamento dos usuários, como também a identificação precisa e atualizada de certos hábitos, inclinações, interesses, preferências. Daí decorre a possibilidade de uma série de usos secundários dos dados, na forma de "perfis" relacionados aos

---

[102] DONEDA, 2010, p. 34.
[103] Vance Packard, em depoimento ao *Subcommittee of the committee on government operations. House of Representatives* apud DONEDA, 2006, p.178.
[104] DONEDA, 2006, p. 180-181.
[105] Ibidem, p.181.

> indivíduos, famílias, grupos. Trata-se de uma nova "mercadoria" cujo comércio pode determinar os tradicionais riscos para a privacidade: mas pode, sobretudo, modificar as relações entre fornecedores e consumidores de bens e serviços, reduzindo a autonomia destes últimos de tal forma que pode chegar a incidir sobre o modelo global de organização social e econômica.[106]

Os titulares de dados, visando esquivarem-se do infortúnio ocasionado pela cessão das informações, que não necessariamente é a ciência dos métodos de tratamento de dados e seus efeitos, mas simplesmente o bombardeio de anúncios e ligações, passam a fornecer dados parcialmente corretos ou até mesmo falsos, numa tentativa de autodefesa, principalmente quando inexistente a possibilidade de consequências negativas a partir daquela omissão.

Para além disso, se por um lado traçar o perfil dos titulares de dados permite uma melhor percepção das propensões individuais e coletivas, de modo a atender as necessidades com maior tempestividade e assertividade, gerando cada vez mais serviços particularizados, por outro pode reduzir a capacidade de inovações, gerar discriminações do que não identifica-se com a maioria, bem como restringir o poder de escolha, constituinte do livre mercado e valor fundamental constitucional, e gerar obstáculos ao livre desenvolvimento da personalidade individual, de modo a imobilizar o sujeito em perfis historicamente determinados.

> (...) dá-se início a um mecanismo que pode bloquear o desenvolvimento daquela comunidade, solidificando-a no seu perfil traçado em uma situação determinada. Por outro lado, penalizam-se os poucos que não correspondem ao perfil geral, iniciando-se um perigoso processo de discriminação das minorias. A "categorização" dos indivíduos e grupos, além disso, ameaça anular a capacidade de perceber a nuances sutis, os gostos não habituais[107].

Existem, ainda, situações em que a coleta de dados pessoais não é solicitada pelo fornecedor de serviços, mas consequência do próprio fornecimento. Assim, observa-se uma correlação entre serviços prestados e informações coletadas, ocasião na qual assume papel importante o princípio da finalidade, segundo o qual a legitimidade da coleta e da circulação das informações ficam subordinadas ao uso primário para o qual foram destinadas.

Nesse contexto, o princípio da finalidade serve de instrumento para coibir a elaboração de perfis, individuais ou coletivos, através da combinação de dados que podem gerar formas de severa discriminação ou de restringente controle[108]. Portanto, essencial que se invoque o mencionado princípio para que sejam respeitadas a finalidade comunicada ao interessado anteriormente à coleta, seu tempo de conservação, além dos critérios de circulação dos dados e transferência a terceiros.

---

[106] RODOTÀ, 2008, p. 62.
[107] Ibidem, p. 83.
[108] Ibidem, p. 104.

Nesse seguimento, o princípio da finalidade constitui elemento essencial para impedir que os dados coletados sejam arbitrariamente compartilhados em contrariedade ao propósito com que foram coletados, em âmbito nacional ou internacional, público ou privado, constituindo uma tentativa de restringir coligações entre bancos de dados.

É nesse sentido que se refere a outra consequência diretamente relacionada à utilização inadequada de dados, a denominada "globalização do universo informático", que consiste na circulação de informações entre setores e até mesmo entidades diferentes. Nesse contexto, o alerta que se faz é justamente com relação ao descumprimento do princípio da finalidade.

Outra forma de utilização inadequada de dados é bastante típica e diz respeito à utilização de dados sensíveis[109] a fim de discriminar o titular. Inicialmente, cumpre ressaltar que a diferenciação dos dados sensíveis presta-se a um tipo de tutela mais específica e rigorosa, tendo em vista que os dados sensíveis são considerados o "núcleo duro" dos dados pessoais. Assim, estabelece-se que os dados sensíveis possuem "potencialidade maior de causar ofensa aos direitos fundamentais, não somente no tocante ao direito à intimidade, mas, especialmente ao princípio da igualdade"[110].

No entanto, é incorreto afirmar que somente a utilização inadequada dos dados sensíveis seria capaz de expor um indivíduo a discriminações. Importa pontuar, nesse sentido, a possibilidade de aplicação das técnicas neste tópico mencionadas a dados "não sensíveis", com a finalidade de atender interesses diversos. Assim, a utilização inadequada de dados pessoais em geral pode vir a ter utilização discriminatória ou perigosa. Além disso, a própria esfera individual pode ser atingida simplesmente pelo fato de pertencer a um grupo traçado com um perfil negativo, por meio de dados não necessariamente sensíveis.

Nesse âmbito, importa destacar a discriminação de consumidores em âmbito privado, através da utilização de sua localização geográfica, a qual não se enquadra no rol dos dados sensíveis. As formas discriminatórias consagraram-se como *geo pricing*, que consiste na diferenciação dos preços de acomodações, a depender da localização geográfica do comprador, e *geo blocking*, que trata da negativa de oferta de vagas. O exercício dessas atividades consiste prática abusiva, além de ocasionar verdadeiro desequilíbrio no mercado e nas relações de consumo.

---

[109] Tidos como informações sobre raça, credo político ou religioso, opções sexuais, histórico médico ou dados genéticos de um indivíduo, com potencial utilização discriminatória.

[110] LIMBERGER, Têmis. **O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais**. Porto Alegre: Livraria do advogado editora, 2007, p. 203.

Assim, destaca-se que recentemente o Departamento de Proteção e Defesa do Consumidor (DPDC), órgão do Ministério da Justiça, condenou uma empresa brasileira ao pagamento de multa milionária por diferenciação de preço de acomodações e negativa de oferta de vagas, quando existentes, de acordo com a localização geográfica do consumidor, sem que esse tenha dado seu consentimento esclarecido ou que sequer tivesse ciência da utilização dos seus dados. No caso em tela foi comprovado que houve discriminação da empresa com consumidores por conta da etnia e localização geográfica.

> EMENTA: PROCESSO ADMINISTRATIVO. CONSUMIDOR. OFENSA À LIBERDADE DE ESCOLHA NAS CONTRATAÇÕES, PELOS CONSUMIDORES. DIFERENCIAÇÃO DE PREÇO DE ACOMODAÇÕES E NEGATIVA DE OFERTA DE VAGAS, QUANDO EXISTENTES, DE ACORDO COM A LOCALIZAÇÃO GEOGRÁFICA DO CONSUMIDOR. TÉCNICAS DE GEO PRICING E GEO BLOCKING. APLICAÇÃO DE SANÇÃO DE MULTA NO VALOR DE R$ 7.500.000,00 (SETE MILHÕES E QUINHENTOS MIL REAIS) [111].

Por fim, destaca-se a utilização inadequada de dados pessoais no âmbito público, como forma de promover políticas públicas ou até mesmo manipulação das massas.

Na primeira situação mencionada, que diz respeito à utilização de dados como forma de promoção de políticas públicas, cita-se o ocorrido na Colômbia, em que houve o fornecimento de dados da população colombiana a uma empresa norte-americana denominada *Choicepoint*[112], a qual por sua vez, vendeu-os ao governo dos Estados Unidos da América, que os detém com a finalidade de favorecer as operações antidrogas no país através do rastreamento de fluxos financeiros suspeitos[113]. No caso em tela, observa-se que a previsão constitucional de tutela de dados pessoais não foi o suficiente para conter a comercialização de dados de 31 milhões de colombianos, correspondente a 78% da população total do país à época.

No que diz respeito à utilização inadequada de dados pessoais com a finalidade de manipular massas, pode-se citar um acontecimento em voga, recente e polêmico, que envolve as últimas eleições norte-americanas. Nesse sentido, as campanhas eleitorais do presidente eleito nos EUA, Donald Trump, supostamente teriam se beneficiado da coleta imprópria de dados pessoais realizada através de um *"quiz"* no *Facebook*.

A coleta teria se dado da seguinte forma: usuários conectaram-se ao *quiz* e deram livre acesso, sem consentimento livre e esclarecido, aos seus dados pessoais e de todos os seus

---

[111] BRASIL. **Nota técnica 92/2018**. Brasília, DF: Ministério da Justiça e Segurança Pública, 2018. Disponível em: http://www.cmlagoasanta.mg.gov.br/abrir_arquivo.aspx/PRATICAS_ABUSIVAS_DECOLARCOM?cdLocal=2&arquivo=%7BBCA8E2AD-DBCA-866A-C8AA-BDC2BDEC3DAD%7D.pdf. Acesso em: 13 nov. 2019.

[112] Também há registros que essa mesma empresa tenha comprado os dados de toda a população eleitora do México e tenha os vendido aos EUA, bem como de demais países latino-americanos, como Venezuela, Costa Rica, Guatemala, Honduras, El Salvador, Nicarágua e Argentina; confira-se em WEBB, Maureen. **Illusions of security**: global surveillance and democracy in the post-11/9 word. City Lights: San Francisco, 2007, p.89/90.

[113] DONEDA, 2006, p.307/308.

amigos na rede, resultando na coleta de dados de 87 milhões de pessoas, usuários da rede social *Facebook*. Assim, os dados coletados em massa teriam sido fornecidos a uma empresa denominada *Cambridge Analytica*, a qual utilizou algoritmos e técnicas de tratamento com a finalidade de traçar os perfis dos usuários, visando extrair sua personalidade. Nesse sentido, a próxima etapa consistiria em detectar os usuários "persuasíveis", que não tivessem posicionamentos extremistas sobre determinados assuntos, a fim de lançar anúncios e publicidade em geral, conforme as suas preferências, para conquistá-los e manipular o seu entendimento a favor do objetivo final, qual seja, eleger o candidato.

O caso mencionado é polêmico, sendo que foi a título denunciativo e a fim de dar maior visibilidade à questão que jornais estadunidenses lançaram matérias a seu respeito em março de 2018[114]. Pala além disso, o Ministério Público do Distrito Federal e Territórios instaurou inquérito civil público[115] para fins de investigar se a empresa *Cambridge Analytica* também não estaria atuando no Brasil de forma análoga à mencionada, usando, de forma ilegal, dados pessoais de milhões de brasileiros para construção de perfis psicográficos, que podem ser utilizados para predizer crenças políticas e religiosas, orientação sexual, cor da pele e comportamento político.

Os casos mencionados são preocupantes, uma vez que demonstram que a manipulação inadequada de dados podem significar um risco à autodeterminação dos povos e até mesmo à própria democracia. No mesmo sentido, não são raras as notícias de vazamento de dados de pessoais por descuido da iniciativa pública ou privada ou até mesmo por um aparato frágil de tutela de dados. Assim, fica evidenciada a urgência de uma legislação capaz de tutelar dados pessoais de maneira adequada.

Nesse sentido, tendo um panorama geral sobre a privacidade e a proteção de dados, analisar-se-á no próximo capítulo o ordenamento jurídico brasileiro, de modo a perquirir os precedentes legislativos da recente Lei Geral de Proteção de Dados. Também busca-se analisar conceitos fundamentais estabelecidos na lei, bem como o tratamento de dados, dando especial valoração ao consentimento como prática da autodeterminação informativa, e, por fim, busca-se sondar as dificuldades de implementação enfrentadas pela própria lei.

---

[114] Vide em https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html e https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump. Acesso em 12 nov. 2019.

[115] Através da Portaria nº 02/2018, de 20 de março de 2018. Disponível em: http://www.mpdft.mp.br/portal/pdf/noticias/Mar%C3%A7o_2018/Instauracao_de_ICP_Cambridge_Analytica.pdf. Acesso em: 12 nov. 2019.

4 PROTEÇÃO DE DADOS NO BRASIL

Conforme já tratado anteriormente, a proteção de dados pessoais no ordenamento jurídico brasileiro por muito tempo não derivou de uma dicção explícita e literal, não se estruturando a partir de um complexo normativo unitário, mas estando diretamente relacionada a cláusulas gerais de tutela da personalidade[116].

O ordenamento contempla a proteção da pessoa humana como seu valor máximo e a privacidade como um direito fundamental, no entanto, a proteção desses direitos nos seus diversos âmbitos de incidência, que deveria ser integrada e dirigida pela tábua axiológica constitucional, por muito operou de forma fracionada, em focos de atuação determinados, destacando-se o *habeas data* e o Código de Defesa do Consumidor[117].

O advento das tecnologias informacionais somada à sua difusão na sociedade, ainda que de forma não igualitária[118], foi capaz de gerar uma ruptura paradigmática na análise do direito, sobretudo no âmbito do ciberespaço. Assim, passou a ser necessário rediscutir controvérsias e posicionamentos pretéritos que se julgavam superados, além da necessidade de proposição de questões inéditas fundamentadas em aspectos sociológicos, políticos e econômicos, que "de tão interdisciplinares, põem em risco a própria especificidade do direito"[119].

Foi exatamente nesse sentido que o documento intitulado "exposição de motivos ao Projeto de lei nº 2.126/2011" foi editado, a fim de elencar uma série razões pelas quais se fazia urgente a promulgação de uma lei que regulamentasse as relações no contexto da internet.

No âmbito dessa discussão, foi invocada a Pesquisa Nacional por Amostra de Domicílios, realizada no ano de 2009 pelo Instituto Brasileiro de Geografia e Estatística (IBGE), a qual sinalizava a existência de 68 milhões de usuários de internet no Brasil, com taxa de crescimento de aproximadamente um milhão a cada três meses. A estatística foi capaz de

---

[116] DONEDA, 2006, p.323.

[117] Ibidem, p. 16/17.

[118] Nesse sentido, o historiador Yuval Harari menciona o surgimento de uma "massa de inúteis", que poderia ter como aspectos motivadores o analfabetismo e a exclusão digital; assim, surgiria um extrato da sociedade não apenas desempregado, mas desempregável. Confira-se em: HARARI, Yuval Noah. **The meaning of life in a world without work**. The Guardian, 2017. Disponível em: https://www.theguardian.com/technology/2017/may/08/virtual-reality-religion-robots-sapiens-book. Acesso em: 13 nov. 2019.

[119] LEMOS, Ronaldo. Direito, tecnologia e cultura. E-book publicado pela licença Creative Commons na plataforma Google Books. 2005. p. 8 apud BOFF, Salete Oro; FORTES, Vinícius Borges. **A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental**: perspectivas de construção de um marco regulatório para o Brasil. Florianópolis: Sequencia, 2014. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552014000100006. Acesso em: 13 nov. 2019.

apontar uma série de riscos, uma vez que o país não dispunha de legislação específica para o ciberespaço, no sentido de assegurar os direitos fundamentais e a possibilidade do desenvolvimento econômico e cultural do país. Nesse contexto, foram apontados quatro riscos significativos.

> Os riscos são, portanto, a) da aprovação desarticulada de propostas normativas especializadas, que gerem divergência e prejudiquem um tratamento harmônico da matéria; b) de prejuízos judiciais sensíveis, até que a jurisprudência se adeque às realidades da sociedade da informação; c) de desencontros ou mesmo omissões nas políticas públicas; e d) de violação progressiva de direitos dos usuários pelas práticas e contratos livremente firmados[120].

Assim, o Marco Civil da Internet surgiu como legislação precursora no que diz respeito à regulamentação das interações estabelecidas em âmbito virtual. Trata-se de uma forma de suprir lacunas normativas que inviabilizavam a atração de investimentos em infraestrutura tecnológica, bem como um avanço em termos de segurança jurídica para o ciberespaço brasileiro[121]. No entanto, apesar de tratar de dados pessoais, não estabeleceu normativas específicas atinentes a esse assunto, restringindo-se ao estabelecimento de princípios e normas incipientes, não sendo possível atender às reais necessidades relativas à proteção de dados de forma direta e específica.

A proteção dos dados pessoais, que se mostrou deficiente e até mesmo tardia quando comparada à legislação de demais países como a Argentina e o Uruguai, finalmente foi tratada em âmbito nacional por meio da Lei nº. 13.709, de 14 de agosto de 2018. A Lei Geral de Proteção de Dados (LGPD) dispõe exclusivamente sobre a proteção de dados pessoais no Brasil, tendo como principal influência o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, no entanto, ainda não está em vigência. Nesse sentido, analisar-se-á os precedentes legislativos que culminaram na promulgação da LGPD.

4.1 Precedentes legislativos

Inicialmente, importa esclarecer que a Constituição Federal de 1988 contempla a liberdade de expressão e o direito à informação no seu artigo 5º, incisos IX e XIV e artigo 220, os quais devem ser confrontados com a proteção da personalidade, em especial, com o direito

---

[120] BRASIL. **Exposição de motivos ao Projeto de Lei n. 2.126/2011**. Brasília, DF: Subchefia de assuntos parlamentares, 2011. Disponível em http://www.planalto.gov.br/ccivil_03/Projetos/ExpMotiv/EMI/2011/86-MJ%20MP%20MCT%20MC.htm. Acesso em 13 nov. 2019.

[121] BOFF; FORTES, 2014.

à privacidade[122]. Este, por sua vez, é tratado em âmbito constitucional por meio da tutela da vida privada e da intimidade em seu artigo 5º, inciso X, e da privacidade nas comunicações no inciso XII do mesmo artigo.

> 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;

Primordial destacar que a referência a "dados" nesse último inciso diz respeito à inviolabilidade de comunicação de dados, assim, não fica resguardado todo direito atinente à proteção de dados. O dispositivo resguarda, portanto, a inviolabilidade da comunicação alheia, no sentido de que uma comunicação entre particulares não passe ao domínio de um terceiro[123].

> A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação[124].

A interpretação subsistente é a de que a inviolabilidade das comunicações é relativa em se tratando de comunicação telefônica, pois é instantânea e não deixa vestígios, podendo ser quebrada por ordem judicial, ao passo que a comunicação por correspondência, telegráfica e de dados deixa informações e provas, assim, não são rigorosamente sigilosos e dependem de interpretação infraconstitucional para poderem ser revelados[125]. No mesmo sentido foi o julgamento do Recurso Extraordinário nº 418.416, ao admitir busca e apreensão de documentos e discos rígidos de computadores em empresas sobre as quais recaíam fortes indícios de práticas irregulares, considerando ser lícita a apreensão da base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial, não se tratando, portanto, de quebra de sigilo das comunicações de dados.

Também em âmbito constitucional, é inviolável o domicílio, nos termos do art. 5º, inciso XI. Destaca-se, nesse contexto, que a inviolabilidade de domicílio e das correspondências foram tratadas em todas as Constituições Brasileiras[126], a começar pela Constituição Política do Império do Brasil, de 1824, a qual no artigo 179 dispõe:

---

[122] DONEDA, 2006, p. 323.
[123] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. São Paulo: **Revista Da Faculdade De Direito**, Universidade De São Paulo, 1993, *88*, p 439-459, p. 446. Disponível em: http://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 07 nov. 2019.
[124] Ibidem, p. 447.
[125] Voto proferido pelo ministro Nelson Jobim no julgamento do Recurso Extraordinário nº 219.780-5, em 13/02/1999.
[126] DONEDA, 2006, p.324.

> VII. Todo o Cidadão tem em sua casa um asylo inviolavel. De noite não se poderá entrar nella, senão por seu consentimento, ou para o defender de incendio, ou inundação; e de dia só será franqueada a sua entrada nos casos, e pela maneira, que a Lei determinar. (...) XXVII. O Segredo das Cartas é inviolavel. A Administração do Correio fica rigorosamente responsavel por qualquer infracção deste Artigo.

Nesse sentido, diante da constitucionalização do direito à privacidade, acaba por haver uma tutela protetora que abarca também os dados pessoais[127], estando diretamente relacionados à privacidade.

A Constituição também prevê o *habeas data* em seu art. 5º, inciso LXXII, enquanto uma garantia constitucional de acesso às informações pessoais que estejam em posse do poder público, admitindo, assim, que o Estado seja coibido a retificar informações inexatas dos impetrantes, bem como anotar contestação ou explicação sobre qualquer dado que esteja sendo objeto de debate[128].

Regulamentado pela Lei nº 9.507/97, o *habeas data* consiste em um instituto comumente tratado nos países latino americanos, o que pode ser facilmente compreendido uma vez analisado o contexto histórico em que surgiu.

> Sinteticamente, há de se apontar para o fato de que um instrumento do gênero tenha uma razão especial de ser em sociedades recém-saídas de regimes militares, como em diversos países latino-americanos na década de 1980 em diante, em cujas sociedades persistia o trauma pelo uso autoritário da informação. Após o fim destes regimes, um instrumento para a requisição das informações pessoais em mãos do poder público era tanto desejado quanto necessário, seja para a tutela dos direitos fundamentais envolvidos como também pelo seu importante papel na formação de uma cultura democrática[129].

Assim, o *habeas data* consiste em uma medida destinada a sanar uma deficiência de liberdades individuais, bem como consolidar as bases democráticas do novo sistema[130]. Não trata-se, entretanto, da coroação de um novo direito, nem tampouco da mudança no perfil material do direito à privacidade, mas presta-se a atrair para si a responsabilidade pela sua efetividade, objetivando dar enfoque a um direito que estava sendo negligenciado[131]. Nesse sentido, o inciso LXXII do art. 5º da Constituição Federal dispõe:

> 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;

---

[127] DRUMMOND, 2003, p. 66.

[128] Conforme artigos 4º, *caput* e § 2º, e 7º da Lei nº 9507/97, que regula o direito de acesso a informações e disciplina o rito processual do *habeas data*.

[129] DONEDA, Danilo. Iguais mas Separados: o Habeas Data no Ordenamento Brasileiro e a Proteção de Dados Pessoais. Paraná: **Cadernos da Escola de Direito**, 2008, p. 17-18. Disponível em: http://revistas.unibrasil.com.br/cadernosdireito/index.php/direito/article/view/444. Acesso em: 31 out. 2018.

[130] Idem, 2006, p. 332-333.

[131] Idem, 2006, p. 335.

> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

É possível vislumbrar que são assegurados os direitos de acesso à informação, bem como de retificação, além do direito de "anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável", nos termos do art. 7º, inciso III da Lei do *Habeas Data*, independente de referir-se a dados tratados de forma automatizada ou manual.

No entanto, algumas limitações são impostas à aplicação do instituto. A primeira delas refere-se à aplicação somente em face do poder público, sendo inoperante diante da iniciativa privada. A necessidade de demonstração de que houve recusa do poder público em dar acesso ou retificar as informações, ou até mesmo a recusa em fazer-se anotar a explicação ou contestação sobre determinado dado, nos termos do art. 8º da Lei nº 9.507/97, é outra limitação significativa, uma vez que sugere que o interessado produza prova negativa. Outra limitação consiste na legitimidade ativa restrita ao próprio titular de dados, estendendo-se somente aos sucessores e cônjuge ou companheiro sobrevivente do falecido[132]. E por fim, também consiste limitação à aplicabilidade do remédio constitucional a exigibilidade de patrono com capacidade postulatória para interposição, contrariamente ao que ocorre no *habeas corpus*, conforme artigo 654 do Código de Processo Penal.

Nesse sentido, uma série de críticas são impostas ao instituto do *habeas data.* Apesar de ter sido marco importante na tutela de direitos da personalidade dos cidadãos brasileiros, bem como instrumento para consolidação de um novo Estado Democrático de Direito, revela-se demasiadamente associada à proteção de liberdades negativas, sendo "um instrumento que proporciona uma tutela completamente anacrônica e ineficaz à realidade das comunicações e tratamentos de dados pessoais na Sociedade da Informação"[133].

No que diz respeito à legislação infra legal, interessa destacar a Lei nº 7.232/84, a qual dispõe sobre a Política Nacional da Informática e tem por objetivos a capacitação nacional nas atividades de informática, lançando princípios como o "estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas", bem como o "estabelecimento de mecanismos e instrumentos para assegurar a todo

---

[132] JEREISSATI, Régis Gurgel do Amaral; DIAS, Eduardo Rocha. **Legitimidade ativa dos sucessores e do cônjuge ou companheiro sobrevivente para impetração do habeas data sob a ótica da preservação da privacidade do morto**. Rio de Janeiro: Civilistica.com, 2017, p. 24. Disponível em: http://civilistica.com/wp-content/uploads/2017/08/Jereissati-e-Dias-civilistica.com-a.6.n.1.2017.pdf. Acesso em: 14 nov. 2019.

[133] DONEDA, 2010, p. 51.

cidadão o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas"[134]. Os princípios elencados abordam temas relevantes, no entanto, a lei não institui os modos como tais princípios deverão materializar-se, assim, constitui uma forma bastante tímida e até mesmo inoperante de proteção de dados pessoais.

A Lei nº 8.078/90, denominada Código de Defesa do Consumidor (CDC), por muito tempo foi o diploma legal que mais se aproximou da proteção de dados pessoais no ordenamento jurídico brasileiro, fomentando uma postura ativa do consumidor, induzindo o civilista a afastar-se das categorias neutras do Código Civil de 1916 e promovendo uma modernização que se irradiou para além das relações de consumo[135]. O CDC foi capaz de lançar um sistema efetivamente preocupado com o consumidor, de modo a confrontar a utilização abusiva das informações sobre consumidores em bancos de dados.

Nesse sentido, o legislador preocupa-se com o "estabelecimento de equilíbrio na relação de consumo através da interposição de limites ao uso pelo fornecedor de informações sobre o consumidor"[136], tutelando um âmbito de situações mais amplo e de maneira mais protetiva que o próprio *habeas data*[137].

Relevante dispositivo legal que deve ser mencionado é o artigo 43, o qual protege o consumidor quanto à difusão de dados a si referentes, em especial assegurando-lhe o direito de ser comunicado quando da inserção do seu nome em cadastros de proteção ao crédito (§ 2º), levando-se em conta o direito de informação[138], o dever de boa-fé[139] e a transparência[140]. Além disso, também importa destacar que cabe ao órgão administrador do cadastro o dever de informar a inscrição, sendo resguardada, ainda, a responsabilização solidária entre o órgão de proteção ao crédito e a empresa credora, nos termos do art. 7º, parágrafo único do CDC.

O dispositivo mencionado também concede ao consumidor o direito de acesso (*caput*) e de retificação (§ 3º), bem como a atualização e pertinência dos dados cadastrais (§ 1º, parte inicial), além do direito ao esquecimento, seja pelo decurso de cinco anos ou pela prescrição da dívida (§ 1º, parte final, e § 5º). Nesse sentido a súmula 323 do STJ dispõe: "a inscrição do nome do devedor pode ser mantida nos serviços de proteção ao crédito até o prazo máximo de cinco anos, independentemente da prescrição da execução", sendo importante frisar

---

[134] Artigo 2º, incisos VIII e IX da Lei nº 7.232/84.
[135] TEPEDINO, Gustavo. As relações de consumo e a nova teoria contratual apud DONEDA, 2006, p.338.
[136] DONEDA, 2006, p.338.
[137] LIMBERGER, 2007, p. 190.
[138] Artigo 6º, inciso III, do CDC.
[139] Artigo 4º, inciso III, do CDC.
[140] Artigo 4º, *caput,* do CDC.

que o termo inicial deve ser o dia seguinte ao vencimento da dívida[141] e que, havendo o adimplemento ou renegociação da dívida, a baixa da inscrição incumbe ao credor, devendo ser feita em tempo razoável[142].

Assim, pode-se falar inclusive na existência do princípio da finalidade, levando-se em conta o princípio da boa-fé objetiva e da própria garantia constitucional da privacidade, pelo qual os dados do consumidor coletados deverão prestar-se somente para os fins que motivaram sua coleta, servindo, inclusive, como fundamentação para a vedação à coleta de dados pessoais e comercialização de bancos de dados de consumidores[143].

Para além disso, é certo que o CDC não restringe o seu âmbito de aplicação somente aos cadastros negativos de crédito; inexistindo ressalvas no artigo 43, anteriormente mencionado, nem tampouco nos demais dispositivos do diploma legal, é certo que a aplicação se dá amplamente aos bancos de dados e cadastros dos consumidores. Nesse sentido, os bancos de dados positivos e negativos apresentam um ponto em comum, qual seja, o direito de informação do comerciante ou do banco, por ocasião de concessão de crédito ou realização de negócio jurídico[144], havendo aplicação do CDC em ambos os casos.

A Lei nº 12.414/11 disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, são os chamados cadastros positivos. Assim, tendo em vista todo exposto, é correto deduzir que referido diploma sujeita-se ao disposto no CDC, em especial à comunicação quando da inscrição do consumidor, nos termos do artigo 43.

No entanto, recente Lei Complementar (nº 166/19) alterou o dispositivo da Lei de cadastro positivo que estabelecia a necessária autorização prévia do potencial cadastrado mediante consentimento informado, para passar a constar sua inscrição compulsória, nos termos do artigo 4º da referida lei, sendo assegurado, no entanto, o direito de cancelamento do cadastro, conforme artigo 5º, inciso I. Assim, questiona-se a validade da Lei Complementar, uma vez que os cadastros positivos submetem-se ao CDC e, no entanto, passaram a contrariar o estabelecido dever de informar, bem como o direito básico de informação e a transparência.

---

[141] BRASIL. Superior Tribunal de Justiça. **Informativo 588**. O termo inicial do prazo de permanência de registro de nome de consumidor em cadastro de proteção ao crédito (art. 43, § 1º, do CDC) inicia-se no dia subsequente ao vencimento da obrigação não paga, independentemente da data da inscrição no cadastro. Brasília, DF: STF, 2016, p. 13. Disponível em: https://scon.stj.jus.br/SCON/SearchBRS?b=INFJ&tipo=informativo&livre=@COD=%270588%27. Acesso em: 21 nov. 2019.

[142] BRASIL. Superior Tribunal de Justiça (4. Turma). **Recurso Especial 870.582/SP**. Relator: Ministro Aldir Passarinho Junior. Julgado em 23/10/2007.

[143] DONEDA, 2006, p.339.

[144] LIMBERGER, 2007, p. 199.

No que diz respeito ao sigilo fiscal e bancário, destacam-se as leis complementares nº 104 e 105, de 2011.

A Lei Complementar nº 104/2001 deu nova redação ao artigo 198 do Código Tributário Nacional para vedar a divulgação de dados fiscais de sujeitos passivos ou de terceiros por parte de agentes do fisco, além de estabelecer ressalvas quanto à requisição de autoridade judiciária no interesse da justiça ou requisição de autoridade administrativa quando da instauração regular de processo administrativo. Para além disso, assegura-se a livre circulação de informações entre a administração pública direta, com a finalidade de prestar assistência mútua para a fiscalização de tributos, bem como a permuta de informações entre a Fazenda Pública da União e Estados estrangeiros, na forma estabelecida em tratados, acordos ou convênios, e no interesse da arrecadação e da fiscalização de tributos.

A Lei Complementar nº 105/2001, por sua vez, dispõe sobre o sigilo das operações de instituições financeiras, comumente denominado sigilo bancário. A lei assegura, via de regra, o sigilo das operações, nos termos dos artigos 1º, *caput*, e 2º, no entanto, prevê diversas exceções, sendo certa a preferência pelo interesse público frente ao direito individual de proteção ao sigilo bancário[145].

Nesse sentido, são estabelecidas ocasiões em que a quebra de sigilo pode se dar diretamente pelos agentes fiscais (art. 6º), havendo processo administrativo ou procedimento fiscal em curso, ou por concessão de ordem judicial (art. 1º, § 4º e outros), como para se apurar a ocorrência de qualquer ilícito, em qualquer fase do inquérito ou do processo judicial, dentre os quais podem ser citados terrorismo, tráfico de drogas, contrabando ou tráfico de armas, crimes contra a administração pública, contra a ordem tributária e previdência social, lavagem de dinheiro ou ocultação de bens.

Exceções ao sigilo bancário também são vislumbrados no que diz respeito a troca de informações entre as instituições financeiras para fins cadastrais, o fornecimento de informações constantes de cadastro de emitentes de cheques sem provisão de fundos, a comunicação às autoridades competentes da suposta prática de ilícitos penais ou administrativos quando os recursos possuam origem criminosa, além da revelação de informações sigilosas com o consentimento expresso dos interessados.

O Código Civil, por sua vez, não faz referência expressa à privacidade de dados, limitando-se a dispor, em seu artigo 21, sobre inviolabilidade da vida privada da pessoa natural

---

[145] OLIVEIRA, Rogerio Alvarez. ALVAREZ, Wanessa Gonçalves. **Particularidades atuais da quebra de sigilo bancário**. Publicado em 03/04/2017. Disponível em: https://www.conjur.com.br/2017-abr-03/mp-debate-particularidades-atuais-quebra-sigilo-bancario-parte. Acesso em: 15 nov. 2019.

e a assegurar que o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma. Assim, somada à previsão legal do artigo 927, que versa sobre a responsabilização civil por ato ilícito, vê-se com bons olhos a possibilidade de integração da responsabilidade civil por danos à pessoa no tocante aos direitos da personalidade[146].

Ainda no âmbito da responsabilidade civil, necessário salientar a Lei nº 5.250/67, que regula a liberdade de manifestação do pensamento e de informação. O artigo 49 da lei prevê a responsabilização de quem violar direito ou causar prejuízo a outrem no exercício das suas liberdades. Além disso, nos casos de calúnia e difamação, havendo prova de que o suposto conteúdo ofensivo era verdadeiro, a responsabilização estaria excluída (§ 1º). Entretanto, a lei admite que, ainda que o fato realmente seja verdadeiro, mas diga respeito à vida privada do ofendido e não tenha sido divulgado em razão de interesse público, subsistirá a responsabilização (§ 1º, parte final). Nesse caso, ainda que a liberdade de manifestação do pensamento e de informação sejam liberdades caras ao Estado Democrático de Direito, os direitos atinentes à vida privada devem remanescer.

Destaca-se, ainda, os processos judiciais que tramitam em segredo de justiça a fim de resguardar interesses dos litigantes. O Código de Processo Civil, nesse sentido, estabelece em seu artigo 189 que tramitarão em segredo de justiça os processos em que constem dados protegidos pelo direito constitucional à intimidade (inciso III), além de incluir os processos em que o exija o interesse público e social (I), relativos ao âmbito familiar (II) e que versem sobre arbitragem (IV).

Na esfera penal, o artigo 201, § 6º, do Código de Processo Penal, estabelece que "o juiz tomará as providências necessárias à preservação da intimidade, vida privada, honra e imagem do ofendido, podendo, inclusive, determinar o segredo de justiça em relação aos dados, depoimentos e outras informações constantes dos autos a seu respeito para evitar sua exposição aos meios de comunicação". Além disso, admite-se a tramitação de determinados autos em segredo de justiça, a título exemplificativo, os que dizem respeito à investigação de organizações criminosas (art. 23, Lei nº 12.850/13) e crimes contra a dignidade sexual (art. 234-B do Código Penal).

A proteção de dados pessoais também encontra respaldo no âmbito do direito penal nos artigos 93 do Código Penal e 748 do Código de Processo Penal, os quais tratam da chamada "reabilitação", instituto que assegura ao condenado o sigilo dos registros sobre seu

[146] LIMBERGER, 2007, p. 193.

processo e condenação, o qual pode ser requerido após dois anos do dia em que for extinta a pena ou finda a execução, conforme artigo 94 do Código Penal. De forma ainda mais protetiva, o artigo 202 da Lei de Execuções Penais dispõe que, após a extinção da pena, não deve constar na folha corrida, atestados ou certidões fornecidas por autoridade policial ou auxiliares de Justiça, qualquer notícia referente à condenação, salvo para instruir processo pela prática de nova infração penal ou outros casos expressos em lei. Nesse sentido, o instituto se presta à recuperação, pelo condenado, de seu *status quo* anterior à condenação, operando-se, portanto, o direito ao esquecimento do regresso.

Ainda no âmbito do direito penal, necessário destacar a Lei 12.737/12, a qual tipifica delitos informáticos, sendo clara a preocupação do legislador em conferir maior proteção na seara penal aos dados. Destaca-se a inclusão do artigo 154-A ao Código Penal para passar a tipificar a invasão de dispositivo informático alheio a fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. No entanto, alguns estudiosos consideram que legislador imprimiu à referida lei uma economia textual desnecessária, não expressando questões relacionadas aos conceitos e às definições fundamentais para a aplicação da norma[147].

Destaca-se, ainda, a importância da Lei de Acesso à Informação, Lei nº 12.527/11, no sentido de estabelecer que os órgãos e entidades do poder público assegurarem a gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação; a proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; bem como a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Assim, conforme já tratado anteriormente, a lei se presta ao acesso da própria população aos dados em posse do poder público, visando coibir o Estado a atuar de maneira transparente e responsável em relação às informações que estão sob sua vigilância. Salienta-se que a lei destina-se a assegurar o direito fundamental de acesso à informação, observando princípios básicos da administração pública, tais como observância da publicidade como preceito geral, sendo o sigilo uma exceção; divulgação de informações de interesse público; utilização de meios de comunicação facilitados pela tecnologia da informação; entre outros[148].

---

[147] BOFF, Salete Oro; FORTES, Vinícius Borges. Internet e Proteção de Dados Pessoais: uma Análise das Normas Jurídicas Brasileiras a partir das Repercussões do caso NSA vs. Edward Snowden. **Cadernos do Programa de Pós-Graduação em Direito PPGDir. UFRGS**, Porto Alegre, v. 11, n. 1, p. 340-370, ago. 2016. Disponível em: http://seer.ufrgs.br/ppgdir/article/view/58918/38152. Acesso em: 19 set. 2018.

[148] Ibidem, p. 357.

Tendo em vista todo o exposto até o momento, inegável que o ordenamento jurídico brasileiro dispõe de diversos diplomas legais capazes de abordar a temática dos dados pessoais, em âmbitos variados. No entanto, nenhuma das legislações aqui elencadas foram capazes de tutelar os dados pessoais de forma direta e ampla, nem sequer foram capazes de regulamentar as relações no âmbito da internet.

A Lei nº 12.965/14, por sua vez, estabelece princípios, garantias, direitos e deveres para o usuário da Internet no Brasil, ocasionando certa mudança de paradigma. O denominado Marco Civil da Internet prevê a proteção de dados pessoais como um de seus pilares (art. 3º, III), além de estabelecer direitos e garantias dos usuários em seu artigo 7º, como o não fornecimento de dados pessoais a terceiros, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (art. 7º, VII); a prestação de informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam vedada pela legislação e estejam especificadas nos contratos de prestação de serviços (VIII); o consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (IX); e, finalmente, a exclusão definitiva dos dados pessoais que tiverem sido fornecidos a determinada aplicação de internet, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas na própria lei (X).

O Marco Civil determina ainda que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (art. 10, caput). Assim, o provedor responsável pela guarda somente deverá disponibilizar os registros, de forma autônoma ou associados a dados pessoais, mediante ordem judicial (art. 10, § 1º), sendo estabelecidas sanções em caso de infrações às normas previstas (art. 12). Para além disso, na provisão de aplicações de internet, onerosa ou gratuita, fica vedada a guarda dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente; também fica vedada a guarda de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular (art. 16).

É possível perceber, portanto, que o Marco Civil da Internet consagra alguns princípios relativos ao tratamento de dados pessoais, dentre os quais podem ser citados os princípios da finalidade, necessidade e transparência, além de atribuir valoração especial ao

consentimento expresso e fazer referência ao direito ao esquecimento. A normativa é capaz de assegurar direitos ao titular de dados, mas pouco detalha sobre a efetividade desses direitos.

> [...] o Marco Civil, nos demais artigos que versam sobre a proteção da privacidade (arts. 7, 9, 10, 11, 12, 15, 19, 21 e 23), não enfrenta vários aspectos dos modelos de negócios tanto das empresas de telecomunicações quanto dos provedores de aplicações de internet que, com o big data, utilizam-se diuturnamente da privacidade, intimidade, honra, segredos, hábitos e pensamentos para vender serviços e ganhar dinheiro[149].

Isto posto, a despeito de inúmeras legislações que tangenciavam a proteção dos dados pessoais, a latente necessidade de regulamentação direta e específica persistiu, sendo certo que a tutela desses direitos por vezes mostrou-se deficiente, deixando os indivíduos cada vez mais expostos.

4.2 Análise da Lei nº 13.709/18 frente ao tratamento de dados pessoais

A Lei nº. 13.709/18, denominada Lei Geral de Proteção de Dados (LGPD), dispõe exclusivamente sobre a proteção de dados pessoais e foi sancionada no intuito de suprir a lacuna jurídica tratada no último tópico.

A LGPD, influenciada pelo GDPR, finalmente concede ao cidadão brasileiro o direito de controle da privacidade de seus próprios dados de forma clara e expressa. Nesse sentido, o regime de proteção de dados não tem por finalidade apenas a tutela da privacidade dos usuários, mas também visa proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, nos termos do artigo 1º da LGPD[150].

> [...] a Lei Geral de Proteção de Dados deixa claro que pretende proteger o usuário-cidadão plenamente, em todos os aspectos da sua autonomia pública e privada, valorizando e preservando sua autodeterminação informativa e sua capacidade decisória. Trata-se, portanto, de eixo valorativo em torno do qual devem ser compreendidas e interpretadas todas as demais disposições previstas pela lei[151].

A LGPD confere proteção à "informação relacionada a pessoa natural, identificada ou identificável", sendo essa a conceituação de dado pessoal (art. 5º, I). Além disso, poderão ser igualmente considerados como dados pessoais aqueles utilizados para formação do perfil

---

[149] GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado**. 1ª ed. São Paulo: Atlas, 2017.

[150] Destaque-se que este tópico é destinado inteiramente à análise da Lei Geral de Proteção de Dados, dando enfoque especial às conceituações basilares e ao modo como se estabeleceu o tratamento de dados no âmbito da lei. Assim, todas as referências a artigos de lei aqui dispostas referem-se a artigos contidos na LGPD.

[151] FRAZÃO, Ana. **A nova Lei Geral de Proteção de Dados Pessoais**: Principais repercussões para a atividade empresarial. Parte I. 2018a. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018. Acesso em: 20 set. 2018.

comportamental de determinada pessoa natural, se identificada (art. 12, § 2º). Nesse contexto, a pessoa identificável é aquela que pode ser apontada, direta ou indiretamente, por referência a um individualizador como por exemplo nome, número identificador, dados de localização, dentre outros, ou por meio da análise do histórico de compras de uma pessoa, a qual pode revelar sua orientação sexual, posicionamento político ou religião.

Assim, ainda que determinado dado tenha sido codificado ou pseudonimizado, mas haja possibilidade de reidentificação do titular, será considerado dado pessoal e abrangido pelo âmbito de proteção da lei. No entanto, em se tratando de dados anônimos, cujo titular não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (art. 5º, III), ou seja, cujo processo de anonimização[152] seja irreversível, não poderão ser objeto de tutela da LGPD, conforme estabelece o art. 12, *caput*.

Aqui cabe relembrar a conceituação de tratamento, tendo em vista sua relevância e abrangência frente à matéria. Tratamento diz respeito a toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, conforme art. 5º, X.

Além disso, inexiste distinção quanto ao modo de tratamento de dados, sendo certo que a LGPD abrange dados automatizados e manuais, desde que organizados conforme determinada lógica utilitarista. O objetivo principal da LGPD é o de proteger os dados pessoais, sensíveis ou não, qualquer que seja o meio ou a tecnologia empregada para o tratamento[153].

Quanto aos sujeitos nas relações de tratamento de dados, destaca-se o agente de tratamento e o titular de dados. O agente de tratamento pode classificar-se enquanto controlador ou operador (art. 5º, IX), sendo certo que ambos podem ser pessoa natural ou jurídica, de direito público ou privado. Nesse sentido, ao controlador competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI) e ao operador, o tratamento de dados pessoais em nome do controlador (art. 5º, VII). Já o titular de dados, sujeito protegido pela lei, deve ser estritamente a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, V).

---

[152] Nos termos do art. 5º, XI, da LGPD, anonimização refere-se à utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

[153] FRAZÃO, Ana. **A nova Lei Geral de Proteção de Dados**: Repercussões para a atividade empresarial: o alcance da LGPD. Parte II. 2018c. Disponível em https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-alcance-da-lgpd-e-repercussoes-para-a-atividade-empresarial-05092018. Acesso em 20 set. 2018.

Destaca-se, ainda, uma quarta figura, o encarregado, que constitui pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (art. 5º, VIII).

Quanto ao âmbito de aplicação, nos termos do art. 3º, necessário destacar que a lei aplica-se independentemente do meio, do país de sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada em território nacional (inciso I), que a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços em território nacional (II), ou, por fim, que os dados pessoais objeto do tratamento tenham sido coletados em território nacional (III).

Nesse sentido, tendo em vista a amplitude do conceito de tratamento de dados, bem como a eficácia extraterritorial da LGPD, o objeto de aplicação da lei torna-se excessivamente amplo, sendo capaz de ensejar grande transformações na relações empresariais e sociais[154].

Ressalta-se, ainda, hipóteses nas quais a lei não se aplica ao tratamento de dados pessoais (art. 4º), podendo ser citados o tratamento: realizado por pessoa natural para fins exclusivamente particulares e não econômicos (inciso I); realizado para fins exclusivamente jornalístico e artísticos, ou acadêmicos, aplicando-se a esta última hipótese os requisitos para tratamento de dados e dados sensíveis (II); realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (III); ou provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto em lei (IV).

Nesse seguimento, necessário destacar que o texto legal indica que as atividades de tratamento de dados pessoais deverão observar a boa-fé e determinados princípios basilares (artigo 6º), os quais serão tratados adiante.

O primeiro princípio consiste no princípio da finalidade, pelo qual a realização do tratamento deve se dar para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (I). Esse princípio relaciona-se intimamente com princípio da adequação, conforme já destacado neste trabalho, e consiste na compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento (II). Já o princípio da necessidade limita o tratamento

[154] FRAZÃO, 2018c.

ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (III). O princípio do livre acesso, também já abordado, estabelece a garantia, concedida aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (IV).

O princípio da qualidade dos dados, por sua vez, funciona como garantia de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (V). O princípio da transparência opera como garantia de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (VI). O princípio da segurança remete à utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (VII).

A prevenção, de seu turno, diz respeito à adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (VIII). O princípio da não discriminação revela a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (IX). E, por fim, o princípio da responsabilização e prestação de contas exige demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (X).

A partir de simples análise dos princípios aqui elencados é possível perceber o quanto eles relacionam-se entre si, e, para além disso, criam um aparato de proteção bastante amplo e positivo ao titular de dados. Analisar-se-á, portanto, como se dá a materialização desses princípios no âmbito do tratamento de dados, bem como a autonomia conferida ao titular de dados, no exercício do consentimento como forma de autodeterminação informativa.

Por questões metodológicas, este tópico do trabalho irá ater-se principalmente à análise dos artigos que versam sobre os requisitos para o tratamento de dados pessoais, dispostos do capítulo 2 da LGPD - artigos 7º ao 14.

Destaca-se que a LGPD prevê as hipóteses em que poderá ser realizado o tratamento de dados, havendo previsões especiais e mais rígidas no tocante aos dados pessoais sensíveis e dados pessoais de crianças e adolescentes. No entanto, independentemente da espécie de dado tratado, é necessário que estejam sempre em conformidade com os princípios estabelecidos em lei, citados acima.

Nesse contexto, a primeira e mais importante hipótese em que se admite o tratamento de dados é mediante o fornecimento de consentimento pelo titular (art. 7º, I). Assim, importante que se delimite de que forma tal consentimento deve ser dado, bem como abordar as exceções à esta regra.

No âmbito da lei, consentimento consiste em "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5º, XII), assim, deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º). Nesse sentido, importa destacar que o consentimento não deve ser extraído de mera omissão do titular, mas de atos positivos que expressem vontade inequívoca, não se admitindo o consentimento presumido.

Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais, conforme art. 8º, § 1º. Além disso, caberá ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com os dispostos legais (§ 2º). Nesse seguimento, obtenção, registro e comprovação de consentimento deverão ser objetos de atenção quando da formação de contratos eletrônicos, por exemplo. Para além disso, o consentimento será inválido quando for dado de forma viciada, sendo vedado o tratamento de dados pessoais nesses casos (§ 3º).

Do ponto de vista da eficácia subjetiva, o consentimento não fica vinculado ao controlador originário, sendo certo que para haver comunicação ou compartilhamento de dados pessoais com outros controladores, necessário que se obtenha consentimento específico do titular para esse fim, nos termos do art. 7º, § 5º, ressalvadas as hipóteses de dispensa do consentimento previstas em lei.

Ademais, o § 4º do artigo 8º estabelece que o consentimento deverá referir-se a finalidades determinadas, mediante o conhecimento estrito de todas as informações necessárias para tal, atendendo-se, portanto, aos princípios da finalidade e adequação. Outrossim, as autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas.

Assim, no que diz respeito à informação que deve ser prestada ao titular de dados, destaca-se o *caput* do artigo 9º e seus incisos:

> O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

O dispositivo citado evidencia a forte relação entre o direito à informação e o princípio da transparência e prestação de contas e somente não é absoluto em razão da ressalva com relação aos segredos comercial e industrial, sendo certo que todas as demais informações sobre o tratamento de dados devem ser prestadas ao titular, sem o que não restará observado o requisito do consentimento informado[155].

Para além disso, nas hipóteses em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca (art. 9º, § 1º). Outrossim, caso haja alterações quanto à finalidade específica do tratamento, sua forma e duração, quanto à identificação do controlador, ou ainda quanto ao uso compartilhado de dados pelo controlador e a finalidade, incumbe ao controlador o dever de informar o titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde das alterações (art. 8º, § 6º).

Ainda, quaisquer alterações nas circunstâncias que justificaram o consentimento do titular ensejarão a necessidade de novo consentimento[156]. Nesse sentido o artigo 9º, § 2º, dispõe: "Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações".

Também evidencia-se a temporariedade do consentimento, vez que pode haver revogação a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (art. 8º, § 5º); a eliminação, por sua vez, consiste no direito do titular de dados solicitar a exclusão dos dados tratados ainda que mediante prévio consentimento, nos termos do inciso VI do art. 18 da Lei.

O legislador também atentou-se para uma problemática já citada neste trabalho, que diz respeito aos casos em que o tratamento de dados pessoais consiste condição para o fornecimento de produto ou de serviço ou para o exercício de direito, assim, o fornecimento de dados pessoais constitui aspecto essencial. Nesses casos, o art. 9º, § 3º da lei, em clara alusão

---

[155] FRAZÃO, Ana. **A nova Lei Geral de Proteção de Dados**: Repercussões para a atividade empresarial: a importância do consentimento para o tratamento dos dados pessoais. Parte III. 2018b. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018. Acesso em: 20 set. 2018.

[156] Ibidem.

ao princípio da transparência, estabelece que o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer seus direitos, os quais encontram-se elencados no art. 18 da lei, que dispõe sobre os direitos do titular face ao controlador.

As demais hipóteses de tratamento de dados arroladas no art. 7º da LGPD constituem exceções à regra, no sentido de que tratam de circunstâncias nas quais o tratamento de dados é permitido sem que haja o consentimento do titular, nos termos esclarecidos acima. No entanto, a existência de prerrogativas à regra do consentimento não revelam que os direitos dos titulares de dados tenham sido igualmente excetuados, nem tampouco que os princípios estabelecidos pelo artigo 6º devem ser menosprezados.

Nesse sentido a normativa estabelece que o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização (art. 7º, § 3º). Além disso, a eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas em lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular (art. 7º, § 6º). Assim, necessário enfatizar os princípios da finalidade e adequação, segundo os quais o tratamento de dados deve se dar estrita e unicamente nas condições que motivaram a coleta.

Importante destacar, ainda, que têm igual abordagem os dados tornados manifestamente públicos pelo titular, estando resguardados os direitos do titular e os princípios previstos em lei, para os quais fica dispensada a exigência do consentimento livre, informado e inequívoco (art. 7º, § 4º).

Nesse sentido, serão tratados brevemente os casos que excetuam a regra do consentimento, disposto no art. 7º, incisos II ao X.

A segunda hipótese de tratamento de dados prevista no rol do artigo 7º diz respeito ao tratamento de dados pessoais para o cumprimento de obrigação legal ou regulatória pelo controlador. Nessa circunstância destaca-se a preponderância do interesse público que justifica a obrigação legal ou regulatória. O inciso III, por sua vez, refere-se exclusivamente ao tratamento e uso compartilhado de dados, pela administração pública, necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições sobre o tratamento de dados pessoais pelo Poder Público (capítulo IV da LGPD).

O inciso IV permite o tratamento de dados para a realização de estudos por órgão de pesquisa. Assim, em que pese a importância das pesquisas científicas, a anonimização dos dados pessoais deve ser garantida, sempre que possível; é nesse sentido que estabelecem-se os comitês de ética nas Universidades, a fim de resguardar os interesses individuais em prol do

desenvolvimento científico. Outra hipótese, elencada no inciso V, diz respeito à necessidade do tratamento de dados para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados. Assim, a solicitação visa assegurar a própria execução do contrato.

O tratamento de dados também poderá ser realizado para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Assim, ressalta-se que não cabe à proteção aos dados pessoais comprometer o necessário direito que as partes têm de produzir provas umas contra as outras, ainda que estas se refiram a dados pessoais do adversário[157].

O inciso VII excetua o consentimento no tratamento de dados para a proteção da vida ou da incolumidade física do titular ou de terceiros; já o inciso VIII o faz para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Assim, necessário destacar ser indispensável que a motivação esteja devidamente justificada e comprovada.

O inciso IX, por sua vez, determina que o tratamento de dados poderá ser realizado quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Esta hipótese merece especial atenção, vez que, ao contrário das situações que foram claramente apresentadas anteriormente, encontra-se eivada de ambiguidade e vagueza.

Na tentativa de elucidar o que constitui "interesse legítimo do controlador" o legislador estabeleceu no art. 10: "o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei". No entanto, o que se observa é que a incompreensão persiste, vez que o dispositivo, além de invocar rol não exaustivo de hipóteses, evoca hipóteses igualmente nebulosas, vagas e ambíguas.

Importa destacar, ainda, que a GDPR também arrolou hipótese análoga a essa[158], dentre os casos em que o tratamento de dados pode se dar sem o consentimento do titular.

---

[157] FRAZÃO, Ana. **Nova LGPD**: as demais hipóteses de tratamento de dados pessoais. Parte IV. 2018e. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018. Acesso: em 22 set. 2018.

[158] Artigo 6º, 1, "f", do Regulamento (UE) 2016/679.

Assim, tendo em vista que o tema é tratado com a mesma imprecisão revelada na normativa brasileira, observa-se que o legislador brasileiro perdeu a oportunidade de tratar a questão com maior diligência e exação. Nesse sentido, a questão do interesse legítimo dos controladores constitui um ponto delicado da LGPD pois, a depender da amplitude da sua compreensão, pode ser capaz de mitigar, por completo, aquela que deveria ser a regra no tratamento de dados, qual seja, o consentimento do titular[159].

Por fim, a última hipótese de tratamento de dados, revelada pelo inciso X, prevê a legitimidade para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Os dados sensíveis, por sua vez, constituem "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"[160]. Assim, representam uma categoria especial de dados para que não sejam utilizados em prejuízos dos seus próprios titulares, como instrumento de categorização ou até mesmo discriminação.

Os riscos da utilização inadequada dos dados sensíveis, bem como a importância da sua qualificação de maneira diversa, foram expostos anteriormente. No entanto, é necessário frisar que a diferenciação entre dados pessoais sensíveis e "não sensíveis" nem sempre é clara e dinâmica, sendo certo que a utilização de dados como a localização geográfica pode ter grande impacto negativo no que diz respeito à geodiscriminação, ainda que não seja necessariamente um dado sensível[161].

Nesse sentido, o artigo 11, § 1º estabelece: "Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica". Assim, pode-se observar grande paralelismo na normativa referente ao tratamento de dados pessoais e dados pessoais sensíveis (artigos 7 e 11, respectivamente), sendo importante destacar que todo o cuidado já expresso anteriormente deve ser tomado em maior medida em se tratando de dados pessoais sensíveis.

---

[159] FRAZÃO, 2018e.

[160] A definição de dados sensíveis dada pela LGPD (exposta neste trabalho no tópico 1.1) aproxima-se em muito da definição atribuída na GDPR, assim, o conceito aqui trazido pode ser encontrado no artigo 9º, 1, da GDPR.

[161] FORTES, Pedro Rubim Borges. MARTINS, Guilherme Magalhães. OLIVEIRA, Pedro Farias. O consumidor contemporâneo no show de Truman: a geodiscriminação digital como prática ilícita no direito brasileiro. **Revista de Direito do Consumidor**, v. 124, p. 235-260, jul.-ago. 2019.

Assim, a LGPD também prevê o tratamento de dados sensíveis quando houver consentimento do titular de dados, no entanto, esse consentimento deve se dar de forma específica e destacada, para finalidades específicas (art. 11, I).

Além disso, também são previstas exceções à regra do tratamento mediante consentimento (art. 11, II, alíneas), podendo ser destacadas hipóteses que possuem grande similitude às citadas anteriormente (art. 7º, II ao X), excetuando-se somente as hipóteses de execução de contratos (art. 7º, V), de legítimo interesse do controlador (art. 7º, IX) e de proteção do crédito (art. 7º, X).

Assim, no lugar da polêmica hipótese de legítimo interesse do controlador, o art. 11, II, "g", da LGPD previu hipótese bem mais restritiva, vinculada essencialmente aos interesses dos titulares de dados, a qual dispõe o tratamento para "garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos".

Importa destacar, ainda, que o art. 11, § 4º veda a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, excetuando-se algumas hipóteses, como, por exemplo, para permitir a portabilidade de dados quando solicitada pelo titular. Além disso, o § 5º veda às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Já no que diz respeito ao tratamento de dados pessoais de crianças e adolescentes, importante destacar que deverá ser realizado em seu melhor interesse (art. 14, *caput*), mediante consentimento específico e em destaque, dado por pelo menos um dos pais ou pelo responsável legal (§ 1º) e em conformidade com a exigência de que os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos garantidos ao titular de dados no art. 18 da lei (§ 2º).

Além disso, incumbe ao controlador realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis (§ 5º).

As informações sobre o tratamento de dados ora tratadas deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (§ 6º).

Excepcionando-se a normativa, o § 3º estabelece que poderão ser coletados dados pessoais de crianças sem o consentimento acima tratado quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para proteção do menor; sendo certo que em nenhum caso poderão ser repassados a terceiro sem o consentimento tratado pelo § 1º do mesmo artigo.

Por fim, o § 4º estabelece que os controladores não deverão condicionar o consentimento específico dos pais ou responsável legal em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. Nesse sentido, apura-se que os serviços ofertados pela internet para crianças e adolescentes não devem ser condicionados ao fornecimento de informações pessoais, salvo as estritamente necessárias à atividade.

Em suma, todas as hipóteses aqui elencadas dizem respeito às formas de tratamento de dados pessoais estabelecidas na LGPD, as quais dão valoração especial ao consentimento livre, informado e inequívoco. Além disso, foram retratadas as exceções impostas ao preceito do consentimento, as quais quase sempre estão relacionadas à aspectos de interesse público e social, e, em alguns casos, ao interesse individual. Importa frisar que todas as formas de tratamento, inclusive as que excetuam a regra do consentimento, exigem o estrito seguimento dos princípios estabelecidos em lei, os quais oferecem grande aparato protetivo ao titular de dados, devendo ser aplicados em todos os casos concretos.

Entende-se, ainda, que a carga valorativa atribuída ao consentimento, somada a todos os requisitos estabelecidos para que o mesmo seja considerado válido, aqui citados, revelam uma faceta prática da autodeterminação informativa, no sentido de que é exatamente nesse ato que o titular determina limites entre sua vida pública e privada.

No entanto, o exercício da autodeterminação informativa não limita-se à autonomia do titular em consentir ou não, sendo certo que expressa-se também através dos direitos estabelecidos pelo artigo 18, dentre os quais podem ser citados o acesso aos dados, a correção de dados incompletos, inexatos ou desatualizados, a portabilidade dos dados a outro fornecedor de serviço ou produto e a revogação do consentimento.

Assim, o que se intenta não é tratar de forma exaustiva todas as formas em que a autodeterminação informativa pode expressar-se por meio da LGPD, mas sim, abordar as formas de tratamento de dados pessoais sob a perspectiva dos princípios estabelecidos em lei, bem como delimitar até que ponto a autonomia do titular de dados é levada em conta, em detrimento dos interesses públicos e sociais.

Diante da análise dos artigos de lei, depreende-se que a LGPD consiste em um diploma moderno e capaz de revolucionar aspectos em âmbito social e econômico. No entanto, alguns desafios quanto à sua aplicação já podem ser vislumbrados.

4.3 Dificuldades vislumbradas à aplicação da Lei nº 13.709/18

Destaca-se, de início, que o texto legal publicado em 14 de agosto de 2018 estabelecia que a lei entraria em vigor 18 meses após a publicação oficial, portanto, a previsão para o término da vacância seria fevereiro de 2020. No entanto, esse prazo foi prorrogado para 24 meses, por força da Lei nº 13.853/19, assim, a lei passaria a entrar em vigor em agosto de 2020. Contudo, recente projeto de lei (PL 5762/2019) foi proposto na Câmara dos Deputados, visando prorrogar o prazo de *vacatio legis* em dois anos, para que a LGPD passe a vigorar a partir de 15 de agosto de 2022.

O projeto de lei justifica-se pelo fato de uma pequena parcela das empresas brasileiras ter dado início ao processo de adaptação às exigências da Lei.

> [...] apenas 17% das instituições consultadas dispõem de iniciativas concretas ou já implementadas em relação à matéria. Além disso, 24% tiveram contato com o tema somente por meio de apresentações, e apenas 24% "têm orçamento específico para colocar em prática ações que garantam a proteção de dados de acordo com as exigências legais[162].

Também é destacada a morosidade do Poder Público na instalação da Autoridade Nacional de Proteção de Dados (ANPD), questionando-se se haveria lapso temporal suficiente para que as propostas de regulamentação sobre a matéria sejam discutidas pela sociedade e aprovadas pelo órgão.

Nesse contexto, questiona-se se a prorrogação do prazo de vacância da lei levaria as iniciativas pública e privada a tomarem as providências para sua adaptação à nova normativa, ou se ocasionaria nova protelação das diligências necessárias ao ajustamento. Além disso, o adiamento da adaptação do país ao referido "nível de proteção adequado", reconhecido internacionalmente e, em alguns casos imposto pela União Europeia, poderia influenciar negativamente nas relações econômicas internacionais do Brasil, sejam essas relações públicas ou privadas.

---

[162] BRASIL. **Projeto de Lei nº 5762/2019**. Altera a Lei nº 13.709, de 2018, prorrogando a data da entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais - LGPD - para 15 de agosto de 2022. Brasília: Congresso Nacional, Câmara dos Deputados, apresentado em 30/10/2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1828120. Acesso em: 21 nov. 2019.

Outro desafio à aplicabilidade da Lei pode ser vislumbrado no tocante à Autoridade Nacional de Proteção de Dados (ANPD). O projeto lei da LGPD previa a criação de uma agência reguladora competente por zelar da proteção dos dados pessoais, entretanto, os artigos referentes à criação e atuação dessa agência foram objeto de veto presidencial por vício de iniciativa, uma vez que uma lei de iniciativa parlamentar, ao criar tal Autoridade, feriria tecnicamente os artigos 2º e 61, §1º, II, da Constituição Federal.

Nesse sentido, a Medida Provisória nº 869/18 foi editada com a finalidade de criar a referida agência reguladora, tendo sido convertida na Lei nº 13.853/19 com veto parcial. A Autoridade Nacional de Proteção de Dados tem previsão legal nos artigos 55-A e seguintes da lei, tendo sido alvo de diversas críticas.

A primeira e mais relevante delas refere-se ao fato de a ANPD ser subordinada ao Poder Executivo, nos termos da parte final do art. 55-A, que qualifica a autoridade como "órgão da administração pública federal, integrante da Presidência da República". Importa, nesse sentido, destacar todo o salientado no tópico 2.1 deste trabalho sobre a importância de que a instituição fiscalizadora seja independente do poder público. Em primeiro lugar, porque o próprio Poder Público é sujeito de fiscalização da Autoridade e, em segundo lugar, para que seja assegurada devida imparcialidade, credibilidade e autonomia de atuação.

Deve ser salientado, no entanto, que a natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, decorridos dois anos da entrada em vigor da estrutura regimental da ANPD (art. 55-A, §§ 1º e 2º).

Um segundo desafio vislumbrado diz respeito à necessidade de pessoas com conhecimento técnico alto para comporem a Autoridade frente à falta de autonomia financeira, o que pode comprometer o interesse de especialistas em proteção de dados no Brasil.

O último empecilho à aplicação efetiva da LGPD diz respeito ao Decreto nº 10.046/19, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

O decreto propõe a criação de um cadastro nacional de dados dos cidadãos brasileiros, em que possa constar desde nome completo, sexo e filiação, até registros das digitais, íris, voz e maneira de andar. Dentre as finalidades de instituição do cadastros podem ser citadas aprimoramento a gestão de políticas públicas e a facilitação do compartilhamento dos dados cadastrais do cidadão entre órgãos da administração pública. Nesse sentido, diversos órgãos do poder público teriam livre acesso aos dados pessoais.

Assim, o decreto divide opiniões entre aqueles que defendem que consiste em uma medida capaz de desburocratizar o serviço público em contraposição aos que acreditam tratar-se de uma deliberação capaz de gerar o que se denomina supervigilância estatal. Além disso, o decreto estabelece novos termos-chave relativos à temática, diversos dos estabelecidos na LGPD.

Nesse sentido, questiona-se se o referido diploma legal não seria uma forma de colocar em xeque as disposições da LGPD frente à administração pública federal. E mais, se não seria um afronta à própria proteção de dados pessoais.

Por fim, destaca-se a importância de que a iniciativa pública e privada tome conhecimento das exigências estabelecidas pela LGPD e adaptem-se à nova lógica jurídica. É de igual relevância que a ANPD seja tornada realidade para passar a atuar junto à sociedade, fazendo jus às suas funções fiscalizadora e consultiva. Tais medidas fazem-se urgentes para garantir a aplicabilidade da Lei e impedir que o direito à proteção de dados seja continuamente desgastado ou simplesmente desconsiderado por alegações de prevalência de interesse e segurança públicas e da lógica de mercado.

5 CONCLUSÃO

O presente trabalho buscou, de início, estabelecer noções iniciais sobre a privacidade, de um aspecto sociológico até as primeiras influências da privacidade em âmbito jurídico. Nesse sentido, foi destacada a primeira abordagem significativa do direito à privacidade na doutrina, através do artigo *"The right to privacy"*, passando-se à análise da evolução do direito à privacidade, que culmina na autonomia do sujeito para delimitar suas esferas públicas e privada, sendo o consentimento grande ferramenta para o exercício da autodeterminação.

No entanto, chama-se atenção para o que se denomina "assimetria informacional", que consiste na disparidade de poder entre os titulares de informação e os seu detentores. Nesse contexto, são destacados os paradoxos da privacidade, consistentes em controvérsias geradas (i) pela crescente utilização da tecnologia e a falsa ideia de privacidade construída, (ii) pelo tratamento de dados que, apesar de serem de âmbito público, são tratados com maior rigidez para que o âmbito privado seja protegido e (iii) pela necessidade de controlar os dados pessoais mesmo quando cedidos a terceiros.

Assim, percebe-se a necessidade de tratar a privacidade enquanto um direito fundamental, criando critérios para a sua tutela e estabelecendo alguns princípios basilares, os quais se prestam à tutela da personalidade do próprio titular de dados. É apresentada, nesse sentido, uma categoria especial de dados pessoais, os dados pessoais sensíveis, que devem ser objeto de proteção mais acentuada tendo em vista seu caráter potencialmente discriminatório. Também são abortados, para além do direito ao sigilo de informações, situações nas quais subsistem o dever de informar, o direito de não saber e até mesmo o direito de não ser lembrado.

Já no que diz respeito especificamente à tutela de dados pessoais, são abordadas perspectivas do seu tratamento sob uma ótica puramente mercadológica, na qual as normas do mercado seriam encarregadas de regularem a própria lógica de proteção de dados, em contraposição a um sistema em que há um conjunto normativo e um mecanismo capaz de zelar pelos interesses do titular de dados pessoais. Nessa perspectiva a tutela de dados pessoais diferencia-se da tutela da privacidade, havendo uma abordagem específica da proteção de dados pessoais e seus principais marcos regulatórios, bem como a diferenciação da abordagem conferida à temática pela União Europeia e pelos Estados Unidos da América, âmbitos completamente antagônicos no tocante à tutela de dados pessoais, sendo que aquela é grande influenciadora de ordenamentos nacionais, abordando a proteção dos dados pessoais como um direito fundamental.

Faz-se, portanto, uma análise da evolução das formas de controle dos dados pessoais, passando do controle individual ao controle por via de mão dupla, no qual o controlador também pode ser controlado, sendo certo a sua materialização se dá por meio do direito de acesso conferido aos titulares de dados. Além disso, é ressaltado o papel de uma autoridade fiscalizadora capaz de efetuar controle difuso dos dados pessoais. No âmbito dessa autoridade, destaca-se a importância de independência do poder público para o exercício eficaz das suas atribuições.

No que diz respeito ao tratamento de dados pessoais, evidencia-se que não há razão para que exista diferenciação entre dados manuais e automatizados, nem entre pessoa física e jurídica enquanto titulares de dados. Também são feitas considerações acerca das exceções criadas às regras de tratamento, bem como da circulação transnacional de dados. Destaca-se, ainda, que o regime de controle de dados abarca o direito de livre acesso, que constitui uma forma de concretizar o controle por via de mão dupla. Assim, relacionou-se o direito de livre acesso à liberdade informacional, em âmbito privado e principalmente público.

O presente trabalho também visou analisar as diferentes formas de tratamento de dados, destacando os riscos quando da utilização inadequada dos dados pessoais, dentre os quais podem ser citados a discriminação e estigmatização social.

Uma vez abordadas as questões pertinentes à privacidade e aos dados pessoais, analisou-se o contexto nacional, abordando diversos diplomas legais que tutelavam, em parte e de forma insuficiente, os dados pessoais. Além disso, observou-se excessiva demora do poder público para sancionar uma lei capaz de tratar da temática de forma clara, extensiva e satisfatória, o que se deu por meio da Lei Geral de Proteção de Dados (LGPD), em 2018.

Nesse sentido, o trabalho prestou-se a analisar conceitos basilares tratados na LGPD, bem como seus princípios. Também foi abordada as formas de tratamento de dados pessoais previstas na lei, dando enfoque especial ao instituto do consentimento, como efetivação da autonomia do sujeito titular de dados. Para além disso, foram abordadas as hipóteses de exceção ao consentimento, o tratamento de dados pessoais sensíveis e o tratamento de dados pessoais de crianças e adolescentes. Por fim, foram expostas dificuldades no que diz respeito à aplicação da lei, a qual se encontra em período de vacância legal.

REFERÊNCIAS

BOFF, Salete Oro; FORTES, Vinícius Borges. **A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil**. Florianópolis: Sequencia, 2014. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552014000100006. Acesso em: 13 nov. 2019.

BOFF, Salete Oro; FORTES, Vinícius Borges. Internet e Proteção de Dados Pessoais: uma Análise das Normas Jurídicas Brasileiras a partir das Repercussões do caso NSA vs. Edward Snowden. **Cadernos do Programa de Pós-Graduação em Direito PPGDir. UFRGS**, Porto Alegre, v. 11, n. 1, p. 340-370, ago. 2016. Disponível em: http://seer.ufrgs.br/ppgdir/article/view/58918/38152. Acesso em: 19 set. 2018.

BRASIL. **Exposição de motivos ao Projeto de Lei n. 2.126/2011**. Brasília, DF: Subchefia de assuntos parlamentares, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/Projetos/ExpMotiv/EMI/2011/86-MJ%20MP%20MCT%20MC.htm. Acesso em: 13 nov. 2019.

BRASIL. Decreto-lei nº. 2.848, de 7 de dezembro de 1940. **Código Penal**. Rio de Janeiro: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 nov. 2019.

BRASIL. Decreto-lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal.** Rio de Janeiro: Presidência da República, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 21 nov. 2019.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 10 nov. 2019.

BRASIL. **Lei complementar nº 104, de 10 de janeiro de 2001**. Altera dispositivos da Lei nº 5.172, de 25 de outubro de 1966 – Código Tributário Nacional. Brasília, DF: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp104.htm. Acesso em: 21 nov. 2019.

BRASIL. **Lei complementar nº 105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp105.htm. Acesso em: 21 nov. 2019.

BRASIL. **Lei complementar nº 166, de 08 de abril de 2019**. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp166.htm. Acesso em: 21 nov. 2019.

BRASIL. **Lei nº 5.250, de 9 de fevereiro de 1967**. Regula a liberdade de manifestação do pensamento e de informação. Brasília, DF: Presidência da República, 1967. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L5250.htm. Acesso em: 21 nov. 2019.

BRASIL. **Lei nº 7.210, de 11 de julho de 1984**. Institui a Lei de Execução Penal. Brasília, DF: Presidência da República, 1984. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7210.htm. Acesso em: 21 nov. 2019.

BRASIL. **Lei nº 7.232, de 29 de outubro de 1984**. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Brasília, DF: Presidência da República, 1984. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L7232.htm. Acesso em: 21 nov. 2019.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 21 nov. 2019.

BRASIL. **Lei nº 9.507, de 15 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Brasília, DF: Presidência da República, 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm. Acesso em: 10 nov. 2019.

BRASIL. Lei nº 10.406 de 10 de janeiro de 2002. **Código Civil**. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 22 out. 2019.

BRASIL. **Lei nº 12.037, de 1º de outubro de 2009**. Dispõe sobre a identificação criminal do civilmente identificado, regulamentando o art. 5º, inciso LVIII, da Constituição Federal. Brasília, DF: Presidência da República, 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L12037.htm. Acesso em: 21 nov. de 2019.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Acesso em: 21 nov. de 2019.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º [...]. Brasília, DF: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 21 nov. de 2019.

BRASIL. **Lei nº 12.654, de 28 de maio de 2012**. Altera as Leis nºs 12.037, de 1º de outubro de 2009, e 7.210, de 11 de julho de 1984 - Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12654.htm. Acesso em: 21 nov. de 2019.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 21 nov. de 2019.

BRASIL. **Lei nº 12.965, de 23 de Abril de 2014**. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 nov. de 2019.

BRASIL. Lei nº 13.105, de 16 de março de 2015. **Código de Processo Civil.** Brasília, DF: Presidência da República, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 22 out. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). 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, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 nov. de 2019.

BRASIL. **Nota técnica 92/2018**. Brasília, DF: Ministério da Justiça e Segurança Pública, 2018. Disponível em: http://www.cmlagoasanta.mg.gov.br/abrir_arquivo.aspx/PRATICAS_ABUSIVAS_DECOLARCOM?cdLocal=2&arquivo=%7BBCA8E2AD-DBCA-866A-C8AA-BDC2BDEC3DAD%7D.pdf. Acesso em: 13 nov. 2019.

BRASIL. **Projeto de Lei nº 5762/2019**. Altera a Lei nº 13.709, de 2018, prorrogando a data da entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais - LGPD - para 15 de agosto de 2022. Brasília: Congresso Nacional, Câmara dos Deputados, apresentado em 30/10/2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1828120. Acesso em: 21 nov. 2019.

BRASIL. Superior Tribunal de Justiça. **Informativo 588**. O termo inicial do prazo de permanência de registro de nome de consumidor em cadastro de proteção ao crédito (art. 43, § 1º, do CDC) inicia-se no dia subsequente ao vencimento da obrigação não paga, independentemente da data da inscrição no cadastro. Brasília, DF: STF, 2016, p. 13. Disponível em: https://scon.stj.jus.br/SCON/SearchBRS?b=INFJ&tipo=informativo&livre=@COD=%270588%27. Acesso em: 21 nov. 2019.

BRASIL. Superior Tribunal de Justiça (4. Turma). **Recurso Especial 870.582/SP**. Relator: Ministro Aldir Passarinho Junior. Julgado em 23/10/2007.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1.334.097/RJ**. Relator: Ministro Luis Felipe Salomão. Data de julgamento: 28 de maio de 2013.

BRASIL. Superior Tribunal de Justiça. **Súmula 323**. A inscrição do nome do devedor pode ser mantida nos serviços de proteção ao crédito até o prazo máximo de cinco anos, independentemente da prescrição da execução. Segunda Seção, 23 nov. 2005. Disponível em: https://ww2.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2011_26_capSumula323.pdf. Acesso em: 21 nov. 2019.

BRASIL. Supremo Tribunal Federal (2. Turma). **Mandado de Segurança 23.669- DF**. Ministro Celso de Mello. Decisão liminar proferida em 12 de abril de 2000.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 973.837/MG**. Relator: Ministro Gilmar Mendes.

BRASIL. Supremo Tribunal Federal (2. Turma). **Recurso Extraordinário 219.780.** Relator: Ministro Carlos Velloso. Julgado em 13/04/1999.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário 418.416.** Relator: Ministro Sepúlveda Pertence. Julgado em 10/05/2006.

BRASIL. Tribunal Superior do Trabalho. **Súmula 443**. Disponível em: http://www3.tst.jus.br/jurisprudencia/Sumulas_com_indice/Sumulas_Ind_401_450.html. Acesso em: 21 nov. 2019.

COSTA JUNIOR. Paulo José. **O direito a estar só: tutela penal da intimidade**. 4. ed. revisada e atualizada. São Paulo: Editora Revista dos Tribunais, 2007.

DISTRITO FEDERAL. **Portaria nº 02/2018, de 20 de março de 2018**. Brasília, DF: Ministério Público do Distrito Federal e Territórios, 2018. Disponível em: http://www.mpdft.mp.br/portal/pdf/noticias/Mar%C3%A7o_2018/Instauracao_de_ICP_Cambridge_Analytica.pdf. Acesso em: 12 nov. 2019.

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

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Capítulo 1. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. Iguais mas Separados: o Habeas Data no Ordenamento Brasileiro e a Proteção de Dados Pessoais. **Cadernos da Escola de Direito**, Centro Universitário Autônomo do Brasil. Paraná: 2008. Disponível em: http://revistas.unibrasil.com.br/cadernosdireito/index.php/direito/article/view/444. Acesso em: 31 out. 2018.

DRUMMOND, Victor. **Internet, privacidade e dados pessoais.** Rio de Janeiro: Editora Lumen Juris, 2003.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista Da Faculdade De Dire**ito, Universidade De São Paulo, 1993, 439-459. Disponível em: http://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 07 nov. 2019.

FORTES, Pedro Rubim Borges. MARTINS, Guilherme Magalhães. OLIVEIRA, Pedro Farias. O consumidor contemporâneo no show de Truman: a geodiscriminação digital como prática ilícita no direito brasileiro. **Revista de Direito do Consumidor**, vol. 124, p. 235-260, jul.-ago. 2019.

FRAZÃO, Ana. **A nova Lei Geral de Proteção de Dados Pessoais**: Principais repercussões para a atividade empresarial. Parte I. 2018a. Disponível em https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018. Acesso em 20 set. 2018.

FRAZÃO, Ana. **A nova Lei Geral de Proteção de Dados**: Repercussões para a atividade empresarial: a importância do consentimento para o tratamento dos dados pessoais. Parte III. 2018b. Disponível em https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018 Acesso em 20 set. 2018.

FRAZÃO, Ana. **A nova Lei Geral de Proteção de Dados**: Repercussões para a atividade empresarial: o alcance da LGPD. Parte II. 2018c. Disponível em https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-alcance-da-lgpd-e-repercussoes-para-a-atividade-empresarial-05092018 Acesso em 20 set. 2018.

FRAZÃO, Ana. **Geo pricing e geo blocking.** As novas formas de discriminação de consumidores e os desafios para o seu enfrenamento. 2018d. Disponível em http://anafrazao.com.br/files/publicacoes/2018-08-15-Geo_pricing_e_geo_blocking_As_novas_formas_de_discriminacao_de_consumidores_e_os_desafios_para_o_seu_enfrentamento.pdf. Acesso em 12 nov. 2019.

FRAZÃO, Ana. **Nova LGPD**: as demais hipóteses de tratamento de dados pessoais. Parte IV. 2018e. Disponível em https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018. Acesso em 22 set. 2018.

GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado**. 1. ed. São Paulo: Atlas, 2017. Disponível em: https://www.academia.edu/37321091/Edoc.site_marco_civil_da_internet_comentado_2017_victor_hugo. Acesso em: 16 nov. 2019.

HARARI, Yuval Noah. **The meaning of life in a world without work**. The Guardian, 2017. Disponível em: https://www.theguardian.com/technology/2017/may/08/virtual-reality-religion-robots-sapiens-book. Acesso em: 13 nov. 2019.

JEREISSATI, Régis Gurgel do Amaral; DIAS, Eduardo Rocha. **Legitimidade ativa dos sucessores e do cônjuge ou companheiro sobrevivente para impetração do habeas data sob a ótica da preservação da privacidade do morto.** Civilistica.com: Rio de Janeiro, 2017. Disponível em: http://civilistica.com/wp-content/uploads/2017/08/Jereissati-e-Dias-civilistica.com-a.6.n.1.2017.pdf. Acesso em: 14 nov. 2019.

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

LIMBERGER, Têmis. **O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais**. Porto Alegre: Livraria do advogado editora, 2007.

MANNHEIM, Karl. **Diagnóstico de nosso tempo**. 3. edição. Rio de Janeiro: Zahar Editores, 1973.

OLIVEIRA, Rogerio Alvarez; ALVAREZ, Wanessa Gonçalves. **Particularidades atuais da quebra de sigilo bancário**. Publicado em 03/04/2017. Disponível em: https://www.conjur.com.br/2017-abr-03/mp-debate-particularidades-atuais-quebra-sigilo-bancario-parte. Acesso em: 15 nov. 2019.

ORGANISATION MONDIALE DE LA SANTÉ. **Droits de l'homme et progrès de la science et de la technique**. [S. l.]: Organisation Mondiale da la Santé, 1969. Disponível em: https://apps.who.int/iris/bitstream/handle/10665/186511/WHA22_PB-9_fre.pdf;jsessionid=D0A9D21B1684C8D2CAF32855F803FF2B?sequence=1. Acesso em: 22 out. 2019.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos do Homem**. [S. l.]: ONU, 1948. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 09 nov. 2019.

PORTUGAL. **Lei da Protecção Dados Pessoais** (transpõe para a ordem jurídica portuguesa a Directiva n.º 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 dados pessoais e à livre circulação desses dados). Disponível em: https://www.cnpd.pt/bin/legis/nacional/lei_6798.htm. Acesso em: 01 out. 2018.

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. A Proteção de Dados Pessoais na Internet no Brasil: Análise de decisões proferidas pelo Supremo Tribunal Federal. **Cadernos do Programa de Pós-Graduação em Direito – PPGDir./UFRGS.** Porto Alegre, dez. 2016. Disponível em: http://seer.ufrgs.br/ppgdir/article/view/61960/39936. Acesso em: 19 set. 2018.

RIBEIRO, Luciana Antonini. A privacidade e os arquivos de consumo na internet - uma primeira reflexão. **Revista de Direito do Consumidor**, v. 41, p. 151 – 165, jan.-mar. de 2002. Doutrinas Essenciais de Responsabilidade Civil, v. 8, p. 1151-1168, out. de 2011.

RODOTÁ, Stefano. **A vida na sociedade da vigilância- a privacidade hoje.** Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. **Elaboratori elettronici e controllo sociale**. Bologna: Il mulino, 1973.

RODOTÀ, Stefano. **Tecnologie e diritti**. Bologna: Il mulino, 1995.

SCHMIDT, Sarah. Privacidade em disputa no Brasil: Marco Civil da Internet, dados pessoais e o "PL Espião". **Ciência e cultura**, São Paulo, v. 68, n. 1, p. 8-10, mar. de 2016. Disponível em: http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252016000100004&lng=en&nrm=iso. Acesso em: 19/09/2018.

SCHREIBER, Anderson. **Direitos da Personalidade.** 2ª edição. São Paulo: Atlas, 2013.

SCHREIBER, Anderson. **Os Direitos da Personalidade e o Código Civil de 2002.** Publicado em 13/05/2013. Disponível em: http://www.andersonschreiber.com.br/downloads/Os_Direitos_da_Personalidade_e_o_Codigo_Civil_de_2002.pdf. Acesso em: 20 nov. 2018.

SCHREIBER, Anderson. **Proteção de Dados Pessoais no Brasil e na Europa.** Publicado em 05/09/2018. Disponível em: http://www.cartaforense.com.br/conteudo/colunas/protecao-de-dados-pessoais-no-brasil-e-na-europa/18269. Acesso em: 26 set. 2018.

SHILLS, Edward. ***Privacy***: its constitution and vicissitudes, law and contemporary problems. Durham: N.C. School of Law, Duke University, 1966, p. 281-306. Disponível em: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3109&context=lcp. Acesso em: 22 nov. 2019.

UNIÃO EUROPEIA. Agência dos Direitos Fundamentais. **Manual da legislação européia sobre proteção de dados**. Luxemburgo: Serviço das publicações da União Europeia, 2014.

UNIÃO EUROPEIA. Parlamento Europeu e Conselho. **Regulamento (UE) 2016/679, de 27 de abril de 2016**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: http://data.europa.eu/eli/reg/2016/679/oj. Acesso em: 19 set. 2018.

UNIÃO EUROPEIA. Tribunal Europeu de Direitos Humanos. **Niemietz v. Alemanha**, 72/1991/324/396, seção 29. Julgado em 16 de dezembro de 1992.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**. Cambridge, v. 4, n. 5. p. 193-220, dec. 15, 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 22 nov. 2019.

WEBB, Maureen. **Illusions of security: global surveillance and democracy in the post-11/9 word**. City Lights: San Francisco, 2007.

ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do *right of privacy* nos Estados Unidos**. Revista Brasileira de Direito Civil**. Rio de Janeiro, v. 3, p. 8-27, jan./mar. 2015, p. 10. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/107/103. Acesso em: 22 nov. 2019.