

**UNIVERSIDADE FEDERAL DE SANTA CATARINA  
CENTRO DE CIÊNCIAS JURÍDICAS  
CURSO DE GRADUAÇÃO EM DIREITO**

**MARIA VICTORIA ANTUNES KRIEGER**

**A ANÁLISE DO INSTITUTO DO CONSENTIMENTO FRENTE À LEI GERAL DE  
PROTEÇÃO DE DADOS DO BRASIL (LEI Nº 13.709/18)**

**FLORIANÓPOLIS**

**2019**

UNIVERSIDADE FEDERAL DE SANTA CATARINA  
CENTRO DE CIÊNCIAS JURÍDICAS  
CURSO DE GRADUAÇÃO EM DIREITO

**A ANÁLISE DO INSTITUTO DO CONSENTIMENTO FRENTE À LEI GERAL DE  
PROTEÇÃO DE DADOS DO BRASIL (LEI Nº 13.709/18)**

Trabalho de Conclusão de Curso apresentado ao  
Curso de Direito da Universidade Federal de Santa  
Catarina, como requisito para a obtenção do título  
de Bacharel em Direito.

Orientador: Prof. Dr. Mikhail Vieira de Lorenzi  
Cancelier

FLORIANÓPOLIS

2019

Ficha de identificação da obra elaborada pelo autor,  
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Krieger, Maria Victoria Antunes  
A ANÁLISE DO INSTITUTO DO CONSENTIMENTO FRENTE À LEI  
GERAL DE PROTEÇÃO DE DADOS DO BRASIL (LEI N° 13.709/18) /  
Maria Victoria Antunes Krieger ; orientador, Mikhail  
Vieira de Lorenzi Cancelier, 2019.  
83 p.

Trabalho de Conclusão de Curso (graduação) -  
Universidade Federal de Santa Catarina, Centro de Ciências  
Jurídicas, Graduação em Direito, Florianópolis, 2019.

Inclui referências.

1. Direito. 2. Consentimento. 3. Dados Pessoais. 4.  
Autodeterminação Informativa. 5. Lei Geral de Proteção de  
Dados Pessoais. I. Cancelier, Mikhail Vieira de Lorenzi .  
II. Universidade Federal de Santa Catarina. Graduação em  
Direito. III. Título.


UNIVERSIDADE FEDERAL DE SANTA CATARINA  
CENTRO DE CIÊNCIAS JURÍDICAS  
COLEGIADO DO CURSO DE GRADUAÇÃO EM DIREITO


TERMO DE APROVAÇÃO

O presente Trabalho de Conclusão de Curso, intitulado "A análise do instituto do consentimento frente à Lei Geral de Proteção de Dados do Brasil (Lei nº 13.709/18)", elaborado pela acadêmica Maria Victoria Antunes Krieger, defendido em 05/12/2019 e aprovado pela Banca Examinadora composta pelos membros abaixo assinados, obteve aprovação com nota 10 (DEZ), cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

Florianópolis, 05 de dezembro de 2019

  
\_\_\_\_\_  
**Mikhail Vieira de Lorenzi Cancellier**  
Professor Orientador

  
\_\_\_\_\_  
**Camila Kohn de Cristo**  
Membro de Banca

  
\_\_\_\_\_  
**Lucas Moser Goulart**  
Membro de Banca



**Universidade Federal de Santa Catarina**  
**Centro de Ciências Jurídicas**  
**COORDENADORIA DO CURSO DE DIREITO**

**TERMO DE RESPONSABILIDADE PELO INEDITISMO DO TCC E**  
**ORIENTAÇÃO IDEOLÓGICA**

Aluna: Maria Victoria Antunes Krieger  
RG: 5.493.439  
CPF: 066.230.209-50  
Matrícula: 15100128  
Título do TCC: A análise do instituto do consentimento frente à Lei Geral de Proteção de Dados do Brasil (Lei nº 13.709/18)  
Orientador: Mikhail Vieira de Lorenzi Cancelier

Eu, Maria Victoria Antunes Krieger, acima qualificada; venho, pelo presente termo, assumir integral responsabilidade pela originalidade e conteúdo ideológico apresentado no TCC de minha autoria, acima referido

Florianópolis, 05 de dezembro de 2019.

---

MARIA VICTORIA ANTUNES KRIEGER

*“Ninguém é suficientemente competente para governar outra pessoa sem o seu consentimento”.*

(Abraham Lincoln)

## **AGRADECIMENTOS**

Hoje, chego ao fim de uma importante etapa da vida segura e confiante de que fiz o meu melhor nesses anos, junto dos melhores.

Aos meus pais, agradeço por todo incentivo, dedicação, amor e compreensão. Obrigada por nunca terem duvidado de mim nessa trajetória e por serem meu maior alicerce. Vocês são meus exemplos de vida e, enquanto seguir seus passos, tenho a certeza de que estarei no caminho certo.

Agradeço também aos meus avós, minha afilhada, tias, tios, primas e primos, que, mesmo de longe, transmitiam amor, paz e compreenderam minha ausência nos últimos tempos – eu amo muito todos vocês.

Muito obrigada, meus amigos! Tanto aqueles que me acompanham desde sempre quanto aqueles que conheci nos últimos tempos: vocês foram elementos fundamentais para eu chegar até aqui. Obrigada pelas alegrias compartilhadas, pelas tristezas divididas e por todos os momentos que guardarei para sempre comigo.

Por fim, agradeço a todos os professores que encontrei durante minha fase escolar, desde o ensino fundamental até o último ano da graduação. Foi cada um de vocês que através de um gesto, uma palavra, ou um sorriso tornaram minha jornada exitosa – vocês são os melhores.

Em especial, agradeço ao meu orientador, Prof. Dr. Mikhail, que desde as primeiras fases demonstrou ser amigo e um grande profissional, um exemplo que pretendo seguir. Obrigada pela paciência, por todo o apoio e por acreditar em mim.

Ao passar do tempo, os degraus se tornam mais altos e a caminhada mais pesada, mas tudo se pode com o apoio destes e de tantos outros que confiam e me ajudam a seguir sempre em frente. Muito obrigada!

## RESUMO

O presente trabalho tem como objetivo analisar o instituto do consentimento no tocante à proteção de dados pessoais, pairando detalhadamente sobre a nova Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18). Diante de uma realidade na qual para estar incluído no meio social é preciso estar online, os dados pessoais acabaram por se tornar moedas de troca no mercado e sua proteção se tornou indispensável para resguardar os direitos dos seus titulares. Nesse sentido, mundialmente se buscou a instituição do consentimento como suporte, inicialmente como única medida e posteriormente em um rol dentre outras, a fim de instituir os indivíduos suas autodeterminações informativas. Porém, sabe-se que, em verdade, por falta de informação ou dentre tantos outros motivos, tal medida protetiva pode se tornar falha se não bem regulada. No Brasil, foi apenas no ano de 2018, com a entrada em vigor em 2020, que surgiu a primeira norma específica sobre a matéria: a LGPD. Partindo de uma análise bibliográfica acerca do tema, fazendo um paralelo com as normas de outros sistemas jurídicos, assim como com as leis brasileiras anteriores à LGPD, o estudo se destina a verificar os limites e alcances do instituto do consentimento atual no ordenamento jurídico brasileiro.

**Palavras-Chave:** Consentimento. Dados Pessoais. Autodeterminação Informativa. LGPD.



## **ABSTRACT**

The current study had the aim of analyzing the institute a consent for protection of personal data, detailing in a new General Law of Personal Data (N. 13.709/18). Before a reality which to be included in the social environment is necessary be online, personal data become currencies in the market and your protection has become indispensable to secure holder's rights. In this sense, sought worldwide a consenting as a support, first like the only measure and later on a roll whit others, an institute for the self-determining informative of individuals. However, it is known that in fact, due to lack of information or for other reasons, such protective measure can cause failure if will not properly regulated. In Brazil, it was not until 2018, wich came into force in 2020, that the first specific norm on a subject emerged: the LGPD. Starting from a bibliography analysis on the subject, paralleling the norms of other legal systems, as well as the Brazilian laws sectoral to LGPD, this study purpose verify the limits and scope of the consent institute in the Brazilian legal system.

**Keywords:** Consent. Personal Data. Self-determining Informative. LGPD.

## **LISTA DE ABREVIATURAS E SIGLAS**

CDC – Código de Defesa do Consumidor

CF/88 – Constituição Federal de 1988

GDPR – *General Data Protection Regulation*

LCP – Lei do Cadastro Positivo

LGPD – Lei Geral de Proteção de Dados Pessoais

MCI – Marco Civil da Internet

PL – Projeto de Lei

STJ – Superior Tribunal de Justiça

## SUMÁRIO

<b>1. INTRODUÇÃO .....</b>	<b>12</b>
<b>2. NOÇÃO GERAL SOBRE DADOS PESSOAIS.....</b>	<b>14</b>
2.1 Conceito.....	14
2.2 A importância da Proteção dos Dados Pessoais na Sociedade da Informação.....	20
2.3 Proteção dos Dados Pessoais e o Direito à Privacidade .....	26
<b>3. O INSTITUTO DO CONSENTIMENTO FRENTE À PROTEÇÃO DOS DADOS PESSOAIS .....</b>	<b>33</b>
3.1 Dualidade do consentimento: autodeterminação informativa e meio de legitimação para o tratamento de dados pessoais .....	35
3.2 Pressupostos de validade: a “adjetivação” do consentimento .....	40
3.2.1 Consentimento informado.....	41
3.2.2 Consentimento livre.....	44
3.2.3 Consentimento inequívoco e com finalidades determinadas .....	45
3.3 Dificuldades e desafios do consentimento no contexto do intenso fluxo informacional.....	46
<b>4. TRAJETÓRIA NORMATIVA DO CONSENTIMENTO ATÉ A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS DO BRASIL (LEI N. 13.709/18) .....</b>	<b>53</b>
4.1 Os basilares Regulamentos da União Europeia.....	56
4.2 As Principais normas Setoriais brasileiras anteriores à LGPD .....	62
4.3 A Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18).....	69
<b>5. CONSIDERAÇÕES FINAIS .....</b>	<b>76</b>
<b>REFERÊNCIAS.....</b>	<b>79</b>

## 1. INTRODUÇÃO

A atual sociedade da informação, resultante das rápidas e constantes mudanças nas tecnologias dos últimos tempos, transformou o modo de se relacionar entre os indivíduos: o que antes era feito através de encontros presenciais e registrados em álbuns de fotografias agora é realizado em chats e publicado nas redes sociais. Sob este novo cenário, os dados pessoais dos usuários passaram a ser a base da economia online.

Neste ambiente, as plataformas digitais oferecem aos seus consumidores serviços taxados como “gratuitos”, uma vez que não há a cobrança do acesso através de boletos ou cartões que possam ser sentidos no bolso. Contudo, tal relação está além da benevolência das empresas.

Em verdade, a moeda encontra-se no fornecimento de dados pelos usuários, ainda que inconscientemente, os quais são coletados, tratados e muitas vezes compartilhados com terceiros, movimentando grandes fortunas e movidos por um mercado no qual o cerne está na publicidade direcionada.

A título exemplificativo, tem-se a ferramenta denominada de “cookies”, por meio da qual rastreia-se as navegações dos indivíduos e, com o resultado, segmenta-se em categorias diversas correlacionadas com anúncios publicitários específicos.

O consumidor, assim, está sob constante vigilância, sendo seus hábitos monitorados a todo o momento e registrados, para, por fim, receberem (sem autorização dos mesmos, na maioria das vezes) publicidades conforme suas preferências e opções anteriores.

Dentre os dilemas causados por tal atitude, ressalta-se os malefícios da exposição indesejada, da possível discriminação e da falta de controle sobre suas próprias informações.

Nesse momento, portanto, a principal angústia está relacionada com os direitos dos titulares sobre seus dados pessoais, que constantemente sofrem invasão devido a objetivos econômicos buscados por estas empresas: a proteção dos dados pessoais torna-se indispensável para a proteção da privacidade dos internautas.

Dentre os regulamentos jurídicos sobre o tema, surge o importante instituto do consentimento o qual, inclusive, por muito tempo foi o cerne das disciplinas e ganhou grande destaque tendo em vista a autodeterminação informativa advinda de tal.

A respeito dele, ao usuário passa a ser assegurado o direito à informação prévia e atualizada, podendo optar pela coleta ou compartilhamento e revogá-la, a qualquer momento.

Para tanto, as informações a serem repassadas aos indivíduos passou a ser o centro das preocupações, uma vez que apenas com o conhecimento claro acerca dos usos e finalidades o consentimento se tornará válido.

Contudo, na realidade, o que se vê são termos de usos com palavras rebuscadas, de muitas páginas, dificilmente lidos e entendidos por aqueles que utilizam as plataformas, fato pelo qual traz um dilema ao instituto que precisa ser contornado pelas legislações.

A previsão jurídica do instituto já foi muito debatida mundialmente, em especial na Europa, que desde a sua Carta de Direitos Fundamentais da União Europeia já previa explicitamente a proteção dos dados pessoais como um direito fundamental.

Contudo, no Brasil, apenas em 2018 com a Lei Geral de Proteção de Dados Pessoais o tema recebeu a sua devida atenção. Por meio desse diploma, o consentimento apresenta-se como uma dentre outras medidas autorizadas da coleta, tratamento e compartilhamento das informações dos usuários, passando a ser adjetivado a fim de evitar a invalidade de tal instituto.

Diante deste cenário, o presente trabalho parte do método dedutivo a fim de verificar as mudanças trazidas em relação ao consentimento com esta nova lei.

Inicialmente, no primeiro capítulo, será analisado alguns conceitos básicos imprescindíveis neste cerne para, assim, chegar ao instituto do consentimento em si no segundo capítulo, analisando suas características e especificidades neste tema.

Já no terceiro capítulo, a análise será frente à proteção de dados pessoais, em especial com as principais leis europeias que servirão de base para o Brasil e as setoriais normas brasileiras, com a atenção final à Lei n. 13.709/18 que entrará em vigor em agosto de 2020.

## 2. NOÇÃO GERAL SOBRE DADOS PESSOAIS

Sob o viés da crescente e rápida evolução ocorrida nos meios digitais, principalmente no final do século XX, as relações sociais se apresentam com uma nova vertente, por meio da qual eliminou-se obstáculos e o mundo todo pode se conectar rápida e simultaneamente.

Assim, tendo em vista a realidade proporcionada pelo *Big Data*<sup>1</sup> e por todo o cenário de informações trocadas online, as interações sociais passam a estar cada vez mais à mercê da tecnologia, possibilitando, assim, o surgimento dos dados pessoais e sua relevância no mundo jurídico.

Neste panorama, o primeiro capítulo deste trabalho tem por objeto e propósito apresentar uma noção geral sobre os dados pessoais, identificando o seu conceito e as suas características, bem como a sua relação com o direito à privacidade e sua tutela primordial em meio à sociedade de informação.

### 2.1 Conceito

Os dados pessoais aqui abordados compreendem certas especificações para serem caracterizados. Inicialmente, tem-se que o termo “dado” manifesta uma informação antes mesmo de ela ser interpretada ou de passar por um processo de elaboração (DONEDA, 2011, p. 93).

Neste sentido, conforme denota Bioni (2018, p. 36), os “dados são simplesmente fatos brutos”, os quais necessitam passar por certo mecanismo de processamento e serem organizados para que possam transmitir alguma informação.

Conforme disciplina de Raymond Wacks, trazida por Mendes (2014, p. 55), tal termo pode estar assimilado à uma “informação em potencial”: o dado apenas será transformado em informação após passar por tratamento<sup>2</sup>.

A partir do momento que une-se o dito vocábulo ao termo “pessoal”, surge um vínculo objetivo que o relaciona a determinada pessoa, de modo que as informações

---

<sup>1</sup> O termo *Big Data* refere-se a dados que extrapolam a capacidade de processamento de sistemas de banco de dados convencionais – representa um enorme de dados complexos, em constante movimento, sejam eles estruturados ou não. (DUMBILL, Edd. Getting up to speed whit big data. In: Big data now: 2012 edition. 2012, p. 3).

<sup>2</sup> A expressão “tratamento de dados” designa as diversas operações técnicas que podem ser realizadas sobre dados pessoais para reduzir a informação e torná-la mais valiosa ou útil (MENDES, 2014, p. 58).

passam a possuir características desta ou, ainda, apresentar dados sobre seus atos e/ou suas manifestações (DONEDA, 2011, p. 94).

Segundo Ronaldo Lemos (2019), em entrevista à imprensa do Superior Tribunal de Justiça<sup>3</sup>, tais dados podem ser considerados como as representações dos indivíduos no mundo virtual, de modo que as decisões a serem tomadas sobre as pessoas nesse meio se darão a partir deles.

Pode-se dizer, ainda, que o conceito contempla aqueles dados que além de indicarem atos de uma pessoa, também identificam seus pensamentos e seu modo de agir. Tendo em vista sua exposição, há a possibilidade de eles passarem pelo processo, via digital, de coleta, armazenamento, processamento ou, inclusive, transferência a terceiros (SANTOS, 2014, p. 351).

Neste sentido, Doneda (2006, p. 156) contempla:

Uma determinada informação pode possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela. Este vínculo significa que a informação refere-se às características ou ações desta pessoa, que podem ser a ela atribuídas em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então, às informações provenientes de seus atos, como os dados referentes ao seu consumo, informações provenientes de suas manifestações, como as opiniões que manifesta, e tantas outras.

Para uma definição doutrinária dos dados pessoais, surgem duas correntes que apresentam amplitudes conceituais distintas: a expansionista e a reducionista. Em relação à primeira visão, o titular<sup>4</sup> em questão é uma pessoa identificável, indeterminada. Para tal, o vínculo desse indivíduo com o seu dado é mediato, indireto, impreciso ou inexato, de modo que surge um alargamento da qualificação dos dados como pessoal.

Já para a corrente reducionista, o titular é uma pessoa específica, identificada, sendo o seu vínculo com o dado tido como imediato, direto, preciso, conquanto retrai-se a qualificação do dado como pessoal (BIONI, 2018, p. 68).

Em termos legais, apesar de existirem leis anteriores definindo a expressão, o conceito mais relevante de dados pessoais surge com o Regulamento 2016/69 da União Europeia, denominado de *General Data Protection Regulation* (GDPR), o qual

---

<sup>3</sup> Disponível em <http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Debater-a-Lei-Geral-de-Protecao-de-Dados-e-refletir-sobre-o-futuro--afirma-ministro-Salomao.aspx>.

<sup>4</sup> Segundo o art. 5º, V, da Lei 13.709/18, titular é a pessoa natural da qual se referem os dados pessoais objeto de tratamento.

utiliza-se das diretrizes da corrente expansionista. Por meio do seu art. 4º, n. 1, o dito Regulamento define<sup>5</sup>:

«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

Tamanha é a importância do vínculo entre o dado e o seu titular para a sua caracterização que “os dados pessoais chegam a fazer as vezes da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável” (DONEDA, 2011, p. 92).

Na mesma linha conceitual do diploma europeu, agora em âmbito nacional, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18) indica, em seu artigo 5º, inciso I, que dado pessoal é a informação relacionada à pessoa natural identificada ou identificável.

Observa-se, assim, que a lei brasileira também apresenta um conceito amplo (característico da corrente expansionista), sem rol exemplificativo, de modo que possibilita classificar qualquer dado como um dado pessoal, independente do seu suporte e formato, seja ele isolado ou em conjunto de outro, desde que consiga identificar uma pessoa natural.

Assim, tendo em vista a amplitude conceitual, pode-se inferir que os dados pessoais destoam uma miríade de informações, partindo desde os dados cadastrais (nome, endereço e e-mail, a título exemplificativo) até dados mais intrínsecos, como raça, saúde, política e dados biométricos do seu titular (LIMA, 2014, p. 155).

Sobre estes últimos, destaca-se a subespécie dos dados pessoais denominada de “dados sensíveis”, a qual, segundo a Lei nº 13.709/18, define-se como:

Art. 5º Para os fins desta Lei, considera-se:

[...]

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

São eles, portanto, aqueles dados alusivos a uma pessoa identificada ou identificável que, quando conhecidos e processados, têm o potencial de gerar certa

---

<sup>5</sup> Versão em português disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=DA>.



utilização discriminatória ou lesiva, apresentado maiores riscos para o titular ou para a coletividade, de modo que devem ser considerados como sensíveis e possuir um tratamento diferenciado quanto ao controle sobre seus usos.

Essa categoria de dados foi consagrada pelo Convênio 108, editado pelo Conselho da Europa em 1861, o qual delimitou que apenas poderiam ser objeto de uso os dados sensíveis que tivessem no direito interno local resguardadas as garantias adequadas para tal (MENDES, 2014, p. 72).

Segundo a consideração n. 51 do *General Data Protection Regulation*, estes dados são assim considerados devido a sua natureza, por estarem relacionados a direitos e liberdades fundamentais, e, conseqüentemente, merecem uma proteção especial. Neste diploma, ressalta-se a inclusão daqueles dados que identifiquem a origem racial ou étnica do seu titular.

Supletiva ao regulamento europeu, advém a Diretiva 95/46 da União Europeia que indica:

Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.

Além deste rol presente na Diretiva, faz-se necessário indicar a necessária proteção de outros dados triviais que, em que pese possam parecer insignificantes, podem acabar se tornando um dado sensível, devido a usos indiscriminados e através de ferramentas como o *Big Data*, capazes de redimensionar uma base de dados.

A título exemplificativo, Bioni (2018, p. 86) relembra o estudo apresentado pela Universidade de Cambridge<sup>6</sup>, publicado na revista científica PNAS (*Proceedings of National Academy of Sciences*), que identificou que, a partir das então inofensivas “curtidas” dos usuários na rede social Facebook, tornou-se possível criar perfis dos usuários, incluindo seus gostos e preferências. Com o resultado da pesquisa, destacou-se o fiel percentual de usuários brancos e negros, republicanos e democratas, como também os homossexuais e heterossexuais entre os analisados.

Na conclusão do trabalho, os pesquisadores destacam ainda, conforme menciona Marineli (2017, p. 200), “a grave ameaça presente à privacidade da pessoas, decorrentes da utilização desses dados por empresas e instituições governamentais”.

---

<sup>6</sup> Disponível em <https://www.pnas.org/content/110/15/5802>.

Sob este mesmo ângulo, tem-se o caso das “listas negras” utilizadas por empregadores para estabelecer um registro de trabalhadores que tenham realizado algo que não seja bem visto por certas empresas (como no caso de terem acionado a Justiça), a fim de que não tivessem eles mais acesso ao mercado de trabalho. Segundo o entendimento do Tribunal Superior do Trabalho<sup>7</sup>, a referida lista tornou-se inadmissível, ensejando indenização à título de dano moral para aqueles que tenham seu nome colocado, tendo em vista o intuito discriminatório da medida (MENDES, 2014, p. 77).

Destaca-se mais uma vez o cuidado necessário para a categorização dos dados sensíveis, uma vez que tal ato pode apresentar inúmeros revés na era da informação. Inicialmente, percebe-se a dificuldade de se identificar previamente quais serão os efeitos que surgirão no futuro com a utilização de determinado dado, tendo em vista que “um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo” (DONEDA, 2006, p. 162).

Ademais, a proibição completa do uso dos dados sensíveis, como é o caso da lei portuguesa de proteção de dados pessoais (Lei n. 67/98)<sup>8</sup>, acaba se tornando deveras prejudicial e se torna aquém de uma solução plausível na atualidade, tendo em vista que esses dados se fazem úteis e necessários em determinadas situações, como no caso de pesquisas médicas.

Nesse sentido, há estudos que buscam uma melhor maneira de utilização dos dados. Tanto isso é verdade que uma das experiências mais aclamadas por especialistas na área, trazida por Ventura e Coeli<sup>9</sup>, é a do *Population Data BC*, a qual apresenta um modelo “como um terceiro confiável que faz a mediação entre pesquisadores e gestores das bases de dados da província de British Columbia (Canadá)”, sendo destes a palavra final a respeito do uso dos dados.

No tocante à segurança dos dados tratados, a pesquisa introduz “princípios legais de privacidade a uma avaliação de riscos das demandas de acesso às bases

---

<sup>7</sup> RR 325/2001-091-09-00.7, julgado em 2-4-2008, rel. Min. Maria de Assis Calsing, 4ª Turma, DJ 18-4-2008.

<sup>8</sup> A Lei n. 67/98 de Portugal prevê, em seu art. 7º, 1, a proibição do tratamento dos dados que aqui indicamos como sensíveis (convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, relativos à saúde e vida sexual), cabendo exceção apenas quando houver interesse vital do seu titular e seja ele impossibilidade de manifestar consentimento, quando forem públicos pelo próprio titular ou quando os dados foram indispensáveis para a defesa judicial (MENDES, 2014, p. 74-75).

<sup>9</sup> Disponível em [http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S0102-311X2018000700502&lng=pt&tlng=pt](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-311X2018000700502&lng=pt&tlng=pt).

de dados populacionais proporcional ao nível de risco envolvido na solicitação de acesso”. Por meio desse modelo, os dados estariam divididos em diversas categoriais, levando em consideração aspectos como em questão de mérito científico, o tipo de dado e a segurança do ambiente em que estará armazenado.

Assim, aqueles dados categorizados como de “alto risco” teriam maior cuidado, bem como teriam sua solicitação revisada para evitar maiores percalços.

Percebe-se, assim, a tamanha relevância do especial tratamento dos dados sensíveis, incubindo à Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18) resguardar uma seção exclusiva (Capítulo II, Seção II) para tratar sobre as específicas hipóteses de uso e manipulação dessa subespécie.

Vale ressaltar que a referida lei, ainda, a fim de evitar confusões, exclui da categoria de dados pessoais os dados anonimizados (art. 5º, inciso III), bem como aqueles que passam por processo de anonimização (art. 5º, inciso XI), uma vez que não podem eles identificar seus titulares, em que pese possam se referirem à pessoa natural.

O diploma foi cuidadoso ao dispor, em seu art. 12, a exceção de que os dados anonimizados serão considerados pessoais quando o processo utilizado para tal puder ser revertido, tendo em vista que não há como garantir com certeza a completa eliminação de vínculos de identificação dos dados.

Tanto isso é verdade que os pesquisadores Arvind Narayanan e Vitaly Shmatikov, para comprovar a falha na retirada de identificadores de dados, conseguiram identificar os titulares dos dados (até então ditos como anonimizados) utilizados em uma pesquisa realizada pela empresa Netflix Prize, após redefinir certas bases desses dados (BIONI, 2018, p. 73).

Entende-se, portanto, que, persistindo qualquer possibilidade de reidentificação dos dados até então anonimizados, faz-se necessário a instituição do regime (mais rigoroso) de proteção dos dados pessoais.

Assim, dada a importância dos dados pessoais em meio à sociedade da informação, em especial aos dados sensíveis, a sua proteção é fundamental para resguardar os direitos de seu titular.

Inclusive, na era tecnológica informacional, é comum se deparar com a prática do *profiling*, instituto por meio da qual forma-se um perfil de certo indivíduo com base nos seus dados pessoais e, com o resultado, decisões são tomadas. “Um perfil assim obtido pode se transformar numa verdadeira representação virtual da pessoa, pois

pode ser o seu único aspecto visível a uma série de outros sujeitos” (DONEDA, 2006, p. 174), podendo ocasionar uma confusão com o próprio cidadão.

Conforme bem apontado por Bioni (2018, p. 91), a soma de todas as variáveis colocadas ilustra a união entre a proteção dos dados pessoais e o próprio rumo da vida das pessoas, “perpassando, transversalmente, os seus mais variados contatos sociais”.

Tratando desse cerne, o Ministro Ruy Rosado de Aguiar, citado por Doneda (2011, p. 95), já indicou em decisão acerca da custódia necessária diante de tratamentos dos dados:

A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações, pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica.

Ainda segundo o Ministro, a relevância sobre o assunto recebe ainda maior destaque ao ser deparar com a visão de que há um “número imenso de atos da vida humana praticados através da mídia eletrônica”, sendo tal estatística crescente cada vez mais com o passar do tempo.

## **2.2 A importância da Proteção dos Dados Pessoais na Sociedade da Informação**

Para Bauman (2011, p. 8), crítico da pós modernidade, o mundo líquido moderno que nos faz mudar constantemente permitiu que hoje pudéssemos dispor de algo até então inimaginável: a Internet, a web mundial, “as autoestradas de informação que nos conectam de imediato, em tempo real, a todo e qualquer canto do planeta”, podendo tudo isso ser transportado nos bolsos através dos pequenos *smartphones*.

Desde a rápida evolução da informática, a partir dos anos de 1950, a atenção dos juristas pairou sobre o tema. Nesse âmbito, Lee Loevinger, trazido por Doneda (2006, p. 169-170), denominou a disciplina sobre os métodos informáticos de

*Jurimetrics* (Jurimetria) e termos como *computer law* e *technology law* passaram a ser comuns no meio jurídico.

Mas foi através da criação e difusão da Internet na década de 1970 que ocorreu um *boom* do compartilhamento de informações e uma revolução no modo de se relacionar, tornando-se um “fenômeno mundial de interconexão” voltado tanto para pessoas, quanto para empresas e governos (MARINELI, 2017, p. 1).

Segundo Mendes (2014, p. 20), conseqüentemente a esse aumento das capacidades e oportunidades dos indivíduos, “os meios de comunicação e informação ampliam, na mesma medida, os riscos a que os indivíduos estão submetidos”.

Tal união entre poder de informação e a tecnologia, sendo a base dessa soma a comunicação e a transferência de dados, quando basear em uma má utilização, “pode ser tão nefasto quanto o poder bélico almejado, por séculos, pelas nações como um indicador de poder e de domínio sobre os povos” (FORTES, 2016, p. 40).

Isso porque, dentre demais dilemas, em 1991, surge a expressão em inglês *ubiquitous computing* formulada por Wieser, que previa as transformações da tecnologia no século XXI que processariam os dados de forma onipresente, de modo que “a tecnologia da informação e o processamento de dados perpassam todas as áreas da vida de um indivíduo” (MENDES, 2014, p. 78-79).

Um dos efeitos imediatos, portanto, está no fato de que os indivíduos perdem, devido ao desequilíbrio de poderes que possuem com os organismos processadores de informações, o controle individual sobre o fluxo de seus próprios dados.

Além do mais, foi através da Internet, bem como por meio dos avanços quantitativos e qualitativos nas manipulações das informações utilizadas como fontes de riqueza, que a sociedade pré-informacional se transforma na sociedade informacional. Por meio desta, agora o consumidor deixa de ser apenas o polo passivo no ciclo do consumo, passando a ter uma participação ativa através de seus dados – “tamanho é a valiosidade das informações dos consumidores que o seu controle e organização são termos essenciais do marketing” (BIONI, 2018, p. 15).

Conforme bem destaca Bauman (2007, p. 115), nesse momento o marketing passa a penetrar “as áreas da existência que até recentemente estavam fora do reino das trocas monetárias e que não eram registradas nas estatísticas do PIB”.

Assim, surge a figura da “publicidade direcionada”, desse modo chamada devido à direção certa das ferramentas do marketing ao potencial consumidor,

descoberto este por meio de seus dados que foram obtidos através de instrumentos tecnológicos, como é o caso do rastreamento da navegação do usuário na Internet.

Sobre o assunto, Doneda (2018, p. 19) explica:

Por meio do registro de navegação do usuário, cria-se um rico retrato das suas preferências, personalizando-se o anúncio publicitário. A abordagem publicitária passa a ser atrelada com precisão ao perfil do potencial consumidor. Sabe-se o que ele está lendo, quais os tipos de websites acessados, enfim, tudo aquilo em que a pessoa está efetivamente interessada e, em última análise, o que ela está mais suscetível a consumir com base nesse perfil comportamental.

Desse modo, a indústria publicitária pode direcionar os seus anúncios, criando perfis cada vez mais estritos dos usuários, com base em um monitoramento ininterrupto de seus atos, influenciando, inclusive, nos seus estados emocionais. A economia passa a ser uma economia voltada na vigilância, na observação constante daqueles que a movimentam para captar os seus dados pessoais e tornar a mensagem publicitária mais oportuna (BIONI, 2018, p. 49).

Ao passo que a Internet possui um modelo de negócio em que o acesso é “gratuito”, isto é, no qual não há prestação pecuniária por aqueles que a utilizam, enganam-se aqueles que acreditam que a ferramenta não retira nada de seus usuários.

Como troca de seus bens de consumo fornecidos, a Internet utiliza dos dados pessoais dos seus “consumidores”, em troca da mencionada publicidade direcionada. Desse modo, o consumidor torna-se também uma parte do produto comercializado, tendo em vista que são seus próprios dados que direcionam a economia em questão.

É através dessa perspectiva que as redes sociais lucram em grandes proporções: a venda dos dados dos seus usuários às empresas, públicas ou privadas, para que ocorra o direcionamento dos seus anúncios, é o que movimenta seus caixas. Segundo Marinelli (2017, p. 197):

Ao postar, inocentemente, informações sobre sua rotina e preferências, curtidas e compartilhamentos, o usuário está fornecendo os dados necessários para que a rede social virtual possa direcionar determinada publicidade. Assim, as redes utilizam essas informações para criar grupos de perfis específicos que possam servir às empresas interessadas em fazer chegar os seus produtos e serviços às pessoas potencialmente interessadas.

Para Bioni (2018, p. 25-26), a terminologia *zero-price advertisement business model* resume bem essa dinâmica. Os usuários não pagam uma quantia monetária (*zero-price*) pelo produto ou serviço. A contraprestação deriva do fornecimento de seus dados pessoais, o que possibilita o direcionamento de conteúdo publicitário e

cuja receita pagará, indiretamente, pelo bem de consumo (*advertisement business model*).

Um dos casos que ganhou mais destaque no que diz respeito à publicidade direcionada foi com a rede social *Myspace*, apresentado por Sibila (2016, p. 34-36), ao lançar a ferramenta como uma novidade no mercado. Para tanto, além dos dados pessoais fornecidos pelos usuários, a empresa utilizou também das informações retiradas com as interações feitas na rede, como gostos e hábitos de consumo.

De acordo com a autora, como resultado, em um primeiro momento, o *Myspace* separou os membros da rede em categorias correspondentes aos seus interesses, de modo que cada usuário pudesse receber a publicidade de acordo com tal. Em que pese as diversas críticas recebidas, os idealizadores do projeto não consideravam o ato invasivo, uma vez que cabia a cada usuário a escolha de se associar à determinada empresa de sua preferência para que, apenas após essa opção voluntária, a publicidade seria direcionada.

Graças ao desenvolvimento das comunicações instantâneas e o surgimento das inúmeras redes sociais (grandes fornecedoras de inúmeros dados disponibilizados por seus usuários), o envio da publicidade de acordo com o comportamento de cada um se tornou uma prática imensamente lucrativa e difundida. Por essa razão o *Facebook*, com apenas três anos desde a sua criação, chegou a ser avaliado por quinze bilhões de dólares<sup>10</sup>.

A rede social, logo de início, apresentou um programa que prometia transformar cada usuário em uma ferramenta de marketing direcionada às empresas do *e-commerce*, denominado então como “o Santo Graal da publicidade”. Tal projeto tinha a premissa de monitorar intensivamente as compras e vendas realizadas entre os integrantes da rede, não estando mais restrito àqueles gostos e preferências anteriormente visados – os atos como consumidores de seus usuários tornaram-se o principal destaque<sup>11</sup>.

Ademais, outro caso que ganhou os noticiários, em 2013, foi quando da revelação feita pelo ex-técnico na CIA, Edward Snowden, a respeito de que o governo dos Estados Unidos espionava as populações de diversos países da América

---

<sup>10</sup> Disponível em <https://piaui.folha.uol.com.br/materia/voce-e-o-produto/>.

<sup>11</sup> Disponível em <https://rockcontent.com/blog/historia-do-facebook-ads/>.

(incluindo o Brasil) e da Europa por meio de servidores de empresas privadas, como o *Google* e o *Facebook* (MARINELLI, 2017, p. 159).

Sobre o assunto, Dilma Rousseff, em 2014, chegou a mencionar em seu discurso no evento NETmundial que casos como este de espionagem “atentam contra a própria natureza da Internet, aberta, plural e livre”. Segundo a então presidenta, os direitos que os indivíduos possuem quando não estão conectados deveriam ser os mesmo daqueles que estão *online* (CANCELIER, 2016, p. 79), o que de fato não se via à época.

Atualmente, as informações são trocadas cada vez mais e a todo o momento, e a Internet se tornou parte da vida diária das pessoas, transformando-se, assim, em uma ferramenta onipresente, por meio da qual os anúncios publicitários puderam ser cada vez mais difundidos por menores custos, dado o direcionamento ao potencial consumidor.

Tal realidade pode ser facilmente detectada, como o que ocorre, por exemplo, quando os *smartphones* compartilham as localizações geográficas de seus proprietários e permitem com que as publicidades cheguem de locais mais próximos de onde se encontram os consumidores. “Tanto isso é verdade que a *Google* comprou o aplicativo *Waze* por um total de US\$ 1,3 bilhão, a fim de monitorar os dados da geolocalização dos usuários” (BIONI, 2018, p. 22).

Veja-se, portanto, que, com o desenvolvimento exponencial das tecnologias e dos meios de interações tanto *online* quanto *offline*, surgem novas relações que necessitam a fiel regulação pelo direito, de modo que a indiferença sobre tal realidade se torna impossível (DONEDA, 2006, p. 39).

Nesse sentido, Mendes (2014, p. 33) explana:

Nos mais diversos papéis sociais, como contribuinte, paciente, trabalhador, beneficiário de programas sociais ou como consumidor, o cidadão tem seus dados processados diuturnamente. A vigilância deixa de ser esporádica e passa a ser cotidiana. A utilização massiva de dados pessoais por organismos estatais e privados a partir de avançadas tecnologias da informação apresenta novos desafios ao direito à privacidade. A combinação de diversas técnicas automatizadas permite a obtenção de informações sensíveis sobre os cidadãos e a construção de verdadeiros perfis virtuais, que passam a fundamentar a tomada de decisões econômicas, políticas e sociais.

Assim sendo, destaca-se a geração de “consumidores de vidro”, expressão de Suzane Lace trazida por Bioni (2018, p. 24) que ilustra a realidade na qual todos (monitores de dados) sabem muito sobre os consumidores e podem, inclusive, ver



sobre eles. O dia a dia está por completo datificado, e as vidas são gravadas, monitoradas e analisadas pelas mais diversas formas.

Conforme destaca Marineli (2017, p. 135), tendo em vista essa realidade, torna-se evidente que a produção de dados pessoais cresce diariamente, sendo escancarados, assim, as informações e momentos da privacidade de seus titulares.

Para ilustrar o cenário, segundo pesquisa dos britânicos pertencentes à ONG que analisa o controle dos dados na Internet (*Privacy Internacional*)<sup>12</sup>, recentemente descobriu-se que aplicativos de controle de ciclo menstrual estariam compartilhando dados de sua rede (como dados de saúde e da vida sexual das usuárias, dentre outras informações) para a plataforma do *Facebook*.

Segundo indica Doneda (2006, p. 1), o mal da atualidade que atinge a sociedade está na falta de proteção devida dos dados pessoais, visto que a “exposição indesejada de uma pessoa aos olhos alheios se dá com maior frequência através da divulgação de seus dados pessoais do que pela intrusão em sua habitação”, do que pela violação da sua correspondência ou outros meios até então considerados como “clássicos” de violação da privacidade.

Outro dilema presente reside no fato de que os dados pessoais são importantes, inclusive, para o desenvolvimento econômico e social, podendo ser utilizado em prol da sociedade da informação: o uso dos dados em si não possui malefícios, mas a má utilização dos tratamentos causa inúmeros transtornos.

Assim, os titulares devem estar cientes do uso (fato que dificilmente ocorre hoje), sendo informados ostensivamente e previamente, tendo controle e o livre direito de manifestar o seu consentimento ou não para tal. “Afinal, a guarda dos dados pessoais e do conteúdo das comunicações privadas deve atender à preservação da intimidade, da vida privada, honra e imagem das partes direta ou indiretamente envolvidas [...]” (MARINELI, 2017, p. 199).

Ademais, o mérito da proteção dos dados pessoais pode ser analisado devido ao fato de que, além das informações retiradas de tais, são eles que representam os indivíduos na sociedade da informação, uma vez que é a partir deles que os organismos sociais criam perfis virtuais e, desse modo, tomam decisões que afetam suas vidas e suas personalidades (MENDES, 2014, p. 123-124).

---

<sup>12</sup> Disponível em <https://www.privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data>.

Faz-se necessário, assim, uma tutela central e primordial dos direitos fundamentais relativos à privacidade e à proteção de dados pessoais para proteger “futuro presente” (FORTES, 2016, p. 12), a fim de assistir o titular que se encontra vulnerável – a função da proteção dos dados não é sobre os dados em si, mas sim a de proteger a pessoa que é detentora desses dados (MENDES, 2014, p. 32).

### **2.3 Proteção dos Dados Pessoais e o Direito à Privacidade**

Com a propagação do princípio da dignidade humana pelas constituições em todo o mundo, principalmente com o término da Guerra Mundial de 1939 e com a Declaração Universal de Direitos Humanos do ano de 1948, os interesses essenciais da existência humana passaram a ser prioridade nas discussões dos juristas (GUERRA, 2010, p. 3-4).

A título exemplificativo, a Constituição Federal da República Federativa da Alemanha (Constituição Weimar) incluiu nas suas previsões, atrelada ao princípio da dignidade da pessoa humana, a ressalva de uma necessária proteção ao livre desenvolvimento da personalidade<sup>13</sup>. Ao mesmo tempo, no âmbito nacional, em que pese ainda viger o Código Civil de 1916, doutrinadores já identificavam em seus estudos a indispensável tutela dos direitos à personalidade. Foi apenas com o projeto de Código Civil de Orlando Gomes (Código atual), que previa um capítulo específico sobre a matéria, que tal garantia passou a ser expressamente prevista (BIONI, 2018, p. 55-56).

Segundo o doutrinador Rubens Limongi França (2011, p. 54), o termo personalidade expressa “características ou conjunto de características que distingue uma pessoa da outra”. Nessa analogia semântica, os direitos da personalidade poderiam ser “os caracteres incorpóreos e corpóreos que conformam a projeção da pessoa humana”.

Dentre a gama de direitos resguardados pela personalidade, encontra-se, como destaque para o presente trabalho, o direito à privacidade e as suas nuances, o qual, conforme afirma Mendes (2014, p. 102), “atua a serviço da promoção da dignidade da pessoa humana”.

---

<sup>13</sup> “Artigo 2º. Todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral”. Versão em português disponível em: <https://www.btg-bestellservice.de/pdf/80208000.pdf>.

A sociedade, que sempre foi constituída como um ambiente por meio do qual a comunicação está presente entre seus pontos centrais (seja para fomentar laços afetivos, econômicos ou políticos), que antes era realizada entre indivíduos isolados, passa hoje a ser realizada entre “um grupo de pessoas (a empresa que comunica) e a massa da sociedade” (SOUZA, 2005, p. 243).

Diante da realidade proporcionada pela evolução das ferramentas tecnológicas, a privacidade tornou-se um elo da personalidade perdido e as informações ditas como pessoais passaram a ser transportadas para toda a sociedade. Com a conexão diária e instantânea à Internet, os dados que antes eram particulares e privados de cada indivíduo são transportados para a rede e deixam seus titulares à mercê desse sistema virtual mundial.

Nesse sentido, Marineli (2017, p. 2) destaca que “entre as violações perpetradas por pessoas e redes sociais mal intencionadas, os danos à privacidade ganham destaque e já figuram entre as principais preocupações dos internautas”.

O termo privacidade pode ser entendido tanto como o desempenho da liberdade do indivíduo, quanto como algo que encontra-se interno a este sujeito, de modo que faz parte da sua natureza enquanto ser humano. “Ter privacidade é fundamental ao indivíduo, não apenas em oposição ao público, mas numa relação interna, visto que não será possível a assunção de seus desejos sem a construção de seu espaço íntimo” (CANCELIER, 2016, p. 85).

Apesar de encontrar dificuldade em delimitar um conceito da privacidade, Doneda (2006, p. 107) apresenta a origem da palavra que, em que pese constantemente empregado na língua inglesa, o vocábulo em si possui raiz latina, derivado do verbo *privari*, que possui como adjetivo a forma *privatus*. “De fato, o desenvolvimento do termo *privacy* na língua inglesa não teve paralelo em idiomas latinos, ao menos como um substantivo simples”.

Segundo ele, ainda, a problemática da privacidade “sempre foi diretamente condicionada pelo estado da tecnologia da sua época”, de modo que sua essência pode variar de acordo com os avanços da tecnologia (DONEDA, 2006, p. 60)

Já para Mendes (2014, p. 101), o instituto da privacidade pode ser analisado sob duas óticas. A primeira refere-se ao ângulo do direito constitucional, por meio do qual a privacidade enquadra-se dentro dos direitos fundamentais; enquanto que, sob a égide do direito civil, a personalidade constitui um “atributo da personalidade de cada indivíduo”. Nas palavras do autor:

Como esses ângulos revelam conteúdos semelhantes e convergentes, que se destinam à promoção e tutela da dignidade da pessoa humana, entendemos que, no tocante à natureza jurídica, o direito à privacidade pode ser enquadrado como um direito fundamental da personalidade humana.

Os debates doutrinários acerca da proteção à privacidade tiveram seu início com o artigo “*The right to privacy*”, de 1890, por meio do qual os autores Warren e Brandeis denunciaram a invasão que diversos aparatos tecnológicos detinham sobre a vida privada dos indivíduos. Com base no artigo, o direito à privacidade estava até então relacionado à uma corrente individualista, categorizada como *the right to be let alone* (MENDES, 2014, p. 27).

Conforme Cancelier (2016, p. 111), reforçando a presença da corrente no texto, percebe-se a partir de sua leitura a projeção de “aspectos individuais do sujeito, sem relacioná-los a qualquer benefício coletivo em sua tutela ou em seu exercício”.

Por meio da visão apresentada pelo trabalho, o direito à privacidade foi tido com um meio autônomo em relação aos demais, sendo diferenciado, portanto, daqueles direitos anteriormente já previstos como a garantia à liberdade e à propriedade.

Nesse sentido, os autores certificam que “o direito à liberdade assegura extensivos privilégios civis, mas não outorga proteção frente à ofensa de sentimentos pela invasão da esfera privada”, enquanto que o direito à propriedade “garante apenas a posse, tangível ou intangível, mas não assegura a tranquilidade de espírito que proporciona impedir a publicação de aspectos reservados da pessoa” (FORTES, 2016, p. 31).

Destaca-se, assim, trecho do artigo (p. 213) apresentado por Marineli (2017, p. 83):

Portanto, devemos concluir que os direitos, assim protegidos, independentemente de sua natureza exata, não são direitos decorrentes de contrato ou de mandados específicos, mas são direitos contra todos; e, como afirmado acima, o princípio que tem sido aplicado para proteger esses direitos não é, na realidade, o princípio da propriedade privada, a menos que seja usado em um sentido mais extenso e incomum. O princípio que protege escritos pessoais e quaisquer outras produções do intelecto ou das emoções é o direito à privacidade, e a lei não tem um outro novo princípio a ser formulado quando confere proteção à imagem, manifestações, atos e relações pessoais, sejam elas doméstica ou não<sup>14</sup>.

---

<sup>14</sup> Tradução livre: “We must therefore conclude that the rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights as against the world; and, as above stated, the principle which has been applied to protect these rights is in reality not the principle of private property, unless that word be used in an extended and unusual sense. The principle which protects personal writing and any other productions of the intellect or of the emotions, is the right to

Pode-se perceber, assim, que Warren e Brandeis tentam ilustrar no relevante artigo a passagem histórica que levou a Common Law a resguardar a proteção do indivíduo nas suas esferas patrimoniais e extrapatrimoniais.

Contudo, com o passar do século XX e o desenvolvimento acelerado da sociedade da informação, o alcance do direito à privacidade foi significativamente ampliado e modificado. Segundo Mendes (2014, p. 29):

De um direito com uma dimensão estritamente negativa e com uma conotação quase egoísta, passou a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático. É nesse sentido que se pode afirmar que o século passado vivenciou um “processo de inexorável reinvenção da privacidade”.

Foi com a década de 1970 e o surgimento de diplomas legais e jurisprudências que trataram sobre o tema que tal transformação tornou-se ainda mais nítida, principalmente pelo fato de que houve a constatação dos dados pessoais como uma projeção da personalidade do indivíduo e, desse modo, são eles merecedores da proteção como direitos fundamentais (MENDES, 2008, p. 29).

Neste cenário, os Estados Unidos editaram a lei denominada de *Fair Credit Reporting Act*, pioneira do país a tratar de armazenamento de dados pessoais que visava regular a privacidade em escritórios de proteção ao crédito e cadastros de consumidores (DONEDA, 2006, p. 141) e, assim, resguardar a privacidade dos titulares daqueles que tinham seus dados coletados e tratados por terceiros.

Contudo, vale ressaltar que o caso mais marcante sobre o tema está na República Federal da Alemanha, ano de 1977, que já possuía uma lei federal para a proteção dos dados pessoais, denominada de *Bundesdatenschutzgesetz*<sup>15</sup>. Neste momento, para a realização de um “censo” nacional, os cidadãos do país foram submetidos a um questionário, que futuramente seria informatizado para o tratamento dos dados coletados, havendo penalidade de multa para aqueles alemães que não o respondessem.

Conforme aponta Doneda (2006, p. 194), “alguns comissários de proteção de dados pessoais e entidades da sociedade civil organizada chamaram a atenção para os problemas que o censo, na forma que foi planejado, poderia acarretar aos cidadãos”, de modo que a Corte Constitucional do país teve que intervir no dilema.

---

privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise”.

<sup>15</sup> Disponível em <https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019>.

Segundo decisão dos juristas, o censo foi considerado inconstitucional por violar expressas previsões que garantiam o direito geral da personalidade, utilizando na sentença termos como “autodeterminação informativa” para indicar que, por se tratar de direito fundamental, apenas os titulares são capazes de decidir a respeito da disposição de seus dados, principalmente quanto aos limites e prazos de utilização.

Nesse sentido, Mendes (2014, p. 31) destaca que tal sentença fez surgir um “marco para a teoria da proteção de dados pessoais”, inspirando legislações nacionais e internacionais a seguirem o seu modelo e reconhecerem tal direito subjetivo como fundamental e proteger os titulares da prática de tratamento sobre seus dados.

Já no âmbito nacional, para o legislador brasileiro, na Constituição Federal de 1988, o direito à privacidade encontra-se inserido dentro do rol de direitos fundamentais, com a expressa previsão de resguarda ao direito à vida privada e à intimidade. “Além disso, manteve a inviolabilidade da moradia e do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (incisos XI e XII)” (MARINELI, 2017, p. 93-94).

Assim, para Doneda (2006, p. 142), a privacidade se torna o cerne em meio às proteções da pessoa humana, não sendo vista apenas como “escudo contra o exterior”, mas também como um elemento indutor da cidadania, “da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral”.

Nesse momento, cabe destacar a interpretação de Ferrajoli (2011), apresentada por Fortes (2016, p. 112-113), de que dentro dos direitos fundamentais encontram-se os bens fundamentais, os quais possuem uma subcategoria denominada de bens personalíssimos, capazes de proteger direitos que não se enquadram dentro os patrimoniais, em que pese se referirem ao próprio indivíduo. Desse modo, “a privacidade e a consequente proteção dos dados pessoais, por serem personalíssimos e não admitirem alienação, merecem a proteção sob a receptividade conceitual dos direitos fundamentais, de modo indubitável”.

Segundo Mendes (2014, p. 175), o bem jurídico tutelado por este direito é duplo: protege a integridade moral das pessoas, tendo em vista seu componente como dignidade da pessoa humana, bem como as liberdades em amplo sentido.

Sobre o assunto, Doneda (2006, p. 26-27) afirma:

É justamente neste desenvolvimento como um direito fundamental que percebemos que a necessidade de funcionalização levou ao seu desdobramento - em consonância com boa parte da experiência doutrinária, legislativa e jurisprudencial. Este desdobramento verifica-se, por exemplo, pela forma com que o tema foi tratado na elaboração da recente Carta dos

Direitos Fundamentais da União Européia (hoje também integrante do projeto de Tratado Constitucional da União Europeia), cujo art. 7º trata do já tradicional direito ao “respeito pela vida familiar e privada”; ao passo que seu art. 8º é dedicado especificamente à “proteção dos dados pessoais”. A Carta, desta forma, reconhece a complexidade dos interesses ligados à privacidade e a disciplina em dois momentos (e artigos) distintos, o primeiro destinado a tutelar o momento individualista de intromissões exteriores; e o segundo para tutela da dinâmica dos dados pessoais em suas várias modalidades - sem que seja fragmentada a sua fundamentação, que é a dignidade do ser humano, matéria do capítulo I da carta que contém os dispositivos mencionados.

Desse modo, observa-se que a previsão do constituinte brasileiro quanto à privacidade, embora trate de importantes defensores da proteção individual, mostra-se insuficiente para a tutela do tema específico dos dados pessoais, uma vez que “essas garantias visam à proteção específica em face de riscos determinados (divulgação de informações íntimas ou interceptação da comunicação, por exemplo), e não abarcam a totalidade dos riscos aos quais o indivíduo está submetido na sociedade da informação” (MENDES, 2014, p. 165).

Segundo entendimento de Rodotà (2008, p. 17), apresentado por Fortes (2016, p. 37), tamanha é importância da proteção de dados pessoais que é possível classificá-la como “a soma de um conjunto de direitos que configuram a cidadania do novo milênio”.

Assim, cabe uma interpretação extensiva e sistemática da Carta Magna brasileira para enquadrar os dados pessoais dentro da garantia da inviolabilidade da intimidade e da vida privada previstas no inciso X do art. 5º do diploma, de modo a manter a atualidade da proteção do titular em face das adversidades da sociedade da informação.

Pode-se perceber que os dados pessoais podem ser categorizados como instrumento que permite com que seu titular desenvolva a sua personalidade de forma livre, representando, assim, um prolongamento do próprio indivíduo e uma perspectiva de suas relações (BIONI, 2018, p. 84).

Para sua proteção como tal, devem estar assegurados como um direito subjetivo do indivíduo, de modo a resguardar sua defesa e limita a atuação do poder estatal ou privado diante de tal. Ademais, deve também possuir uma visão como um dever estatal de proteção, numa visão objetiva, por meio da qual “representa a necessidade de concretização e delimitação desse direito por meio da ação estatal, a partir do qual surgem deveres de proteção do Estado para garantia desse direito nas relações privadas” (MENDES, 2014, p. 176).

Nesse sentido, para Lei Geral de Proteção de Dados Pessoais, segundo Bioni (2018, p. 109), “a disciplina da proteção dos dados pessoais tem como objetivo proteger os direitos fundamentais e o livre desenvolvimento da personalidade (art. 1º), repetindo-os como um dos seus fundamentos ao lado do desenvolvimento econômico-tecnológico da inovação (art. 2º)”.



### 3. O INSTITUTO DO CONSENTIMENTO FRENTE À PROTEÇÃO DOS DADOS PESSOAIS

Apesar de servir como um alerta, a “teletela orwelliana”<sup>16</sup> está aquém da realidade. Isso porque, diferente da concreta figura do Grande Irmão, a vigilância atual encontra-se diluída e dispersada, diferenciando-se da ideia de dois atores definidos na relação (observador e observado) para se enquadrar em um modelo de negócio pautado na vigília dos consumidores potenciais entre os todos os cidadãos.

Conforme ilustra Bauman (2001, p. 25), esta “modernidade líquida” da atualidade faz com que as relações se tornem mais voláteis, caracterizadas por intensas incostâncias e incertezas consequentes das perdas de pontos de referências dos indivíduos socialmente estabelecidos.

Em verdade, como ressalta Bioni (2018, p. 141-143), a atual “multifacetação é resultado desse complexo ambiente de economia dos dados pessoais”. Desse modo, o que antes era visto como uma grande tela por George Orwell, agora se transformou em uma rede de vigilância - com características fluidas de dispersão dos dados captados por inúmeros atores que os utilizam economicamente, por meio da qual os cidadãos são analisados e segmentados por seus hábitos e gostos.

Por essa característica de fluidez, o controle dos dados se torna um ato de difícil operação, ficando a mercê desse sistema. Conforme o autor supramencionado (2018, p. 145), “a realidade esconde um quadro mais problemático que a ficção”. Nesse cenário, o complexo informacional resultante desse fluxo contínuo e opaco dos dados pessoais importa em regulamentos imprescindíveis que capacitem os cidadãos a controlar suas informações.

Atrelando as diretrizes protetoras do direito da privacidade à proteção de dados pessoais, os sistemas jurídicos (ainda que com vertentes diversas) concordaram a respeito dos princípios básicos a fim de permitir a instituição do consentimento como uma defesa ao titular. Tanto isso é verdade que Mendes (2014, p. 68) destaca:

A convergência internacional estabelecida acerca dos princípios é marcante: mesmo os ordenamentos jurídicos mais diversos preveem praticamente os mesmos princípios de proteção de dados, com mínimas diferenças. Esse quadro comum de princípios é conhecido por “Fair Information Principles” e

---

<sup>16</sup> Como ponto de partida, o romance já demonstra as entraves de uma vigilância ostensiva, na figura do Grande Irmão - figura estatal que estava sob o controle de todos os fatos e cidadãos por meio de câmeras instaladas nas residências. Contudo, na narração de George Orwell (pseudônimo de Erick Arthur Blair), havia uma falha na vigília: além de que apenas os sons acima de sussurros poderiam ser captados, a instalação das câmeras era mau calculada, havendo espaços internos fora de sua visão (BIONI, 2018, p. 139).

teve a sua origem na década de 70 de forma quase simultânea nos EUA, Inglaterra e Alemanha.

No solo americano, foi no ano de 1972 que o Poder Executivo realizou sua primeira ação, no âmbito do Departamento de Saúde, Educação e Bem-Estar: a designação de um comitê consultivo acerca dos sistemas automatizados de dados pessoais. Um ano depois, os estudos divulgaram um relatório que, além de propor redefinição do conceito de privacidade, apresentou um rol princípios tidos como fundamentais acerca do tratamento de dados dos cidadãos<sup>17</sup>.

Na mesma época, na Inglaterra, conforme aponta Mendes (2014, p. 69), foram estabelecidos princípios básicos de proteção após um estudo sobre os riscos advindos com os processamentos automatizados realizados por organizações privadas. Já na Alemanha, em 1970, tem-se a primeira lei que trata da matéria (Lei do Estado de Hesse), a qual englobou as diretrizes de ambos os países e serviu de exemplos para os futuros regulamentos acerca da proteção de dados pessoais (REINALDO FILHO, 2018)<sup>18</sup>.

Nesse sentido, observa-se o princípio da finalidade. Por meio dele, exigiu-se o estabelecimento de uma conexão entre o tratamento dos dados e a finalidade daqueles que o coletam, sendo, ao mesmo tempo, um meio de restrição ao compartilhamento com terceiros e medida verificadora da adequação e razoabilidade do uso dos dados pessoais (MALHEIRO, 2017, p. 34).

Ressalta-se também o princípio da publicidade ou, comumente conhecido, da transparência, segundo o qual ocorre a vedação da manutenção de bancos de dados sigilosos e os repassa para conhecimento (DONEDA, 2006, p. 216). Para Mendes (2014, p. 70), tal princípio “reafirma o preceito democrático”, uma vez que sua base está pautada em um instrumento (transparência) que visa combater abusos.

Veja-se ainda o o princípio da responsabilidade, o qual, conforme indica Malheiro (2017, p. 34), busca garantir a reparação do indivíduo quando da ocorrência de danos materiais e/ou morais em virtude de atentados à sua privacidade, bem como o princípio da segurança física e lógica, que determina que os bancos de dados devam ser assegurados por mecanismos que protejam seus dados contra extravios e desvios que não tenham sido assegurados pelos seus titulares (DONEDA, 2006, p. 217).

---

<sup>17</sup> Disponível em: <https://aspe.hhs.gov/report/records-computers-and-rights-citizens>.

<sup>18</sup> Disponível em: <https://jus.com.br/artigos/67668/lei-de-protacao-de-dados-pessoais-aproxima-o-brasil-dos-paises-civilizados>.

Por fim, surge com destaque o princípio do consentimento, instrumento por meio do qual o controle sobre os dados pessoais passa a ser do próprio titular, cabendo a ele “determinar um maior nível de proteção ou maior fluxo de seus dados, expressando - em tese - sua permissão, sua anuência, sua aprovação para certa forma de tratamento de dados pessoais” (MALHEIRO, 2017, p. 34).

Para tanto, conforme preceitua o princípio, o consentimento exige uma manifestação do indivíduo livre, específica e informada, resguardando situações mínimas para o tratamento de dados sem o consentimento (MENDES, 2014, p. 70).

Nesse sentido, Doneda (2006, p. 371):

O consentimento do interessado para o tratamento de seus dados é um dos pontos mais sensíveis de toda a disciplina de proteção de dados pessoais; através do consentimento, o direito civil tem a oportunidade de estruturar, a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos deste consentimento à natureza dos interesses em questão.

Assim, o consentimento se apresenta como uma medida regulatória capaz de autorizar e proibir, ao mesmo tempo, atividades acerca do tratamento de dados, cabendo aos indivíduos escolherem consciente e racionalmente sobre o que lhes diz respeito.

Unindo-se aos demais princípios protetores, o consentimento exige que haja prévia comunicação, clara e transparente, acerca da finalidade do futuro tratamento dos dados. Nesse sentido, para o tratamento dos dados, como no caso do *data mining*, mecanismo de potencial teor discriminatório, o instrumento do consentimento exige o fornecimento de informações, pautadas no princípio da transparência, sobre os processamentos (MALHEIRO, 2017, p. 36).

### **3.1 Dualidade do consentimento: autodeterminação informativa e meio de legitimação para o tratamento de dados pessoais**

Já utilizado nos meios contratuais, o instituto do consentimento, que até então expressava uma declaração de vontade de negociar partindo de um indivíduo a terceiro, ao ser aplicado para o ambiente da proteção de dados pessoais, passa a designar a liberdade e autonomia dos usuários acerca da ciência sobre o procedimentos que serão realizados com seus dados, concordando com tais ações (CORRÊA, 2019, p. 29).

Assim, nos normativos que tratam sobre a matéria (conforme se verificará no próximo capítulo), o consentimento encontra-se no cerne, com o objetivo de colocar o titular no centro do controle sobre a coleta e o tratamento de suas informações, “preservando, assim, a sua capacidade de livre desenvolvimento da personalidade” (MENDES, 2014, p. 60).

Seria dever do Estado, neste cenário, legislar sobre os meios e formas pelos quais o indivíduo terá a sua disposição no momento do ato de controle. Ainda conforme a autora:

Por se constituir um direito sobre as informações pessoais, a proteção de dados pessoais tem um forte componente de autoconformação, tendo em vista que somente o indivíduo pode determinar o âmbito da própria privacidade, isto é, em que medida as suas informações pessoais podem ou não ser coletadas, processadas e transferidas. Nesse aspecto, nota-se que a proteção de dados pessoais é marcada por esse acentuado viés de autocontrole e de liberdade pelo titular.

O consentimento surge, portanto, como um instrumento do indivíduo que possibilita o exercício da sua autodeterminação informativa, cabendo a ele anuir (ou não) com a coleta e tratamento de suas informações.

Em relação ao instituto, Bioni (2015, p. 43) ainda ressalta a ideia trazida por Tene e Polonetsky de que o consentimento aparece como uma “carta coringa regulatória”, com o objetivo de representar as autorizações e proibições do titular em meio a um complexo sistema de coletas e tratamentos de dados pessoais.

Desse modo, percebe-se que, a fim de deixar de ser enquadrado como um simples meio de fornecimento de dados, o indivíduo passa a figurar como um elemento central ao longo da evolução da proteção dos dados pessoais, a ponto desta proteção ser equiparada “ao direito do cidadão autogerenciar as suas informações pessoais” (MALHEIRO, 2017, p. 35).

Relembrando os ensinamentos de Mendes, Cancelier (2016, p. 128-129) ressalta a ideia de que o consentimento, assim, apresenta-se como “uma das formas de exercício da autodeterminação informativa”, tendo em vista a liberdade dada ao indivíduo em relação ao desenvolvimento de sua personalidade.

Nesse sentido, Malheiro (2017, p. 34):

O consentimento é uma forma de implementar o direito à autodeterminação informativa, visto que envolve a própria participação do indivíduo, que funciona como mola propulsora da estrutura da proteção de dados, permeando todo o processo de tratamento de dados.

Tamanha é a particularidade do consentimento no cenário de proteção dos dados que, quanto a sua natureza jurídica, cabe categorizá-lo de acordo com os efeitos e consequências que surgem de tal.

Observa-se que Mendes (2014, p. 62-63), ao analisar as correntes acerca do tratamento de dados pessoais, constata a polêmica em torno do assunto. Tanto isso é verdade que, conforme identifica a autora, na Alemanha (país pioneiro na regulamentação sobre o tema) havia três correntes diversas: a primeira, relacionada à natureza de uma “declaração de vontade negocial” (*rechtsgeschäftliche Erklärung*); a segunda, voltada ao entendimento do consentimento como um ato jurídico unilateral, afastado de uma natureza negocial (*Realhandlung*); e, por fim, a terceira, no sentido de que seria uma similitude de um negócio jurídico, sem realmente o ser (*geschäftsähnliche Handlung*).

A terceira e última vertente é a que tem sido predominante nos regulamentos e, segundo o entendimento de Mendes (2014, p. 63), parece ser a mais adequada: encontra-se clara e nítida “a natureza atípica do consentimento para o processamento de dados, que tem características negociais, ao mesmo tempo em que possui também um caráter personalíssimo”.

Desse modo, enquanto, por um lado, a sua função como protetor dos dados pessoais estaria voltada àquela dos negócios jurídicos, tendo em vista ser um instrumento de autodeterminação do indivíduo, um exemplo acerca da sua capacidade civil retira a aplicação da norma: estando o caráter personalíssimo do consentimento relacionado ao processamento de dados, o principal objetivo passa a ser a identificação daquele que detém a capacidade de discernimento para autorizar determinado tipo de coleta ou tratamento de dados, não sendo necessária a capacidade civil para tanto (MALHEIRO, 2017, p. 39).

Percebe-se, assim, a dicotomia existente que impede enquadrar o consentimento como uma natureza única, uma vez que, ao mesmo tempo, está relacionado a um direito personalíssimo e à utilidade dos dados pessoais.

Observa-se que o Regulamento Geral de Proteção de Dados, em seu art. 4º item 11<sup>19</sup>, prevê o instituto do consentimento como sendo uma declaração de vontade

---

<sup>19</sup> «Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que

inequívoca do indivíduo “livre, específica, informada e explícita”, por meio da qual retira-se a sua aceitação acerca do tratamento de seus dados. Nesse sentido, pode ser admitido como um instrumento da autonomia privada do cidadão (MALHEIRO, 2017, p. 37).

Analisando em um ambiente mais amplo, que vai além da proteção dos dados pessoais, Orlando Gomes (2008, p. 55) entende que o instrumento do consentimento está relacionado ao direito contratual, no qual “os indivíduos exprimem a sua vontade de contratar, dando ciência uma a outra da sua intenção negocial para que seja selado um compromisso entre elas”.

Já para Doneda (2006, p. 377-378), contudo, relacionado a um ato unilateral vinculado a uma autorização (tratamento dos dados pessoais), tendo sua orientação voltada ao poder de autodeterminação informativa do indivíduo, sem, contudo, relacionar-se com uma estrutura contratual.

Desse modo, seria inapropriado considerar o consentimento em natureza negocial, uma vez que, caso assim fosse, seria permitida a inclusão desse instituto nas estruturas contratuais, além de dificultar o exercício das prerrogativas da personalidade que deveriam ser analisados e respeitados.

Desse modo, desataca o autor (2006, p. 378):

Verifica-se, portanto, que a fundamentação deste consentimento reside na possibilidade de autodeterminação em relação aos dados pessoais, e que esta autodeterminação deve o elemento principal a ser levado em conta para caracterizarmos tanto a natureza jurídica bem como os efeitos deste consentimento.

Conforme o entendimento de Ruaro, Rodrigues e Finger (2011, p. 61), o consentimento passa a ser identificado como um mecanismo que expressa a escolha do indivíduo e, ato contínuo, refere-se aos valores fundamentais relacionados. Assim sendo, ao mesmo tempo em que identifica a autodeterminação informacional do usuário (como condição de acesso à sua esfera privada), ele se mostra um importante instrumento de legitimação.

Outra circunstância acerca do consentimento que merece relevância, está relacionada às possibilidades de revogação do consentimento declarado pelo

---

os dados pessoais que lhe dizem respeito sejam objeto de tratamento”. Versão em português disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=DA>.

indivíduo, visto ser uma das prerrogativas essenciais da autodeterminação do cidadão titular dos dados pessoais.

Inerente à ideia de proteção da personalidade do seu titular, a possibilidade de sua revogação encontra-se tácita. Segundo Doneda (2006, p. 380), tal ato seria, inclusive, uma atribuição da própria natureza jurídica do consentimento, uma vez que, decorrente da autodeterminação, o indivíduo não está submetido a efeitos vinculantes da sua escolha. Já quanto àquele que recebeu a autorização para o uso dos dados e depois a vê revogada, nada se poder fazer, uma vez que está inerente à natureza da atividade.

Para Mendes (2014, p. 61-64), no mesmo sentido, a revogação do consentimento sem qualquer justificativa é a vertente que mais condiz com a realidade, uma vez que está intrínseco à proteção dos dados pessoais (como direito à personalidade). Isso se vê, inclusive, em virtude de o indivíduo detentor dos dados pessoais enfrentar uma série de dificuldades para que possa mensurar os riscos e consequências do seu consentimento.

Ademais, veja-se que a ideia de revogação está atrelada, ainda, ao direito de mudar de ideia do cidadão. A contrario sensu, a título exemplificativo do que ocorre com a realidade, diversos websites enviam notificações aos usuários quando das mudanças e atualizações das suas políticas de privacidade aos seus usuários, sem, contudo, abrir possibilidade para que estes possam revogar (ou renovar) seus consentimentos anteriormente expressos.

Sobre o assunto, o artigo *Click here to consent forever* de Clusters<sup>20</sup> ressalta:

[...] o consentimento é geralmente solicitado no momento do registro, mas raramente é renovado. Como resultado, consentir uma vez implica em consentir para sempre. Ao mesmo tempo, dadas às rápidas transformações no Big Data e análise de dados, o consentimento pode facilmente tornar-se desatualizado (quando o consentimento anterior não mais reflete as preferências dos usuários)<sup>21</sup>.

Para o autor, portanto, conforme apresenta Malheiro (2017 p. 51), deveriam ser postas datas limites de validade dos consentimento, a ponto e que ele “expiraria” findo

---

<sup>20</sup> Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3047128](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047128).

<sup>21</sup> Tradução livre do trecho: “(...) consent is usually asked for when registering, but rarely is consent renewed. As a result, consenting once often implies consent forever. At the same time, given the rapid changes in Big Data and data analysis, consent may easily get outdated (when earlier consent no longer reflects a user’s preferences)”.

o prazo e, assim, o consentimento manteria sua prerrogativa de manter-se sempre atualizado.

Conforme traz a Escola Nacional de Defesa do Consumidor (2010, p. 70-71), a ideia da revogação, ainda, deve ser entregue aos usuários através de mecanismos ostensivos e facilitados aos usuários, tendo em vista serem eles o elo fraco da relação.

Observa-se, assim, que, ao utilizar da sua autodeterminação, não encontra-se o indivíduo restrito a consequências de natureza obrigacional, que o vinculariam ao seu consentimento anteriormente entregue (DONEDA, 2006, p. 381).

O que irá agregar maior ou menor valor ao instituto, conforme se verá a seguir, será a sua adjetivação no decorrer dos regulamentos, como é o caso de ele vir acompanhado de “informado”, “livre” e “expresso” (MENDES, 2014, p. 46).

### **3.2 Pressupostos de validade: a “adjetivação” do consentimento**

A validade do consentimento em si, para Mendes (2014, p. 65), dá-se a partir de determinados pressupostos que merecem ser observados, sendo eles: “i) o titular deve emitir consentimento por sua livre e espontânea vontade; ii) o consentimento deve ser voltado a uma finalidade específica; iii) deve haver informação ao usuário sobre os objetivos da coleta, processamento e uso de dados e consequências sobre não consentir com o tratamento”.

Ademais, trazendo, de início, validade ao consentimento, a declaração do indivíduo deve preceder a coleta de seus dados, isto é, ser obtida antes da interferência de terceiros, a fim de servir como um instrumento de informação acerca do que será consentindo, inclusive dos riscos e consequências de sua decisão. Além disso, a possibilidade de revogação do consentimento deve estar sempre presente, “tanto com relação à autorização para o tratamento, quanto para a própria circulação dos dados colhidos” (SOUZA, 2018, p. 30).

Segundo artigo publicado pela Universidade de Leiden<sup>22</sup>, os autores Schermer, Clusters e van der Hof entendem que a validade do consentimento se dá quando seja ele fornecido por um indivíduo que tenha ciência dos riscos e consequências que acompanham a sua declaração de vontade, além de que seja ele assegurado de coerção, autorizando determinado tratamento de dados específicos.

---

<sup>22</sup> Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2412418](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418).



Veja-se, assim, que a validação do consentimento está relacionada a presença de adjetivos, sendo denominada, portanto, de “adjetivação do consentimento”.

Desse modo, para que o consentimento seja tido como válido, diversas regulamentações pressupõem determinados pressupostos (adjetivos), podendo-se depreender um quadro comum entre as normas com relação aos adjetivos atrelados ao consentimento de “informado”, “livre”, “inequívoco” e com “finalidades determinadas”.

### **3.2.1 Consentimento informado**

Agregado à boa-fé negocial, o adjetivo *informado* surge como um direito ao usuário e um dever aos responsáveis pelo tratamento dos dados pessoais: direito-dever de informação. Para tornar o consentimento válido, antes de mais nada, faz-se necessário que o titular detenha informações suficientes para se capacitar e decidir.

Analisando o significado do próprio termo informação, Bioni (2018, p. 191) traz as afirmações de Cláudia Lima Marques de que “é ‘dar’ forma, é colocar (in) em uma ‘forma’, aquilo que um sabe ou deveria saber (o expert) e que outro (leigo) ainda não sabe”.

Tamanha é sua importância no ambiente da proteção de dados pessoais que, na maior parte da doutrina, a expressão “consentimento informado” é substituída pelo simples termo “consentimento”, estando inerentes, portanto, as informações elementares disponíveis ao indivíduo.

Sobre o adjetivo em questão, Malheiro (2017, p. 44) destaca a sobrecarga da autodeterminação informativa que ele guarda, estando os indivíduos no controle total de suas informações e suas vidas, bem como apresenta o dever de aquele que indicará sua vontade seja completamente informado do que está consentindo, “de forma que esteja ciente das consequências e riscos daquela decisão”.

Dessarte, o consentimento informado é colocado como um mecanismo de garantia de que as decisões tomadas pelo indivíduo serão racionais e ponderadas e, conseqüentemente, caso não houvesse o dito consentimento, haveria a constatação de uma quebra do princípio da autonomia.

Sob esta análise, constata-se duas relevantes informações: i) considerando o elemento formal (“dar forma”), retira-se que a maneira pela qual a declaração de vontade do titular será externalizada é de suma importância; ii) acerca da utilidade da

informação a ser passada, entende-se que deve haver acréscimo de conhecimento ao usuário, trazendo proteção àquele que a recebe, sendo ela, portanto, “imprevisível e original” (BIONI, 2018, p. 192).

Para tanto, o modelo básico do consentimento (consentimento informado) parte por duas etapas, para o referido autor, sendo elas: o pedido pelo controlador e a declaração de vontade (ou não) pelo indivíduo. Neste cerne, percebe-se que é necessário, antes de tudo, ações por parte dos interessados nos dados, como o fornecimento de informações sobre o conteúdo e processo acerca do consentimento, para que o seu titular tome a decisão.

Acerca do tema, indica Lisboa (2012, p. 28):

O emitente deve buscar o equilíbrio ideal entre os elementos da mensagem, transmitindo a informação em um grau de originalidade e imprevisibilidade que, ao mesmo tempo, desperte a atenção do receptor e possibilite a sua compreensão. Agindo desta maneira, o emitente da informação terá maior êxito no processo comunicativo, podendo inclusive exercer legitimamente o convencimento necessário para que o destinatário adote a conduta dele esperada. A comunicação adequada e eficiente provoca a reação no destinatário da mensagem.

Contudo, necessário destacar que as informações disponibilizadas não são todas aquelas que detém o seu transmissor, até porque, além de difícil concretização, é prescindível transpassar todo o “patamar informativo” ao receptor leigo no assunto (BIONI, 2018, p. 192).

Dentre as que deverão ser repassadas, é importante que o titular tenha a ciência sobre quais dados seus serão coletados e utilizados, bem como as suas finalidades e os procedimentos utilizados. Ademais, segundo Malheiro (2017, p. 45), o indivíduo deverá ter a ciência tanto a respeito de que modo poderá consentir (como ao clicar em uma caixa ou preencher um formulário) como quanto à possibilidade dos meios pelos quais poderá revogar o seu consentimento.

Nesse sentido, Corrêa (2019, p. 31-32) ressalta:

Além disso, o consentimento deve ser, também, informado. Isto porque, o titular só poderá controlar seus dados e decidir sobre sua utilização se for informado adequadamente, possuindo à sua disposição, as informações necessárias para tal decisão. Apesar de o cidadão dificilmente alcançar o mesmo nível informativo do fornecedor, a informação permite a autoproteção, cabendo ao titular compreender os riscos e possíveis implicações que a utilização de seus dados pode causar.

A fim de ilustrar os principais requisitos que transformam o puro consentimento em um consentimento informado, o artigo publicado pela Universidade de Leiden, apresenta uma tabela ilustrativa<sup>23</sup> que comparou determinadas redes sociais que diziam utilizar de consentimentos informados e quais eram os anseios dos usuários acerca, tendo por base os regulamentos sobre proteção de dados da União Europeia.

Da apresentação, observa-se que, em meio às informações necessárias aos usuários, destaca-se a clareza do modo pelo qual os dados serão tratados, além da identificação do sujeito responsável por tal atividade e suas medidas protetivas.

Assim, não se trata de apenas informar. As informações entregues aos usuários deverão ser específicas, completas, detalhadas, confiáveis, acessíveis e de fácil compreensão. “Somente dessa forma é possível imaginar que o cidadão tenha instrumentos suficientes para tomar uma decisão informada e consciente” (MALHEIRO, 2017, p. 46).

O que se vê, em verdade, é a necessidade de informar o usuário a respeito dos prejuízos que poderá sofrer com o compartilhamento de seus dados, das invasões e suas consequências à sua privacidade, para que ele, detentor e titular de suas informações, possa iniciar o procedimento da tomada de decisão de maneira racional. Portanto, percebe-se a fundamental ponderação entre aqui que será transmitido, para que seja informado o suficiente sem que isso prejudique a qualidade da informação.

Como lembra Bioni (2018, p. 194-195), exemplificando a teoria, tem-se as chamadas “tabelas nutricionais” de privacidade, por meio das quais símbolos e ilustrações são utilizados para indicar os procedimentos de coleta e tratamento, apresentando-se, assim, como ótimo meio informacional que facilita o entendimento do usuário sobre temas relevantes.

Acerca do princípio da informação, Doneda (2006, p. 383):

A informação, neste caso, refere-se a uma completa consciência do interessado sobre o destino de seus dados pessoais caso este forneça o consentimento para o tratamento. Esta informação inclui: a quem o dado se destina, para qual finalidade será utilizado, por quanto tempo, quem terá acesso a seus dados, se estes dados poderão ser transmitidos a terceiros, e mais tantos outros detalhes quanto sejam necessários em uma determinada situação para que o interessado possa formar sua convicção, livre e consciente, para realizar o ato de autodeterminação.

---

<sup>23</sup> Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3047134](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047134).

Destaca-se, portanto, que o consentimento informado implica em um conhecimento prévio de elementos necessários para que o titular dos dados pessoais possa iniciar a racionalização de suas decisões. “Se, ao final, o titular for empoderado com o controle de seus dados pessoais, ter-se-á, então, o seu adimplemento perfeito” (BIONI, 2018, p. 196).

### 3.2.2 Consentimento livre

Com base no histórico normativo, inclusive do brasileiro em relação ao direito privado, verificou-se que o instituto do consentimento esteve muitas vezes atrelado aos “defeitos do negócio jurídico”<sup>24</sup>: para que a relação comercial seja válida, é preciso que o consentimento da parte seja “livre e consciente” (BIONI, 2018, p. 190).

Agora, nesta perspectiva, a declaração de vontade deverá advir sem qualquer coação (física ou moral), partindo de uma escolha livre e espontânea vontade do indivíduo (MALHEIRO, 2017, p. 46).

Observa-se que, no entendimento de Souza (2018, p. 30), o instituto do consentimento estaria categorizado como um ato unilateral, devendo-se separá-lo em duas etapas: quando da declaração de vontade que concede o processamento dos dados (ingresso no ambiente privado do titular) e quando da autorização acerca do compartilhamento dos dados.

Desse modo, para que o processamento dos dados seja lícito, o consentimento do titular deverá indicar a concordância desse indivíduo na sessão de seus dados que, para ser considerada válida, deverá ter sido entregue de forma livre e específica, “numa real demonstração de vontade do mesmo”, independente do ambiente em que os dados foram coletados (SOUZA, 2018, p. 30).

Nesse momento, como bem destaca Bioni (2018, p. 197-198) a análise deve estar sobre o grau de assimetria existente para, daí, entender quais eram as possibilidades de escolha do usuário - “o ‘cardápio de opções’ à disposição do cidadão calibrará o quão livre é o seu consentimento”. Nas palavras do autor:

A questão central é sempre checar a existência de algum tipo de subordinação - assimetria de poder - que possa minar a voluntariedade do consentimento, devendo haver uma análise casuística para se concluir se o consentimento pode ser adjetivado ou não como livre.

---

<sup>24</sup> Conforme previsão do Código Civil: erro (arts. 138-144), dolo (arts. 145-150), coação (arts. 151-155), estado de perigo (art. 156), lesão (art. 157) e fraude contra credores (arts. 158-165).

Assim, ao se referir em ausência do controle de terceiros, o consentimento livre indica que o usuário praticou o ato a partir de uma escolha “ –se recusar o consentimento não é uma escolha viável, ou por ser impossível, ou por trazer um impacto muito negativo ao titular dos dados, então não há uma escolha real e, portanto, não há consentimento” (MALHEIRO, 2017, p. 47). Neste sentido, quando a declaração de vontade advém sem este adjetivo, o consentimento encontra-se viciado.

Conclui-se, portanto, que a partir de um consentimento dito como livre e informado, sabe-se que, fora a ciência sobre os meios de monitoramento (coleta e tratamento), é necessário que os indivíduos tenham concordado com tais medidas.

A respeito do assunto, a Escola Nacional de Defesa do Consumidor (2010, p. 66):

Como condições para o consentimento livre e informado, é necessário que o monitoramento se processe de forma clara e transparente e que sejam fornecidas aos usuários informações sobre quais dados serão colhidos, a forma como eles serão utilizados e por quem serão utilizados, entre outras informações essenciais. Além disso, é fundamental que o usuário tenha condições de desistir a qualquer momento de ser objeto deste monitoramento.

Desse modo, entende-se que, para que os usuários tenham o julgamento sobre a conveniência, riscos e consequências da coleta e tratamento de seus dados, devem ter recebido, previamente, informações necessárias que lhes permitiram optar (ou não) livremente pela cessão de seus dados – a decisão de entrega dos seus dados deverá ser dada em meio a tantas outras que poderiam ter sido feitas (CORRÊA, 2019, p. 31).

### **3.2.3 Consentimento inequívoco e com finalidades determinadas**

Inicialmente tem-se que o tratamento dos dados passa a ser uma atividade exercida com um fim “específico e explícito”, ao passo que, ao relacionar com o instituto do consentimento, atrela-se ele à imprescindibilidade de direção, servindo, inclusive, como um caminho a ser perseguido (posteriormente) para a verificação da informações passadas ao usuário que deu origem à declaração de vontade livre (BIONI, 2018, p. 199).

Partindo para uma carga participativa intermediária do indivíduo sobre seus dados, tem-se a adjetivação com o termo *inequívoco*, por meio do qual se encontram

tácitas autorizações dentro do contexto do fluxo informacional. Nesse sentido, tem-se situações nas quais o consentimento torna-se prescindível, uma vez que se encontram dentro das “legítimas expectativas” do titular dos dados.

Além do mais, ao atrelar o instituto do consentimento à inequívoca declaração, a declaração de vontade passa a ser um ato de origem do indivíduo que exponha a sua vontade (CORRÊA, 2019, p. 32).

Já quanto à categorização de consentimento com *finalidade determinada*, a carga participativa do titular dos dados passa a ser pré-intermediária, tendo em vista que, por estar vinculado aos princípios de informação e transparência, tal adjetivação recebe uma maior importância (MALHEIRO, 2017, p. 47).

Sob este cerne, o consentimento deve estar voltado a um fim específico, excluindo-se propósitos genéricos que poderiam fazer com que o titular emitisse um “cheque em branco” aos coletores de dados - afasta-se a possibilidade de uma declaração de vontade genérica por parte do titular dos dados e de uma interpretação extensiva além das que estariam previstas (DONEDA, 2006, p. 383).

Assim, como bem conclui Cancelier, Cristo e Mafra (2017, p. 08), vale ressaltar que o instituto do consentimento encontra-se inserido em um contexto específico, único, de modo que a declaração de vontade que autoriza a coleta e o processamento de determinado dado, em determinada situação, não se estende a outros ambientes diferentes daquele.

### **3.3 Dificuldades e desafios do consentimento no contexto do intenso fluxo informacional**

Com o passar dos anos, o papel do consentimento tem sido alterado e no cenário do Big Data, com o contínuo e expoente fluxo informacional, “tem sido crescente o ceticismo acerca da efetividade do consentimento” para a proteção dos dados pessoais (MALHEIRO, 2017, p. 53).

Por meio dessa rede montada, representada pelo compartilhamento das informações (ainda que segmentadas), entre diversos atores “cooperativos”, que buscam obter perfis específicos dos potenciais consumidores, “esse fluxo informacional passa a ser de difícil determinação, interminável e imprevisível” (BIONI, 2018, p. 145-146).

Sobre essa realidade, é clara a necessidade de que, ao menos, o titular fosse detentor do conhecimento de todo o processo, de todos os sujeitos envolvidos e de todas as ferramentas utilizadas para a mineração de seus dados pessoais, a fim de que fosse capaz de controlar suas informações através do instituto do consentimento. Contudo, diante das limitações racionais inerentes ao ser humano e outros dilemas, dificilmente tal ideal é colocado na prática.

Neste cenário, como bem aponta Slove (2013, p. 1880-1903)<sup>25</sup>, o consentimento restou uma alternativa falha, uma vez que os indivíduos sequer leem as políticas de privacidade que aderem ou, quando lêem, não entendem suas disposições. Ademais, caso compreendem, dificilmente possuem uma prévia ciência que lhes permitiria manifestar sua concordância ou, ainda, quando possuem, não há hipóteses e graus de escolha que permitam aos indivíduos selecionar e definir suas preferências.

Inclusive, para Doneda (2006, p. 373-374), o consentimento é tido como um “procedimento inócuo”, visto que as suas consequências são pouco visíveis aos interessados.

Observa-se que alguns aspectos são determinantes para as dificuldades enfrentadas, dentre os quais destaca-se: o dilema a respeito da eficácia do consentimento em face de, quando não consentido, o usuário é excluído do “mercado de consumo e da sociedade”; quando da afronta à proteção de dados realizada após o consentimento dado válido; bem como em relação aos problemas decorrentes do sistema denominado de “paradoxo da privacidade” (MENDES, 2014, p. 61).

A respeito deste último instituto, destaca-se a percepção de que, mesmo ao perseguir pela tutela jurídica que cabe ao indivíduo, há a necessidade de autorização para o tratamento de dados. Assim, quando há o consentimento no centro das prerrogativas de proteção dos dados, o titular adquire a sua tutela correspondente apenas em um momento que ocorre depois de consentir com a coleta e tratamento, “valendo-se do questionamento de algum efeito deste” (MALHEIRO, 2017, p. 40).

Conforme apresenta Doneda (2006, p. 375), a partir deste “paradoxo da privacidade”, o instituto do consentimento deveria ser retirado da posição central que

---

<sup>25</sup> Disponível em: [https://harvardlawreview.org/wp-content/uploads/pdfs/vol126\\_solove.pdf](https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf)

ele ocupa, uma vez que, “escorado na tecnicidade”, estaria neutralizando a ação dos direitos fundamentais.

Assim, o consentimento antes tratado como um mecanismo de “livre construção da esfera privada” passa a ser tido como uma ficção, tendo em vista que o seu uso pode ser movido pelos interesses daqueles que pretendem utilizá-lo. Porém, conforme já visto, o consentimento está respaldado pela autodeterminação individual do titular na tutela de seus dados, cabendo a esse indivíduo, portanto, conceder ou negar - “não é o consentimento em si que transmuda a informação pessoal em um bem jurídico” (MALHEIRO, 2017, p. 41).

Ademais, outra dificuldade em relação ao instituto é apontada por Bioni (2018, p. 146) acerca de que “as capacidades cognitivas do ser humano são limitadas, minando a sua capacidade de absorver, memorizar e processar todas as informações relevantes para um processo de tomada de decisão”. De fato, a impossibilidade é evidente no sentido de que seja possível captar todos os sujeitos envolvidos num amplo modelo de negócio pautado pelo fluxo de dados, quem dirá entender (principalmente para os leigos acerca da datificação) as ações feitas com as informações coletadas.

Freud, analisando o subconsciente humano há mais de um século, já afirmava que o indivíduo não era capaz de deter o total controle sobre as suas informações (RUARO, RODRIGUES E FINGER, 2011, p. 46).

Sob este cerne, observa-se as “barreiras psicológicas” que dificultam a habilidade de controle das informações por seus titulares. De imediato, ressalta-se a “teoria da decisão da utilidade subjetiva”, por meio da qual o titular analisa apenas os benefícios próximos, rápidos, sem sopesar os malefícios à privacidade que poderão surgir posteriormente (BIONI, 2018, p. 147).

Tanto isso é verdade que, conforme indica Sansana (2018, p. 16), uma pesquisa realizada pela Universidade de Stanford verificou que, dentre os usuários entrevistados que se deparavam com contratos, termos de aceite e políticas de privacidade, 97% não liam e passavam direto para a parte do “eu aceito”.

Portanto, tendo o titular valorizado o imediato e consentido com o compartilhamento de seus dados, dificilmente regressará com sua decisão, uma vez que “teve acesso a um produto ou serviço sopesará mais essa perda do que o ganho



de retomar, em tese, o controle de seus dados pessoais” (BIONI, 2018, p. 147-148). Em que pese haver um singelo consenso entre os usuários acerca da necessidade de proteção de seus dados, as atitudes desses atores se contradizem com suas estimas.

Nesse sentido, o autor (2018, p. 148-149) ressalta:

A crença de que o cidadão é um sujeito racional e capaz de desempenhar um processo genuíno de tomada de decisão para controlar seus dados pessoais é posta em xeque por toda essa complexidade envolta ao fluxo das informações pessoais. Ele está em uma situação de vulnerabilidade específica em meio a uma relação assimétrica que salta aos olhos, havendo uma série de evidências empíricas a esse respeito.

Tanto isso é verdade que Bioni (2018, p. 149-160) apresenta estudos empíricos que confirmam a sobrecarga existente sobre o consentimento. Entre tais, destaca-se o estudo da Universidade de Stanford e Carnegie Mellon denominado de *Mental Models*<sup>26</sup>.

A dita pesquisa, tendo como mentoras Lorrie Cranor e Aleecia McDonald, buscou identificar paradigmas presentes nas mentes dos consumidores virtuais sobre as diretrizes da publicidade direcionada através de entrevistas com os usuários. Inicialmente, além de constatar a falta de conhecimento técnico dos entrevistados para que pudessem “autodeterminar os seus dados no plano da coleta”, verificou-se um baixo índice (23%) daqueles que utilizava o modo de navegação privada, a fim de bloquear o recolhimento de seus dados, além de um número ainda menor (apenas 17%) dos que confirmaram a exclusão dos cookies durante a navegação (BIONI, 2018, p. 149).

Ao analisar esses últimos (deletam cookies), constatou-se que poucos o faziam em razão da proteção da sua privacidade, trazendo à luz o vício no processo de tomada de decisão quanto ao controle dos dados pessoais. Nesse sentido, Bioni (2018, p. 150) destaca que, dentre esses poucos, as respostas dadas eram curiosas, como: “i) “alguém recomendou que eu fizesse e, assim, eu tenho feito desde então” ou; ii) “minha mãe, minha filha ou meu pai me disseram”. Em termos percentuais, apenas 30% esclareceram que a “limpeza” de seus cookies estaria relacionada às questões de segurança e privacidade”.

Contudo, em que pese os dados apontados, a pesquisa ainda constata que os usuários afirmam se preocupar com o fluxo de dados: 70% afirma levar em

---

<sup>26</sup> Disponível em: <http://www.casos.cs.cmu.edu/publications/papers/METHOD08.pdf>.

consideração se a rede acessada para comprar online realiza compartilhamento de dados com terceiros (parceiros), bem como 64% julgam a atividade de vigilância dos consumidores como invasiva. Desse modo, tornou-se clara a contradição existente entre o modelo de negócio online e a perspectiva dos usuários.

Agravando a discordância, a última etapa da entrevista dividiu os entrevistados em dois grupos: os que pagariam um dólar para que os websites não pudessem adquirir seus dados e os que ganhariam um desconto no mesmo valor, desde que fosse aberta a coleta das suas informações. Em relação ao primeiro grupo, uma porcentagem pequena (11%) afirmou pagar a quantia, enquanto que a grande maioria (69%) dos usuários do segundo grupo acatou com o desconto, ainda que isso ocasionasse a perda do controle de seus dados. Por fim, juntou-se os dois grupos e constatou-se um consenso entre os entrevistados quanto à privacidade: 69% afirma se tratar de um direito, não devendo haver a obrigação de quitação para sua resguarda (BIONI, 2018, p. 150-151).

Constatou-se, assim, segundo como bem conclui o autor (2018, p. 152), a vulnerabilidade dos titulares de controle de suas próprias informações, uma vez que não estão capacitados para tomar atitudes acerca de tal. Segundo as pesquisadoras, o pouco conhecimento sobre o funcionamento do colhimento dos dados e seu tratamento e a busca por benefícios imediatos (ainda que resultem em perda de privacidade) resultam na desvalorização da técnica de tomada de decisões.

A prática da não leitura é mais comum, principalmente em virtude das suas longas extensões de escritas complexas, com detalhes extremamente técnicos e de difícil compreensão. Nesse sentido, conforme estudo apresentado por McDonald e Cranor (2008, p. 17)<sup>27</sup>, caso usuários realizassem a leitura de todas as políticas de privacidade das quais aderem, gastariam um montante de 244 horas por ano.

Como solução do dilema, necessário compreender que o instituto do consentimento não condiz com a falta de interesse do titular para a proteção de seus dados, mas sim uma representação do “ato de escolha no âmbito da autodeterminação individual” (MENDES, 2014, p. 61-62).

A respeito dessa realidade enfrentada, os doutrinadores acreditam se tratar de um “mito do consentimento”, uma vez que tal instrumento se mostra fictício e

---

<sup>27</sup> Disponível em: <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>.

ilusório: seus efeitos se perdem e os titulares dos dados perdem a autodeterminação informativa que lhes era prometida (MALHEIRO, 2017, p. 56).

A respeito disso, Rodotà (2008, p. 77):

[...] é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em “controle”. Aliás, a insistência em meios de controle exclusivamente individuais pode ser o álibi de um poder público desejo de esquivar-se dos novos problemas determinados pelas grandes coletas de informações, e que assim se refugia em uma exaltação ilusória dos poderes do indivíduo, o qual se encontrará, desta forma, encarregado da gestão de um jogo no qual somente poderá sair como perdedor.

Por fim, merece destaque, ainda, a dificuldade ocasionada em virtude de o “não consentimento” excluir e retirar o usuário do meio social online. Neste cenário, o elo mais fraco da relação (titular dos dados pessoais) “rende-se às forças do mercado informacional” (BIONI, 2018, p. 163) – o consentimento passa a ter um custo social.

Veja-se que, com a realidade do *sistema zero-price advertisement business*, por meio do qual o usuário concede seus dados para utilizar dos serviços e produtos, sem o pagamento de pecúnia, o consentimento surge como a porta de entrada.

Desse modo, para que o indivíduo tenha acessado ao ofertado, deve manifestar a autorização a respeito da coleta e tratamento de seus dados, deixando, assim, de ser livre o seu consentimento. “Nesse contexto, faz-se necessário, ao menos, que as normas gerais de proteção de dados pessoais contrabalanceiem tais interesses contrapostos. Caso contrário, pode haver uma distorção da própria proteção de dados pessoais ancorada no consentimento do seu titular” (BIONI, 2015, p. 54).

Sobre o assunto, Ponticelli (2018, p. 40):

Entretanto, mesmo que superada a barreira da desinformação e atingindo o objetivo de se possibilitar um verdadeiro esclarecimento dos termos de tratamento, de forma que o consentimento seja livre de qualquer vício, ainda há o revés de que, e muitos casos, o usuário é compelido ao aceite de qualquer imposição feita pelo agente de tratamento, uma vez que a conexão entre algumas aplicações, como o Facebook ou Google, e a vida em sociedade é muito próxima, fazendo com que o indivíduo que não participe dessas aplicações sofra com um constante isolamento social.

Assim, conforme apresentado pelo Article 29, trazido por Bioni (2015, p. 54-55), surge a possibilidade de um consentimento dito como “granular”, por meio do qual

o titular tem a liberdade de decidir sobre: (i) quais serão seus dados coletados; (ii) por quais modalidades de tratamentos eles serão submetidos; (iii) por qual período de tempo e frequência; e (iv) a possibilidade de compartilhamento com terceiros.

De acordo com Corrêa (2019, p. 32-33), o consentimento granular permite ao titular fragmentar as suas autorizações, ingressando, aos poucos e de maneira gradual, em meio ao fluxo de dados - por meio de tal, “o consentimento é procurado em cada tentativa de acesso aos dados pessoais”.

Desse modo, a realidade anterior na qual o indivíduo exercia a sua autodeterminação ao não consentir em transmitir seus dados e, conseqüentemente, via-se “alijado do acesso a determinado bens ou serviços” (DONEDA, 2006, p. 373) passa a ser deixada para trás, podendo o usuário ponderar a sua escolha.

Conclui-se, portanto, que, em que pese o indivíduo estar no controle de suas informações ser um grande passo para a proteção dos dados pessoais, a implementação do consentimento possui diversas dificuldades e se torna uma atividade complexa, principalmente devido à realidade na qual “nem sempre é possível ao indivíduo dimensionar as conseqüências futuras” ocasionadas com a disposição de seus dados (MENDES, 2014, p. 65).

Assim, o próximo capítulo analisará como as legislações têm tratado o tema para, por fim, verificar a disposição do instituto do consentimento na nova Lei Geral de Proteção de Dados Pessoais.

#### **4. TRAJETÓRIA NORMATIVA DO CONSENTIMENTO ATÉ A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS DO BRASIL (LEI N. 13.709/18)**

Na visão de Viktor Mayer-Scönberger, trazida por diversas doutrinas, o traçado evolutivo das leis que disciplinam a proteção dos dados pessoais em todo o mundo pode ser visto, a princípio, por quatro gerações distintas - parte-se de um cerne mais técnico e restrito para, por fim, ampliar as disposições e as técnicas referentes às tecnologias modernas (DONEDA, 2011, p. 96).

O contexto relacionado à primeira geração de leis que regulamentam os dados pessoais encontra-se voltado a aflições ocasionadas pelo processamento intensivo de dados pessoais direcionado à construção do Estado Moderno, além de representar uma reação às ideologias de concentração dos imensos bancos de dados nacionais (MENDES, 2014, p. 38).

Nesse momento, os regulamentos se direcionaram especificamente para a própria tecnologia, vista então como um meio que carecia de orientação para enquadrar-se dentro dos valores democráticos. A realidade da época, portanto, está relacionada à ideia de arquitetar “normas rígidas que tomassem o uso da tecnologia” (BIONI, 2018, p. 114).

Tanto isso é verdade que, como bem ressalta Doneda (2006, p. 208), os núcleos destes normativos estavam relacionados com a entrega do consentimento por parte dos titulares dos dados para a criação destes bancos de dados, além do “controle *a posteriori* por órgãos públicos”, o que fez, assim, com que o Estado fosse colocado como o destinatário principal desses regulamentos.

A respeito de tal, Mendes (2014, p. 39) ainda expressa:

Ademais, ao priorizar o controle rígido dos procedimentos, as normas desse período deixavam para segundo plano a garantia do direito individual à privacidade, o que pode ser percebido a partir do próprio jargão técnico utilizado nas normas.

Contudo, com o passar do tempo, logo esta primeira geração tornou-se obsoleta, vislumbrada como “virtualmente ineficaz” para uma proteção, por estar baseada em um simples regime de autorizações, marcado pela rigidez, e que ainda exigia “um minucioso acompanhamento” (DONEDA, 2006, p. 209).

Nesse sentido, como aponta Bioni (2018, p. 114), tendo em vista o exponencial crescimento das ferramentas tecnológicas, o tratamento de dados pessoais passou a ir além do domínio governamental, trazendo novos autores na

relação e a necessidade de uma evolução, também, na legislação sobre o tema: surge, assim, a segunda geração de leis de proteção de dados pessoais.

Nesta nova geração, a proteção dos dados se transfere para o próprio titular, de modo que cabe ao cidadão, através do seu consentimento, “estabelecer as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais” (BIONI, 2018, p. 115). Desse modo, o cerne dessa linhagem se encontra na autonomia entregue ao titular para o controle do trânsito de suas informações pessoais.

Sobre este momento, Mendes (2014, p. 40) ressalta:

Tais normas buscavam tratar prioritariamente do direito à privacidade, em vez de procedimentos. A temática da proteção de dados pessoais passa a se associar diretamente ao direito à privacidade, às liberdades negativas e à liberdade individual em geral.

Observa-se, portanto, o espírito desta geração voltado à sua estrutura, agora pautada na privacidade e na liberdade negativa da proteção dos dados pessoais, que passa a ser efetivada pela própria atuação dos seus titulares (DONEDA, 2006, p. 209).

Posteriormente, já na terceira geração, Bioni ressalta (2018, p. 116) que a linha desenvolvida anteriormente passa a ser ampliada: cabe ao cidadão participar de todos os processos que envolvem o tratamento de seus dados, incluindo, portanto, etapas como a coleta inicial e o compartilhamento com terceiros ao fim.

Constata-se, segundo o autor, a extensão dos regulamentos dessa época até atingir o conceito central da “autodeterminação informacional”, como bem trazido pela Corte Constitucional alemã ao julgar o censo do país: o titular merece ter um controle amplo sobre seus dados pessoais.

Neste momento, destaca-se a “sofistificação” da proteção dos dados pessoais, principalmente devido ao fato de ir além da liberdade entregue ao cidadão sobre ceder (ou não) seus dados a tratamento para abranger, inclusive, os meios de garantia da efetividade da atividade (DONEDA, 2006, p. 211). Consequentemente a tal, a tutela passa a ser vista como uma ação mais complexa do que era antes.

A principal distinção desta geração àquela anterior, segundo Mendes (2014, p. 40-41), está voltada ao fato de que a participação dos indivíduos nos tratamentos dos dados é colocada, agora, como um “envolvimento contínuo em todo o processo”, isto é, desde a coleta até o compartilhamento com terceiros, fugindo, assim, da ideologia do “tudo ou nada”.

Todavia, essa geração ainda acabou tendo percalços. Em verdade, a autodeterminação informativa se dava apenas para uma pequena parcela dos indivíduos que, efetivamente, cobriam as consequências econômicas e sociais derivadas das suas prerrogativas, o que dá ensejo ao surgimento da quarta geração (DONEDA, 2011, p. 98).

Nesse sentido, Bioni (2018, p. 116) ressalta:

Na feliz expressão de Mayer-Schonberger, somente os eremitas alcançariam a proteção plena de seus dados, já que, como decorrência da sua recusa em fornecê-los, amargariam o custo social decorrente da exclusão de tais atividades.

Desse modo, por fim, tem-se a quarta geração, abrangendo as principais leis que se encontram vigentes hoje e trazendo como distinção das demais a preocupação por eliminar as desvantagens do enfoque individual. Tanto isso é verdade que Bioni (2018, p. 117) realça a ideia de que o consentimento, diante de tal, começa a sofrer limites e condições (como no caso de compartilhamento de dados sensíveis), a fim de adequar a autonomia do titular de acordo com determinadas.

Conforme ainda observa o autor, tais medidas não alteraram o cerne dos regulamentos, sendo o consentimento ainda o traço marcante, apenas apresentaram uma “adjetivação” do termo, de modo que ele passa a ser tratado como “livre, informado, inequívoco, explícito e/ou específico”.

Para tanto, tais dispositivos se voltaram para enaltecer os titulares dos dados em face dos terceiros que coletam e realizam o tratamento dos dados, reconhecendo, assim, a assimetria existente nessa relação. Ao mesmo tempo, determinadas liberdades são retiradas dos indivíduos tendo em vista a sua maior importância e necessária proteção, além de ser intensamente buscada a relativização do “poder de barganha” pertencente àqueles controladores dos dados (DONEDA, 2011, p. 98).

Assim sendo, como destaca Mendes (2014, p. 43), esta última geração, na tentativa de solucionar os problemas anteriores, apresenta normas (como é o caso da Lei Geral de Proteção de Dados Pessoais do Brasil) em que o titular tem um maior autocontrole sobre seus dados.

Tendo em vista a grandiosidade do instituto do consentimento nas normas que tratam sobre a proteção de dados pessoais, este último capítulo do presente trabalho busca percorrer sobre o instituto dentre os principais diplomas na Europa (grande pilar da proteção à autodeterminação informativa), para, posteriormente,

analisar as normas brasileiras que foram setoriais à LGPD, e, por fim, esta última norma propriamente dita, novidade no ordenamento jurídico do país.

#### 4.1 Os basilares Regulamentos da União Europeia

Em que pese haver regulamentos anteriores<sup>28</sup> que mencionavam a proteção de dados pessoais e o instituto do consentimento, os países europeus (em especial os membros da União Europeia) passaram a se preocupar com o tema intensivamente a partir de 1980.

Neste ano, o Conselho da Europa promove a Convenção de 108, por meio do qual, já na própria introdução, apresenta-se a relação entre os dados pessoais e o livre fluxo informacional transfronteiriço. Percebe-se a sua influência, inclusive, quando da edição da Diretiva Europeia de Proteção de Dados Pessoais (95/46/EC)<sup>29</sup>, que traz o preâmbulo da Convenção anterior, além de diretrizes mais específicas (BIONI, 2018, p. 122).

Avante à proteção do titular de controlar seus dados, a diretiva inova ao introduzir deveres àqueles responsáveis pelo tratamento dos dados (*data controllers*)<sup>30</sup>.

Tanto isso é verdade que, dentre os seus princípios correlacionados, encontra-se o princípio da proporcionalidade que condiciona a estes sujeitos o tratamento apenas de dados que sejam essenciais ao fim desejado: “trata-se da ideia da minimização dos dados (*data minimization*) que permitirá, em última análise, que o titular dos dados pessoais maximize a sua esfera de controle sobre as suas informações pessoais” (BIONI, 2018, p. 123).

---

<sup>28</sup> “Em 1970, o Estado alemão de Hesse editou a primeira lei sobre essa matéria. A Suécia conta com o *Datalegen*, Lei 289 de 11 de maio de 1973. Desde 1977, a Alemanha tem uma lei federal de proteção de uso ilícito de dados pessoais. A Dinamarca regulamenta a questão da proteção de dados pelas Leis 243 e 244, ambas de 08 de julho de 1978, que estenderam a proteção também para as pessoas jurídicas. A França tem a Lei 78-77, de 06 de janeiro de 1978. A Espanha tem a peculiaridade de ter uma regra constitucional determinando a regulamentação da proteção da privacidade contra invasões da atividade informática (art. 18, par. 1º.). A Constituição de Portugal de 1977 tem texto ainda mais completo (art. 35), pois contempla a previsão do direito do cidadão de conhecer os dados que lhe são concernentes, de que esses dados sejam utilizados de acordo com a finalidade para o qual foram recolhidos e, ainda, de retificá-los (em caso de erro) e de atualizá-los”. Disponível em: [http://www.lex.com.br/doutrina\\_24316822\\_A\\_DIRETIVA\\_EUROPEIA\\_SOBRE\\_PROTECAO\\_DE\\_DADOS\\_PESSOAIS\\_UMA\\_ANALISE\\_DE\\_SEUS\\_ASPECTOS\\_GERAIS.aspx](http://www.lex.com.br/doutrina_24316822_A_DIRETIVA_EUROPEIA_SOBRE_PROTECAO_DE_DADOS_PESSOAIS_UMA_ANALISE_DE_SEUS_ASPECTOS_GERAIS.aspx)

<sup>29</sup> Versão em português disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>.

<sup>30</sup> Isto é possível perceber a partir da Seção VIII do referido diploma, que trata a respeito da confidencialidade e segurança do tratamento.



No art. 2º do referido documento, estabeleceu-se a identificação de terminologias básicas relativas ao tema para que, posteriormente, fossem colocados os princípios que estão intrínsecos à coleta, tratamento e utilização dos dados pessoais (MALHEIRO, 2017, p. 62).

Destaca-se, nesse dispositivo ainda, sua alínea h, na qual o consentimento é visto como “qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento”.

Já no art. 7º, alínea a<sup>31</sup>, desta Diretiva, observa-se a colocação do consentimento como um pressuposto que confere legalidade ao tratamento de dados pessoais, ressalvando as hipóteses em que houver previsão contratual ou legal (MENDES, 2014, p. 60).

Tamanha é a importância do instituto que, ao prever as restritas hipóteses de coleta e tratamento dos dados sensíveis, novamente o consentimento aparece, agora atrelado ao adjetivo *explícito* (grifou-se):

Art. 8º. Tratamento de certas categorias de dados.

1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.

2. O nº 1 não se aplica quando:

a) **A pessoa em causa tiver dado o seu consentimento explícito para esse tratamento**, salvo se a legislação do Estado-membro estabelecer que a proibição referida no nº 1 não pode ser retirada pelo consentimento da pessoa em causa (...).

Ademais, como bem lembra Brum da Silva e Leal da Silva<sup>32</sup>, a Diretiva ainda inova ao possibilitar aos indivíduos a correção e alteração das suas informações coletadas, além de revogar o consentimento anteriormente entregue, atos pelos quais destoa-se a autodeterminação informativa:

Artigo 12. Direito de acesso. Os Estados-membros garantirão às pessoas em causa o direito de obterem do responsável pelo tratamento:

b) Consoante o caso, a rectificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente directiva, nomeadamente devido ao carácter incompleto ou inexacto desses dados;

---

<sup>31</sup> “Art. 7º. Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se : a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento;”.

<sup>32</sup> Disponível em: <http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65>.

O regulamento se pauta, portanto, sobre o titular e os *data controllers*, de modo que a regulamentação europeia sai da terceira geração e passa a ser enquadrada na quarta geração de leis de proteção de dados pessoais (BIONI, 2018, p. 123-124).

Transformando os ordenamentos jurídicos nacionais em ordens jurídicas parciais, a União Europeia apresenta uma construção jurídica própria dentre seus 28 países membros (MALHEIRO, 2017, p. 60).

Sob este cenário, surge a Diretiva Europeia (2002/58)<sup>33</sup>, que traz especificações sobre a privacidade nas comunicações eletrônicas que, além de adjetivar o consentimento para o tratamento de dados pessoais como os diplomas anteriores, introduz a ideia de que deve ele ser *prévio* à coleta (BIONI, 2018, p. 124).

Observa-se que, como bem aponta Doneda (2006, p. 222), o referido diploma constitui-se fonte secundária dentro do sistema de fontes do direito comunitário europeu, tendo, assim, encargo primordial de uniformização legislativa.

A fim de uniformizar os ordenamentos entre os países integrantes da União Europeia, normas como esta servem para garantir direitos fundamentais, sendo, dentre todos, o máximo encontrado na Carta dos Direitos Fundamentais da União Europeia que, desde que entrou em vigor no ano de 2009, já previu a proteção dos dados pessoais dentre seu rol de grande importância (MALHEIRO, 2017, p. 61):

Art. 8º. Protecção de dados pessoais

1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

Em 2015, o direito comunitário europeu reformou seus diplomas, dando origem à GDPR - *General Data Protection Regulation*, grande protetora do consentimento, que, especificamente, tratou sobre o tratamento de dados pessoais e

---

<sup>33</sup> “Art. 13º. Comunicações não solicitadas. 1. A utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de correio electrónico para fins de comercialização directa apenas poderá ser autorizada em relação a assinantes que tenham dado o seu consentimento prévio”. Versão em português disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT>.

sua livre circulação. Em que pese o novo diploma ter revogado o anterior, ressalta-se que o Regulamento manteve seus princípios e objetivos (MALHEIRO, 2017, p. 63).

Dentre sua disciplina, observa-se a presença do instituto diversas vezes desde as suas considerações, demonstrando, conforme previsão do item 32, a adjetivação dada no novo instrumento de *livre, específico, informado e inequívoco*. Veja-se o referido dispositivo (grifou-se):

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

Ressalta-se, neste item, a abrangência do consentimento, que deverá estar relacionada a “todas as atividades de tratamento realizados com a mesma finalidade”, ao passo que é possível relacioná-lo, portanto, à expressão *finalidades determinadas*.

Além desta previsão, o consentimento é colocado como sendo informado em mais oportunidades do diploma (destaque ao item 42<sup>34</sup> das considerações), de modo que se observa a grande importância dada pelo Regulamento a este adjetivo específico. Dessa forma, o usuário poderá emitir uma manifestação de vontade com

---

<sup>34</sup> “(42) Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, **deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance**. Em conformidade com a Diretiva 93/13/CEE do Conselho, uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, **o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina**. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado” (grifou-se).

“conhecimento de causa”, o que reforça a ideia da autodeterminação informativa (MALHEIRO, 2017, p. 64).

Vale ressaltar ainda, segundo o item 60 das considerações, o imprescindível direito do titular ter a ciência acerca dos perfis e de seus riscos e consequências, além do que ocorrerá com os acessos caso o usuário não conceda seus dados:

(60) Os princípios do tratamento equitativo e transparente exigem que o titular dos dados seja informado da operação de tratamento de dados e das suas finalidades. O responsável pelo tratamento deverá fornecer ao titular as informações adicionais necessárias para assegurar um tratamento equitativo e transparente tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados. O titular dos dados deverá também ser informado da definição de perfis e das consequências que daí advêm. Sempre que os dados pessoais forem recolhidos junto do titular dos dados, este deverá ser também informado da eventual obrigatoriedade de fornecer os dados pessoais e das consequências de não os facultar. Essas informações podem ser fornecidas em combinação com ícones normalizados a fim de dar, de modo facilmente visível, inteligível e claramente legível uma útil perspectiva geral do tratamento previsto. Se forem apresentados por via eletrónica, os ícones deverão ser de leitura automática.

Do mesmo modo, toda vez que houver alteração na finalidade do tratamento dos dados, o controlador deverá imediatamente fornecer as informações novas ao indivíduo que concedeu seus dados, como indica o item 61:

(61) As informações sobre o tratamento de dados pessoais relativos ao titular dos dados deverão ser a este fornecidas no momento da sua recolha junto do titular dos dados ou, se os dados pessoais tiverem sido obtidos a partir de outra fonte, dentro de um prazo razoável, consoante as circunstâncias. Sempre que os dados pessoais forem suscetíveis de ser legitimamente comunicados a outro destinatário, o titular dos dados deverá ser informado aquando da primeira comunicação dos dados pessoais a esse destinatário. Sempre que o responsável pelo tratamento tiver a intenção de tratar os dados pessoais para outro fim que não aquele para o qual tenham sido recolhidos, antes desse tratamento o responsável pelo tratamento deverá fornecer ao titular dos dados informações sobre esse fim e outras informações necessárias. Quando não for possível informar o titular dos dados da origem dos dados pessoais por se ter recorrido a várias fontes, deverão ser-lhe fornecidas informações genéricas.

Desse modo, como indica Bioni (2018, p. 125), constata-se que o consentimento neste diploma europeu deve partir de uma “ação afirmativa ou declaração” que destaque esta manifestação de vontade do titular dos dados pessoais.

Convém dar destaque, ainda, ao artigo 46, item 1 do GDPR, que traz a restrição no sentido de que, obtido o consentimento adjetivado do titular, o

compartilhamento dos dados apenas poderão ser realizados com destino a países ou organizações internacionais que tenham leis nacionais que detenham proteções adequadas:

Artigo 46.º. Transferências sujeitas a garantias adequadas

1. Não tendo sido tomada qualquer decisão nos termos do artigo 45.o, n.o 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.

Por fim, ressalta-se que o Regulamento apresenta outras hipóteses legais de tratamento de dados pessoais, que vão além do consentimento, estando elas previstas no artigo 6º do Regulamento (MALHEIRO, p. 63). Neste sentido, veja-se a expressa previsão do item 40 das considerações (grifou-se):

(40) Para que o tratamento seja lícito, os dados pessoais deverão ser tratados **com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo**, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar.

Observa-se, portanto, como bem aponta Bioni (2018, p. 126), que o instituto do consentimento, em que pese continuar sendo o cerne do GDPR, aparece como “um dos fios condutores da recente reforma” dentre outros possíveis para a proteção dos dados pessoais.

Unindo as disciplinas dadas pelo diploma, de Sá (2018, p. 12) resume:

Em linhas gerais, segundo o GDPR, as empresas precisam obter o consentimento expresso e inequívoco dos titulares de dados para autorizar a coleta e tratamento desses dados, devendo expor claramente como essas informações serão utilizadas, além de explicar o mecanismo pelo qual os indivíduos poderão revogar esse consentimento, a qualquer momento.

Atualmente, segundo REINALDO FILHO<sup>35</sup>, muitos dos países europeus já possuem leis, em consonância com a GDPR, que tratam especificadamente da

proteção de dados pessoais, como é o caso da Áustria, Bélgica, República Checa, Finlândia, Hungria, Irlanda, Itália, Luxemburgo, Holanda, Suécia, Suíça e Inglaterra.

#### **4.2 As Principais normas Setoriais brasileiras anteriores à LGPD**

Tendo em vista que por muito tempo o Brasil não detinha legislação específica que tratasse sobre a proteção de dados pessoais, foi preciso harmonizar as mais diversas normas que mencionassem o tema para a aplicação pela doutrina e jurisprudência, “com a finalidade de construir um sistema de proteção de dados que, nos termos da Constituição Federal, proteja efetivamente a personalidade do cidadão” (MENDES, 2014, p. 141).

Partindo para análise linear no decorrer do ordenamento jurídico brasileiro, percebe-se que, como bem aponta Doneda (2011, p. 103), a proteção de dados pessoais foi assegurada, em princípio, implicitamente nos primeiros normativos.

Segundo o referido autor, apenas no item 45 da Declaração de Santa Cruz de La Sierra<sup>36</sup> (documento resultante da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo), assinada pelo país em 15 de novembro de 2003, foi possível destacar uma primeira alusão expressa à proteção de dados pessoais em caráter de direito fundamental.

Contudo, o início da segurança dada ao titular dos dados pessoais no Brasil se deu, ainda que de maneira tácita, a partir da Constituição Federal de 1988, na qual, como proteção ao direito da personalidade e, principalmente, à personalidade, destacam-se as garantias dadas pela liberdade de expressão (art. 5º, IX) e pelo direito à informação (art. 5º, XIV).

Ademais, a Carta Magna apresenta a inviolabilidade da vida privada e da intimidade, em seu art. 5º, inciso X, vedando a interceptação das comunicações telefônicas, telegráficas ou de dados (art. 5º, XII), além de instituir o instrumento judicial denominado de habeas data (art. 5º, LXXII), por meio do qual se estabelece a garantia de acesso e retificação dos dados pelos indivíduos. Veja-se os dispositivos supramencionados:

---

<sup>36</sup> “45. Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras iberoamericanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade”. Disponível em: <https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf>

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;

[...]

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;

[...]

XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

[...]

LXXII - conceder-se-á habeas data:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

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

A respeito da ação de habeas data, segundo Doneda (2011, p. 104), a CF/88 permitiu que os indivíduos pudessem ter acesso às suas informações colocadas em órgãos públicos, de modo a ser possível constatar certa “influência da experiência europeia ou norte-americana relativa à proteção de dados pessoais já em pleno desenvolvimento à época” (DONEDA, 2011, p. 104).

Porém, como ressalta o autor, a análise das disposições constitucionais conscritas “sob o prisma de sua comunicação e de eventual interceptação” acaba por não abranger a grandeza de todo o sistema. A partir de então, outras normas passaram a colocar a proteção dos dados em suas previsões (implícita ou explicitamente), destacando-se, seguindo a linha cronológica, o Código de Defesa do Consumidor de 1993.

Assim, conforme o artigo 43 disciplina do diploma consumerista, apresentam-se a proteção frente aos bancos de dados e cadastros dos consumidores, os quais o CDC indica serem instrumentos amplos e capazes de absorver inúmeros dados, indo muito além de meras informações negativas que objetivassem a concessão de crédito, como muitos acreditavam (BIONI, 2018, p. 126-127).

Segundo o dispositivo, para que esses dois institutos funcionem em regularidade com a lei, devem preencher determinados requisitos, como, por exemplo,

a imprescindível comunicação da abertura de um cadastro ou registro de dados pessoais de consumo (MENDES, 2014, p. 142). Veja-se:

Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

§6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

Com o exemplo das legislações europeias à época, o CDC buscou assegurar ao titular o controle de seus dados, de modo que fosse ele capaz de autodeterminar as suas próprias informações. Percebe-se tal segurança, inicialmente, quando o diploma indica que o consumidor deve ser comunicado da abertura de um banco de dados pessoais por ele não solicitado (§2º), de maneira prévia para que possibilite o seu acompanhamento (BIONI, 2018, p. 127).

Para Doneda (2011, p. 103), ao elaborar esta lei no tocante à concessão de crédito, o legislador teria se baseado em uma sistemática pautada no *Fair Information Principles*, de modo que uma parcela da doutrina brasileira a considera como um “marco normativo dos princípios de proteção de dados pessoais” no país.

A respeito dos princípios e da necessidade de informação dada pela normativa, Bioni (2018, p. 127-128) destaca:

A referida transparência só tem razão de ser porque o operador dos bancos de dados terá, simetricamente, os deveres de: i) garantir o seu acesso pelo consumidor (art. 43, caput, do CDC); ii) exatidão de tais informações; iii) que o banco de dados se restrinja para finalidades claras e verdadeiras e, por fim; iv) que seja observado o limite temporal de cinco anos para o armazenamento de informações negativas (art. 43, § 1º, do CDC).



Percebe-se, portanto, segundo o autor (2018, p. 128), a tentativa do diploma consumerista de proteger o titular, dando possibilidade de conferência, alteração e exclusão de seus dados, e, assim, conferindo-lhe autodeterminação informacional.

Já no ano de 2011, tendo em vista os bancos de dados anteriormente regulados pelo CDC, a Lei 12.414/2011, denominada de “Lei do Cadastro Positivo”, estabelece novas disciplinas sobre tais, porém agora em relação aos dados derivados de operações financeiras e dos adimplementos dos consumidores, facilitadores da concessão de crédito.

Nesta norma, foi sistematizada a ideia de que o titular possui como um de seus direitos o poder de gerenciar seus dados pessoais, a fim de reduzir a assimetria da relação entre titular e controladores.

Para tanto, como bem aponta de Sá (2018, p. 24), o diploma adotou o entendimento de que, para o compartilhamento de dados tornar-se lícita, ocorreria apenas após a obtenção do consentimento<sup>37</sup> – a referida lei consolida, a partir de tal, a “evolução do conceito de autodeterminação informativa no nosso ordenamento” (MENDES, 2014, p. 146).

Assim, em que pese seguir os princípios regentes das relações de consumo, a Lei de Cadastro Positivo ultrapassa a ideia do CDC de uma simples notificação quanto da abertura dos bancos e passa a exigir o real consentimento do seu titular, devendo ele agora ser “informado e externado por meio de assinatura em um instrumento específico ou em cláusula apartada” (BIONI, 2018, p. 129).

Nesta seara, o diploma introduz a lógica do opt-in no ordenamento jurídico brasileiro, de modo que, segundo Monteiro (2018), “essa alteração automaticamente incluiria os dados de mais de 30 milhões de brasileiros em sistemas geridos por empresas”.

Ainda, surge o dever do controlador da base de, além de não utilizar de informações desnecessárias para seu fim, deixar de coletar dados sensíveis - o diploma apresenta um limite de coleta e de tratamento dos dados a fim de possibilitar ao seu titular a gerência sobre suas informações. Neste sentido, o seu art. 3º:

---

<sup>37</sup> “Art. 4º. O gestor está autorizado, nas condições estabelecidas nesta Lei, a: (...) IV – disponibilizar a consulentes: (...) b) o histórico de crédito, mediante prévia autorização específica do cadastrado”.

Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.

[...]

§ 3º Ficam proibidas as anotações de:

I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e

II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Importante destacar, ainda, a previsão do art. 17<sup>38</sup> da lei, por meio da qual a atuação de autoridade administrativa para o controle da atividade de processamento de dados foi expressa, “de modo a se ter um sistema administrativo de fiscalização e resolução de conflitos em conjunto com um sistema clássico judicial de resolução de lides” (MENDES, 2014, p. 147-148).

Ademais, no seu artigo 5º, dentre os direitos assegurados aos cadastrados, há a previsão acerca da ciência prévia destes, de modo que devem ser eles informados a respeito do armazenamento, de quem governará seus dados, do objetivo de tal e para quem seus dados serão compartilhados, retomando, assim, a ideia de que o futuro consentimento (se vier) será válido (CORREA, 2019, p. 46):

Art. 5º São direitos do cadastrado:

[...]

V - ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais.

Conforme leitura de Doneda (2006, p. 386), o referido diploma é responsável, também, por integrar ao nosso ordenamento jurídico alguns dos princípios relativos à proteção de dados pessoais em outros países, de modo que a LCP “refletisse com maior intensidade, em seu tempo, um modelo de proteção de dados pessoais – ainda que restrito ao seu âmbito, referente aos históricos de crédito”.

Inaugurando a especificidade de normativos no tocante à segurança dos direitos e garantias nas relações eletrônicas, tem-se o Marco Civil da Internet (Lei

---

<sup>38</sup> “Art. 17. Nas situações em que o cadastrado for consumidor, caracterizado conforme a Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor, aplicam-se as sanções e penas nela previstas e o disposto no § 2º. §1º Nos casos previstos no caput, a fiscalização e a aplicação das sanções serão exercidas concorrentemente pelos órgãos de proteção e defesa do consumidor da União, dos Estados, do Distrito Federal e dos Municípios, nas respectivas áreas de atuação administrativa. §2º Sem prejuízo do disposto no caput e no § 1º deste artigo, os órgãos de proteção e defesa do consumidor poderão aplicar medidas corretivas e estabelecer aos bancos de dados que descumprirem o previsto nesta Lei a obrigação de excluir do cadastro informações incorretas, no prazo de 10 (dez) dias, bem como de cancelar os cadastros de pessoas que solicitaram o cancelamento, conforme disposto no inciso I do caput do art. 5º desta Lei”.

12.965/2014) que, segundo Bioni (2018, p. 130) apresenta como destaque nas suas disposições “uma técnica normativa prescritiva e restritiva das liberdades individuais”.

Nesse sentido, como ressalta o autor, em um momento no qual o caso de espionagem delatado pelo ex agente da Agência Nacional de Segurança dos Estados Unidos, surge a expressa proteção à privacidade, como também aos dados pessoais<sup>39</sup>, sendo esta última regulamentada em lei posterior.

Observa-se, assim, que o cerne do diploma não está na regramento detalhado sobre a proteção de dados pessoais, deixando esta incumbência à normativo ulterior, o qual veio a ocorrer apenas em 2018, com a Lei Geral de Proteção de Dados Pessoais (MALHEIRO, 2017, p. 68). Porém, já é possível encontrar no Marco Civil da Internet a base dos direitos assegurados aos usuários.

A título exemplificativo, após o escândalo narrado, o art. 7º do diploma recebeu novos dispositivos, todos referentes estes direitos e à proteção de dados pessoais e, conforme De Lucca, Simão Filho e Lima (2015, p. 266):

Para além dessa guinada quantitativa, constata-se, sobretudo, uma alteração de conteúdo do próprio texto da lei, tendo o legislador eleito um parâmetro normativo muito claro a respeito da proteção dos dados pessoais. Trata-se da autodeterminação informacional fundada na perspectiva de que o próprio usuário deve ter controle sobre as suas informações pessoais, autodeterminando-se. Socorrer-se, por isso, a técnica de se exigir o consentimento do titular dos dados pessoais para que eles sejam coletados, processados e compartilhados [...].

Os novos traços trazidos pela revisão do diploma expressam o indispensável consentimento do titular para que seja possibilitada as ações feitas sobre seus próprios dados (BIONI, 2018, p. 131-132).

Nesse sentido, o Marco Civil da Internet estabelece que esse importante instituto deve ser *livre, expresso e informado* (art. 7º, VI, VIII, IX e XI<sup>40</sup>) - quem utiliza dos dados deve ser claro e indicar completamente as informações ao usuário, através

---

<sup>39</sup> “Art. 3º. A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei;”.

<sup>40</sup> “Art. 7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; [...] VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;”.

de mecanismos cristalinos e completos, acerca de todo os procedimentos (coleta, uso, armazenamento, tratamento e proteção) relativos aos seus dados, sendo que, quando concedido o tratamento, as finalidades anteriormente indicadas não poderão sofrer mutações (MALHEIRO, 2017, p. 69).

Em atenção ao adjetivo *livre*, Masso, Abrusio e Florencio Filho (2014) destacam, desde já, a necessidade de ser dado ao titular dos dados a possibilidade de optar parceladamente sobre as cláusulas ou contratos, e não o todo, “desde que seja informado das consequências possíveis, como uma eventual impossibilidade de utilizar o serviço como um todo”.

Ademais, o MCI apresenta ainda o direito de o titular, uma vez finalizada sua relação com aqueles que coletaram seus dados devidamente, requerer a exclusão definitiva de suas informações<sup>41</sup>.

Acerca deste tema, Bioni (2018, p. 132) afirma:

Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento. Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento dos dados com terceiros até o direito de deletá-los junto ao prestador de serviços e produtos de Internet ao término da relação.

Tendo em vista a necessidade de uma lei específica para sistematizar um assunto de extrema importância, no ano de 2015, o Ministério da Justiça apresentou um anteprojeto de lei que tratava sobre a proteção de dados pessoais<sup>42</sup>.

Trazendo a contribuição da sociedade para tal, foi aberta a consulta pública acerca do tema, através do site Pensando Direito<sup>43</sup>, pelo prazo de 10 meses, recebendo, ao final, mais de duas mil interações (MALHEIRO, 2017, p. 70).

Neste período, em 2017, importante destacar que o Superior Tribunal de Justiça, julgando sobre o tema<sup>44</sup>, repercutiu na mídia ao considerar abusivas as cláusulas de contratos padrões de determinado banco que permitiam o compartilhamento dos dados de seus consumidores (dados de hábitos de consumo) com as empresas parceiras.

---

<sup>41</sup> “Art. 7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;”.

<sup>42</sup> A plataforma pode ser acessada em: <http://pensando.mj.gov.br/dadospessoais/>

<sup>43</sup> Disponível em: <https://direitosnarede.org.br/blog/>

<sup>44</sup> REsp 1.348.532-SP, Rel. Min. Luis Felipe Salomão, j. 10/10/2017.

Nas palavras do voto do relator, Ministro Luis Felipe Salomão:

Com efeito, a controvérsia dos autos, conforme dito, está na determinação da abusividade de cláusula contratual que retire do consumidor a possibilidade de optar, válida e livremente, pelo compartilhamento dos dados que dá a conhecimento de certo e determinado banco, no momento em que ele contrata o serviço de cartão de crédito.

Desse modo, segundo o STJ, a referida cláusula estaria ferindo princípios como o da transparência e da confiança, consideradas, portanto, abusivas.

Posteriormente, já em 2018, o documento advindo da consulta pública, após algumas mudanças, tornou-se o Projeto de Lei n. 53/2018.

### **4.3 A Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18)**

Decorrente do Projeto de Lei nº 53/2018, a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018), baseada nos dispositivos presentes na GDPR, apresenta seu cerne na identificação de mecanismos pelos quais entidades públicas e privadas possam coletar e tratar dados derivados de pessoas identificadas ou identificáveis (ENJISMAN e LACERDA, 2019<sup>45</sup>).

Tamanha é a importância da legislação própria no país que, como indica Monteiro<sup>46</sup> (2018), com LGPD “o Brasil entra para o rol de mais de 100 países que hoje podem ser considerados adequados para proteger a privacidade e o uso de dados”.

Observa-se que, após consultas públicas, o Congresso Nacional, ao aprovar o PL e posteriormente instituir a Lei 13.709/18, colocou o instituto do consentimento como uma das hipóteses de permissão de tratamento (art. 7º, inciso I<sup>47</sup>), mas não a única.

Neste sentido, Bioni (2018, p. 133-134) destaca:

Isso significa dizer que, em termos de técnica legislativa, o consentimento não só deixou de ser a única base legal para o tratamento de dados, como também foi alocado topograficamente sem ser hierarquicamente superior às demais bases legais por estarem elas horizontalmente elencadas em incisos do art. 7º da LGPD.

---

<sup>45</sup> Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/coluna-do-tozzinifreire/lei-geral-de-dados-pessoais-01012019>.

<sup>46</sup> Disponível em: <https://baptistaluz.com.br/institucional/lei-geral-de-protacao-de-dados-do-brasil-analise/>.

<sup>47</sup> “Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular;”.

Contudo, o consentimento não perdeu a sua importância: segundo o autor (2018, p. 134), conforme os princípios da lei, a carga participativa do titular sobre o trânsito de seus dados mantém-se no cerne das previsões, constatando-se a presença do termo 37 vezes na referida lei.

Nesse sentido, o artigo publicado pelo SERPRO intitulado “Seu consentimento é lei!”<sup>48</sup>, que busca elucidar pormenores a LGPD, menciona:

Se a gente fosse eleger a principal palavra da Lei Geral de Proteção de Dados Pessoais (LGPD), a escolhida seria, sem dúvidas, CONSENTIMENTO. É o titular, ou seja, a pessoa quem se referem os dados que deve, se quiser - ao ser questionada, de forma explícita e inequívoca - autorizar que suas informações sejam usadas, por empresas e órgãos públicos, na hora da oferta de produtos e serviços, gratuitos ou não.

Tanto isso é verdade que, seguindo mesma linha das disciplinas europeias da quarta geração, o consentimento no Brasil prescinde dos adjetivos *livre*, *informado*, *inequívoco*, atrelado a *finalidades determinadas*, conforme se observa do art. 5º, XII, da LGPD (grifou-se):

Art. 5º. Para os fins desta Lei, considera-se:

[...]

XII - consentimento: **manifestação livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma **finalidade determinada**.

No tocante à declaração de vontade *livre* do titular, observa-se que a LGPD indica as vertentes qualitativa (deve a informação ser clara, adequada e ostensiva) e quantitativa, ao ilustrar, ainda que em rol taxativo, as espécies de informações que deverão ser repassadas, no seu art. 9º, *caput*:

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

---

<sup>48</sup> Disponível em: <https://www.serpro.gov.br/lgpd/cidadao/seu-consentimento-e-lei>.

Avançando pelo dispositivo, observa-se as importantes previsões em seus dois parágrafos que tratam sobre o instituto: no primeiro<sup>49</sup>, o legislador destaca que a ciência dada ao titular antes do seu consentimento deve partir de informações corretas e claras, de modo que, caso houver atos enganosos ou abusivos por parte dos controladores, o consentimento dado passa a ser nulo; já no segundo<sup>50</sup>, a ênfase está na mudança da finalidade dos tratamentos dos dados coletados - qualquer alteração deve ser notificada ao titular para que este, por livre vontade, decida se deseja manter o seu consentimento ou se prefere revogá-lo (AGOSTINELLI, 2018<sup>51</sup>).

Nesse sentido, como indica Bioni (2018, p. 195), vale destacar que o consentimento *informado* implica em um conhecimento prévio de elementos necessários para que o titular dos dados pessoais possa iniciar a racionalização de suas decisões.

Para tanto, a LGPD concretiza essa realidade ao prever, inicialmente em seu art. 6º, inciso VI<sup>52</sup>, o princípio da transparência como a necessária transmissão de informações (conforme a lei, “claras, precisas e facilmente acessíveis”), bem como quando destaca a possibilidade de nulidade da declaração de vontade no momento em que tal princípio não esteja concretizado (art. 9º, §1º<sup>53</sup>).

Assim, segundo o referido autor, o regulamento tenta perfectibilizar o processo prévio, trazendo a boa-fé atrelada a uma relação sincera e cristalina, garantindo a solidificação da autodeterminação informacional dos usuários (elo fraco da relação).

Ademais, tal previsão pode ser constatada, ainda, dentro dos deveres dos controladores, uma vez estar prevista a necessidade de ser transpassado, com

---

<sup>49</sup> “§1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca”.

<sup>50</sup> “§2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações”.

<sup>51</sup> Disponível em: <http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7025/67647038>.

<sup>52</sup> “Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;”.

<sup>53</sup> “Art. 9º [...] §1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca”.

clareza, aos titulares, os procedimentos pelos quais os dados irão passar antes do próprio consentimento. “Deixar claro o porquê, para que, como e quando serão utilizados os dados pessoais são informações essenciais para que o controlador informe ao titular” (SANSANA, 2018, p. 20).

Ao unir o consentimento ao adjetivo *livre*, a LGPD propõe a busca por uma declaração de vontade realizada pelo livre-arbítrio do titular dos dados, sem qualquer força ou pressão externa (BIONI, 2018, p. 197).

Para tanto, a lei brasileira de proteção de dados reserva ao cidadão a segurança de que ele deverá ser informado, sempre que a coleta de seus dados for um requisito para atingir determinado fim, as modalidades por quais poderá exercer seus direitos (art. 9º, § 3º<sup>54</sup>), como é o caso da revogação do consentimento antes declarado.

Já a respeito do adjetivo *inequívoco*, ressalta-se a interpretação de que não poderá haver incertezas quanto à autorização dada pelo titular acerca da entrega de seus dados, sendo ônus do controlador elaborar a prova de que houve a vontade do titular, seja por meio escrito ou diverso:

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

A escolha do legislador para tal previsão demonstra a sua preocupação em vedar a previsão do consentimento em “cláusulas escondidas, estimulando a publicidade do uso que será feito pelo controlador dos dados pessoais dos usuários” (SANSANA, 2018, p. 18).

Assim, segundo de Sá (2018, p. 34), diferente do que ocorre nos Estados Unidos onde um simples aviso de que houve atualização nas Políticas de Privacidade ou Termos de Uso já aceitas, no ordenamento jurídico brasileiro torna-se imprescindível a prova de mais um consentimento adjetivado (art. 8º, §2º<sup>55</sup>).

Conforme Enjisman e Lacerda (2019), está é uma das grandes novidades da lei, visto que, agora, ao controlador (aquele que coleta os dados e os utiliza, seja pessoa natural ou jurídica, de direito público ou privado) caberá comprovar a obtenção

---

<sup>54</sup> “Art. 9º. [...] §3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei”.

<sup>55</sup> “Art. 8º. [...] §2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei”.



do consentimento. Isto é, aqueles responsáveis pelos “bancos de dados terão que criar estruturas tecnológicas que garantam o arquivamento do consentimento, assim como o cumprimento de outros direitos agora assegurados ao titular”

Aplicando o princípio da *finalidade* ao sistema (art. 6º, I, da LGPD<sup>56</sup>), inicialmente tem-se que o tratamento dos dados passa a ser uma atividade exercida com um fim “específico e explícito”, ao passo que, ao relacionar com o instituto do consentimento, atrela-se ele à imprescindibilidade de direção.

Tal fato serve, inclusive, segundo Bioni (2018, p. 198), como um caminho a ser perseguido (posteriormente) para a verificação da informações passadas ao usuário que deu origem à declaração de vontade livre.

Desse modo, o tradicional “li e aceito” passa a ser meio inaceitável para obtenção do consentimento, tendo em vista que não demonstra a capacidade de consentir dos titulares dos dados. Neste sentido, Enjisman e Lacerda (2019) indicam:

São várias as opções que podem ser utilizadas. Um bom exemplo seria elencar um vídeo assistido até o final, seguido da redação, pelo titular, de uma frase determinando que está de acordo com os usos de seus dados descritos no vídeo. Além disso, seria possível também solicitar o consentimento por foto, vídeo gravado pelo titular, ou até mesmo por opt-in, após a apresentação da Política de Privacidade de maneira didática e de simples entendimento, com as finalidades de tratamento separadas e sendo possível consentir individualmente para cada uma delas.

Ademais, retira-se dos princípios previstos nesta lei, além dos clássicos já vistos em demais legislações (i.e., especificação dos propósitos do tratamento), que o recente diploma apresenta novidades, enquadrados na modernidade, como se pode perceber dos princípios da adequação e da necessidade, objetivando que os dados sejam indispensáveis para o propósito do tratamento, de modo proporcional e não excessivo - trata-se do sistema de minimização dos dados (BIONI, 2018, p. 134-135).

Sobre tal, Campos Soares<sup>57</sup> (2019) afirma:

Esse rígido conjunto de requisitos, verdadeiros qualificadores do consentimento, deve ser corretamente apreendido e aplicado pelo agente de tratamento de dados, seja ele o controlador ou o operador. Deve, por igual, ser avaliado com cautela pelo respectivo encarregado de proteção de dados,

---

<sup>56</sup> “Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;”.

<sup>57</sup> Disponível em: <https://www.conjur.com.br/2019-mai-11/pedro-soares-questao-consentimento-lei-protacao-dados>.

incumbido da tarefa de desenvolver meios para a correta aplicação da lei e acompanhar, no âmbito interno da empresa, o seu cumprimento.

Partindo como a máxima expressão participativa do titular, têm-se ainda os adjetivos *específico* e *expresso*.

Em relação àquele, tamanha é a sua relevância que a Lei Geral de Proteção de Dados Pessoais o retoma em quatro cenários específicos presentes nas previsões do art. 7º, § 5º (relação de terceiros desconhecidos do titular), art. 11, inciso I (quando se tratar de dados sensíveis), art. 14, §1º (quando os usuários forem crianças e adolescentes), bem como no art. 33, inciso VIII (casos de transferências dos dados ao exterior, em países nos quais a proteção dos dados é diversa da brasileira). Assim, ao unir tal adjetivo à declaração de vontade, a LGPD busca acrescentar mais uma proteção em face das situações de maior ameaça.

Contudo, diferente do que a GDPR chamou de *expresso*, o diploma brasileiro apresenta o termo *específico* com a ressalva de que o consentimento do titular já deve estar voltado à finalidades. Nesse sentido, para Bioni (2018, p. 202), tal especialidade aderida à declaração de vontade serve como “um vetor para que haja mais assertividade do titular em relação a esses movimentos ‘específicos’ de seus dados”.

Para verificar tal especificação, deve-se partir para análise dos procedimentos realizados pelo titular para demonstrar o seu consentimento, como é o caso de caixas de texto, imagens ou símbolos em sua navegação, de modo que sua deliberação nas situações previstas ressalte aos olhos frente ao intenso fluxo de dados.

Percebe-se, portanto, que por detrás das características impostas ao consentimento por meio de adjetivos, há a ponderação da “carga participativa exigida” do titular sobre o fluxo de seus dados pessoais (BIONI, 2018, p. 203).

A LGPD está nivelada, além de seus próprios princípios, com “as tendências internacionais por conta do protagonismo dado ao titular em relação aos seus dados” (ENJISMAN e LACERDA, 2019), de modo que a intensa busca do diploma está na atuação daqueles que controlam os dados coletados, a fim de que comprovem agir intensivamente para que o titular possa consentir livre, informada e inequivocadamente.

Assim, conclui-se que a inovação trazida pela lei está relacionada com a ideia de que o instituto do consentimento deixou de ser o único meio possível de legitimar os tratamento de dados pessoais, sendo, por exemplo, necessário avaliar ainda qual

o propósito da coleta por terceiros e, assim, identificar qual o inciso previsto no art. 7º da lei que melhor atenda às suas necessidades.

## 5. CONSIDERAÇÕES FINAIS

Conforme visto no presente trabalho, no segundo capítulo, a expressão “dados pessoais” retoma aqueles dados que, além de estarem relacionados a determinada pessoa, eles identificam ainda seus pensamentos e seus modos de agir, seus costumes e hábitos de consumo, de modo que, quando expostos, ficam a mercê de coletas, tratamentos e compartilhamentos com terceiros. Assim, tem-se que os dados pessoais destoam uma miríade de informações dos usuários quando disponibilizados na via digital.

A sua proteção, a partir da evolução tecnológica, passou a ser o centro da discussão de muitos juristas, com atenção especial a partir da década de 1970, na qual presenciou-se o fenômeno mundial de interconexão entre todos os indivíduos online.

Desde então percebeu-se que, quando interligada a informação com a tecnologia, com base no fornecimento dos dados pessoais, os usuários estariam pouco protegidos e viam sua privacidade ser afrontada constantemente.

A fim de resguardar sua proteção, tais informações passaram a ser identificadas legalmente como mecanismos pelos quais o titular possa desenvolver sua personalidade de forma livre, vindo a representar, assim, uma extensão do próprio indivíduo.

Ademais, atrelando os dados pessoais como uma projeção da personalidade dos indivíduos, sendo assim merecedores de proteção como direitos fundamentais, tais informações encontram-se abrigadas pelo direito à privacidade.

Nesse sentido, conforme visto no terceiro capítulo, surge o instituto do consentimento, instrumentalizado em uma dualidade, uma vez ser visto como a confirmação da autodeterminação informativa e como meio de legitimação para o tratamento dos dados pessoais.

Com base em tal, quando devidamente adjetivado de livre, informado, inequívoco e com finalidades determinadas, cabe ao usuário decidir quando consentir com a coleta de seus dados, para qual instintos e por quanto tempo.

Porém, para que seja verdadeiramente válido, o consentimento exige a fiel informação por parte daqueles que tratam os dados, identificando todos os sujeitos envolvidos e todas as ferramentas utilizadas para tal, o que em realidade é pouco visível e necessitaria de intensa regulamentação e controle.

Desse modo, o instituto passa a ser uma medida muitas vezes falha, tendo em vista que sequer há a leitura por parte dos usuários dos termos de uso ao consentir, ou, quando lêem, não entendem as cláusulas propostas pelas plataformas digitais.

Legalmente, como visto no último capítulo, o instituto se apresenta com maior relevância, inicialmente, na União Europeia, com destaque para a Diretiva Europeia de Proteção de Dados Pessoais (95/46/EC), que estabeleceu o consentimento como qualquer manifestação livre, específica e informada, por meio da qual o indivíduo possa delimitar a sua vontade de que sejam seus dados passíveis de tratamento. Neste regulamento, o instituto era visto como pressuposto de validade do tratamento, sendo exceção apenas quando houvesse previsão legal ou contratual a respeito.

Já com o *General Data Protection Regulation*, no ano de 2015, o consentimento passa a ser ainda mais adjetivado (livre, específico, informado e inequívoco), sendo relacionado como uma dentre outras medidas passíveis de legitimar o tratamento de dados.

Já no Brasil, por muito tempo o ordenamento jurídico ficou aquém de uma legislação específica sobre o tema. Desse modo, outras normas foram setoriais para que os juristas pudessem discutir, com destaque ao CDC e à Lei do Cadastro Positivo que tratavam a respeito de operações financeiras e adimplemento dos consumidores.

Conforme disposições dos dois diplomas, o compartilhamento de dados coletados apenas poderiam ser legitimados com a obtenção do consentimento (sem qualquer adjetivação), vindo a LCP a ser marcada pela evolução do conceito de autodeterminação informativa no sistema legal brasileiro.

Já no Marco Civil da Internet, no ano de 2014, em que pese não haver um regramento detalhado sobre a proteção de dados pessoais, o consentimento passa a ser adjetivado como livre, expresso e informado, de modo que, quando concedido, deveria respeitar as finalidades previamente indicadas.

Foi apenas em 2018, com a Lei Geral de Proteção de Dados Pessoais que o Brasil passou a ser corretamente disciplinado sobre o assunto.

Neste regulamento, o consentimento encontra-se novamente adjetivado, agora de livre, informado, inequívoco, expresso e atrelado a finalidades determinadas, de modo que é assegurado incisivamente ao titular o direito de receber informações prévias e claras para que possa consentir devidamente.

Ademais, a lei tenta perfectibilizar o processo prévio, atrelando o princípio da boa-fé à relação estabelecida, de modo a garantir a solidificação da autodeterminação informacional dos usuários.

Para tato, o comum “li e aceito” passa a ser visto como meio inadequado de proteção, estando aquém das especificidades correlacionadas e imprescindíveis ao consentimento.

Nesse aspecto, a LGPD passa a ser nivelada dentre as tendências mundiais, tendo em vista o destaque que é dado ao titular dos dados como o protagonista dentro de sua relação com seus dados pessoais.

Contudo, vale ressaltar ainda que, em que pese ser o cerne do regulamento, o instituto do consentimento foi colocado nesta lei, assim como no GDPR, como um dentre outros meios possíveis de legitimar o tratamento de dados pessoais.

Assim, diante da análise realizada, observa-se que a autodeterminação informacional, instituída a partir do consentimento, sempre esteve no cerne dos diplomas, tanto europeus, quanto brasileiros, porém agora vista na LGPD como uma medida, dentre tantas outras possíveis de legitimar o tratamento de dados pessoais.

## REFERÊNCIAS

- AGOSTINELLI, Joice. **A importância da Lei Geral de Proteção de Dados Pessoais no ambiente online**. Toledo Prudente Centro Universitário. Encontro de Iniciação Científica, 2018. Disponível em: <<http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7025/67647038>>. Acesso em: 02 nov. 2019.
- BAUMAN, Zygmunt. **44 cartas do mundo líquido moderno**. Rio de Janeiro: Jorge Zahar, 2011.
- BAUMAN, Zygmunt. *A modernidade líquida: o sujeito e a interface com o fantasma*. Rio de Janeiro: Jorge Zahar, 2001.
- BAUMAN, Zygmunt. **Vida líquida**. Rio de Janeiro: Jorge Zahar, 2007.
- BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2018.
- BIONI, B. R. **Xeque-Mate: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. GPOPAI/USP, 2015. Disponível em: <[http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE\\_MATE\\_INTERATIVO.pdf](http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf)>. Acesso em: 16 out. 2019.
- BRASIL. **Código de Defesa do Consumidor**. Lei n. 8.078, de 11 de setembro de 1990. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/l8078.htm](http://www.planalto.gov.br/ccivil_03/leis/l8078.htm)>.
- BRASIL. **Constituição da República Federativa do Brasil**. Promulgada em 05 de outubro de 1988. Disponível em <[http://www.planalto.gov.br/ccivil\\_03/Constituicao/Constituicao.htm](http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm)>.
- BRASIL. **Lei do Cadastro Positivo**. Lei n. 12.965, de 23 de abril de 2014. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm)>.
- BRASIL. **Lei Geral de Proteção de Dados Pessoais**. Lei n. 13.709, de 14 de agosto de 2018. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm)>.
- BRASIL. **Marco Civil da Internet**. Lei n. 12.414, de 9 de junho de 2011. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2011/Lei/L12414.htm](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm)>.
- CANCELIER, Mikhail Vieira de Lorenzi. **Infinito particular: Privacidade no século XXI e a manutenção do direito de estar só**. Florianópolis, 2016.
- CANCELIER, Mikhail Vieira de Lorenzi; CRISTO, Camila Kohn de; MAFRA, Gabriela. **Evasão de informações privadas: proteção à privacidade nos casos de pornografia de vingança**. 2017. Disponível em: <<https://egov.ufsc.br/portal/conteudo/evas%C3%A3o-de-informa%C3%A7%C3%B5es-privadas-prote%C3%A7%C3%A3o-%C3%A0-privacidade-nos-casos-de-pornografia-de-vingan%C3%A7>>. Acesso em: 15 out. 2019.
- CARLEY, Kathleen; PALMQUIST, Michael. **Extracting, Representing and Analyzing Mental Models**. Disponível em: <<http://www.casos.cs.cmu.edu/publications/papers/METHOD08.pdf>>. Acesso em: 08 out. 2019.

CUMBRE IBEROAMERICANA. Declaração de Santa Cruz de La Sierra, de 14 e 15 de novembro de 2003. Disponível em: <<https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf>>.

CUSTERS, Bart. **Click Here to Consent Forever: Expiry Dates for Informed Consent**. VI. 3, 2016. Disponível em: <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3047128](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047128)>. Acesso em: 06 out. 2019.

CUSTERS, Bart; van der HOF, Simone; SCHERMER, Bart Willem; APPLEBY-ARNOLD, Sandra; BROCKDORFF, Noellie. **Informed Consent in Social Media Use: The Gap between User Expectations and EU Personal Data Protection Law**. 2013. Disponível em: <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3047134](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047134)>. Acesso em: 07 out. 2019.

CORRÊA, Ana Carolina Mariano. **Análise do consentimento na Lei de Proteção de Dados Pessoais no Brasil e sua aplicação no mundo jurídico**. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Presbiteriana Mackenzie, São Paulo, 2019.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. (Coord.). **Direito & Internet III: Marco Civil da Internet**. São Paulo: Quartier Latin, 2015.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental**. Revista Espaço Jurídico 12/103. Joaçaba: Unoese, 2011.

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

DUMBILL, Edd. **Getting up to speed whit big data**. In: Big data now: 2012 edition. 2012, p. 3.

EJNISMAN, Marcela Waksman; LACERDA, Maria Eugenia. **O consentimento na internet na nova Lei Geral de Dados Pessoais**. Jota, 2019. Disponível em: <<https://www.jota.info/opiniao-e-analise/columnas/coluna-do-tozzinifreire/lei-geral-de-dados-pessoais-01012019>>. Acesso em 30 out. 2019.

FORTES, Vinícius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet**. Rio de Janeiro: Editora Lumen Juris, 2016.

JORNAL OFICIAL DA UNIÃO EUROPEIA. **Regulamento (UE) 2016/679**. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=DA>>. Acessado em: 22 ago. 2019.

LANCHESTER, John. **Você é o produto**: Mark Zuckerberber e a colonização das redes pelo Facebook. Revista Piauí, 2017. Disponível em: <<https://piaui.folha.uol.com.br/materia/voce-e-o-produto/>>. Acesso em: 18 nov. 2019.

LISBOA, Roberto Senise. **A obrigação de informar**. São Paulo: Almedina, 2012.

LIMA, Caio César Carvalho. **Marco Civil da Internet: Garantia da privacidade e dados pessoais à luz do marco civil da internet**. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

MALHEIRO. Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet: uma análise comparada do Regulamento Geral de Proteção de Dados**



**européu e do Projeto de Lei 5.276/2016.** Trabalho de Conclusão de Curso (Bacharelado em Direito) — Universidade de Brasília, Brasília, 2017.

MARINELLI, Marcelo Romão. **Privacidade e redes sociais virtuais.** Rio de Janeiro: Lumen Juris, 2017.

MCDONALD, A.M.; CRANOR LF. **The cost of reading privacy policies.** *I/S Journal for Law and Policy for the Information Society*. Privacy Year in Review, 2008. Disponível em: <<http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>>. Acesso em: 10 out. 2019.

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

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.** Dissertação (Mestrado) - Faculdade de Direito da Universidade de Brasília. Brasília, 2008.

MINISTÉRIO DA JUSTIÇA, Departamento de Proteção e Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia.** Escola Nacional de defesa do Consumidor, Caderno de Investigações Científicas. Vol 2, 2010. Disponível em: <<https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>>. Acesso em: 22 out. 2019.

MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados no Brasil - Análise.** Disponível em: <<https://baptistaluz.com.br/institucional/lei-geral-de-protecao-de-dados-do-brasil-analise/>>. Acesso em: 28 out. 2019.

OFFICE OF THE ASSISTANT SECRETARY FOR PLANNING AND EVALUATION. **Records, Computers and the Rights of Citizens.** Disponível em: <<https://aspe.hhs.gov/report/records-computers-and-rights-citizens>>. Acesso em: 16 out. 2019.

PONTICELLI, Murilo Meneghel. **O direito fundamental à proteção de dados pessoais e a privacidade.** Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade do Sul de Santa Catarina, Tubarão, 2018.

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. **A proteção de dados pessoais na internet no Brasil: análise de decisões proferidas pelo Superior Tribunal Federal.** Revista Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS, v. 11, n. 2, 2016. Disponível em: <<https://seer.ufrgs.br/ppgdir/article/view/61960/39936>>. Acesso em: 30 out. 2019.

REINALDO FILHO, Demócrito. **Lei de proteção de dados pessoais aproxima o Brasil dos países civilizados.** 2018. Disponível em: <<https://jus.com.br/artigos/67668/lei-de-protecao-de-dados-pessoais-aproxima-o-brasil-dos-paises-civilizados>>. Acesso em: 05 out. 2019.

REINALDO FILHO, Demócrito. **A Diretiva Europeia sobre Proteção de Dados Pessoais - uma Análise de seus Aspectos Gerais.** Disponível em: <[http://www.lex.com.br/doutrina\\_24316822\\_A\\_DIRETIVA\\_EUROPEIA\\_SOBRE\\_PROTECAO\\_DE\\_DADOS\\_PESSOAIS\\_\\_UMA\\_ANALISE\\_DE\\_SEUS\\_ASPECTOS\\_GERAIS.aspx](http://www.lex.com.br/doutrina_24316822_A_DIRETIVA_EUROPEIA_SOBRE_PROTECAO_DE_DADOS_PESSOAIS__UMA_ANALISE_DE_SEUS_ASPECTOS_GERAIS.aspx)>. Acesso em: 30 out. 2019.

RODOTÀ, 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.

RUARO, Regina Linden; RODRIGUES, Daniel Piñeiro; FINGER, Brunize. **O direito à proteção de dados pessoais e a privacidade**. Revista da Faculdade de direito UFPR, Curitiba, PR, v. 53, jun. 2011. Disponível em: <<https://revistas.ufpr.br/direito/article/view/30768/19876>>. Acesso em: 13 out. 2019.

SÁ JUNIOR, Sérgio Ricardo Correia de. **A regulação jurídica da proteção de dados pessoais no Brasil**. Monografia apresentada ao Programa de Pós-Graduação em Direito da Propriedade Intelectual - PUC-Rio, Rio de Janeiro, 2018.

SANSANA, Alexandre Gomes. **Privacidade, consentimento, legítimo interesse e a nova Lei Geral de Proteção de Dados Pessoais**. Trabalho de Conclusão de Curso (Pós-Graduação) - Instituto de Ensino e Pesquisa em Direito Societário, São Paulo, 2018.

SANTOS, Manoel J. Pereira dos. **Responsabilidade Civil na Internet e demais Meios de Comunicação**. 2. ed. São Paulo: Saraiva, 2014.

SANTOS, Orlando Gomes dos. **Contratos**. 26 ed. São Paulo: Forense, 2008.

SCHERMER, Bart Willem; CUSTERS, Bart; van der HOF, Simone. **The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in data Protection**. 2014. Disponível em <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2412418](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418)>. Acesso em: 07 out. 2019.

SERPRO. **Seu consentimento é lei!**. Disponível em: <<https://www.serpro.gov.br/lgpd/cidadao/seu-consentimento-e-lei>>. Acesso em: 31 out. 2019.

SIBILIA, Paula. **O show do Eu: a intimidade como espetáculo**. 2ª Edição. Rio de Janeiro: Contraponto Editora Ltda., 2016.

SILVA, Leticia Brum da; SILVA, Rosane Leal da. **A proteção jurídica de dados pessoais na Internet: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil**. Disponível em: <<http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65>>. Acesso em: 25 out. 2019.

SOARES, Pedro Silveira Campos. **A questão do consentimento na Lei Geral de Proteção de Dados**. Consultor Jurídico, 2019. Disponível em: <<https://www.conjur.com.br/2019-mai-11/pedro-soares-questao-consentimento-lei-protacao-dados>>. Acesso em: 01 nov. 2019.

SOLOVE, Daniel. **Privacy self-management and the consent dilemma**. Harvard Law Review 126. 2013. Disponível em: <[https://harvardlawreview.org/wp-content/uploads/pdfs/vol126\\_solove.pdf](https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf)>. Acesso em: 08 out. 2019.

SOUZA, Carlos Aurélio Mota de. O cidadão, a sociedade, a mídia e a justiça. In: MARTINS FILHO, Ives Gandra; MONTEIRO JUNIOR, Antônio Jorge (coordenadores). **Direito à privacidade**. Ideias e Letras: São Paulo, 2005.

SOUZA, Thiago Pinheiro Vieira de. **A proteção de dados pessoais como direito fundamental e a [in]civildade do uso de cookies**. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Federal de Uberlândia, Minas Gerais, 2018.

**STJ. Debater a Lei Geral de Proteção de Dados é refletir sobre o futuro, afirma ministro Salomão.** Disponível em:

<<http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Debater-a-Lei-Geral-de-Protecao-de-Dados-e-refletir-sobre-o-futuro--afirma-ministro-Salomao.aspx>>. Acesso em: 15 ago. 2019.