

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO  
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS  
FACULDADE DE DIREITO

**O CONSENTIMENTO DO CONSUMIDOR NO MARKETING DIRETO À LUZ DA LEI  
GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

BRUNA LUIZA BARBOSA CRUVINEL

Rio de Janeiro

2020

BRUNA LUIZA BARBOSA CRUVINEL

**O CONSENTIMENTO DO CONSUMIDOR NO MARKETING DIRETO À LUZ DA LEI  
GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor Dr. Carlos Augusto Thomaz.

Rio de Janeiro

2020

## CIP - Catalogação na Publicação

C957c Cruvinel , Bruna Luiza Barbosa  
O consentimento do consumidor no marketing  
direto à luz da Lei Geral de Proteção de Dados  
Pessoais / Bruna Luiza Barbosa Cruvinel . -- Rio de  
Janeiro, 2020.  
58 f.

Orientador: Carlos Thomaz .  
Trabalho de conclusão de curso (graduação) -  
Universidade Federal do Rio de Janeiro, Faculdade  
Nacional de Direito, Bacharel em Direito, 2020.

1. Tutela do consumidor contra o marketing direto  
. 2. A eficácia do consentimento como instrumento  
de viabilização da autonomia informativa. 3. Uso dos  
dados pessoais na economia da informação. I. Thomaz  
, Carlos, orient. II. Título.

BRUNA LUIZA BARBOSA CRUVINEL

**O CONSENTIMENTO DO CONSUMIDOR NO MARKETING DIRETO À LUZ DA LEI  
GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor Dr. Carlos Augusto Thomaz.

Data de aceitação: \_\_\_/\_\_\_/\_\_\_.

Banca Examinadora:

\_\_\_\_\_  
Orientador

\_\_\_\_\_  
Membro da Banca

\_\_\_\_\_  
Membro da Banca

Rio de Janeiro  
2020

## RESUMO

Esta monografia analisa a eficiência do consentimento como instrumento de autodeterminação informacional na esfera do marketing direto à luz da Lei Geral de Proteção de Dados Pessoais. Diante da popularização das tecnologias de informação que levou a uma economia fundamentada na vigilância do consumidor e a exploração de dados pessoais pela área de marketing. O direito à proteção de dados pessoais busca inibir práticas abusivas e invasivas que ameaçam o livre desenvolvimento da personalidade do indivíduo e seu direito à igualdade e à liberdade. E ainda, garantir ao titular o controle dos seus dados pessoais por meio do consentimento. A evolução da tutela do titular dos dados consolidou o protagonismo do indivíduo e do consentimento no exercício do direito à autonomia informativa. Assim, investiga-se o papel do consentimento e sua (in)eficácia na operacionalização da autodeterminação informacional considerando a realidade prática. Por fim, além do consentimento, conclui-se pela necessidade de novos elementos para viabilizar efetivamente o direito à autodeterminação informacional: a privacidade contextual e a intervenção estatal por meio da Autoridade Nacional de Proteção de Dados.

Palavras-chave: Consentimento; Autodeterminação informacional; Marketing Direto; Proteção de Dados Pessoais; Consumidor; Vulnerabilidade.

## **ABSTRACT**

The objective of this paperwork is to understand the limits of consent, the risks and the consequences arising from the processing of personal data as an economic asset by the area of advertising, focusing on direct marketing. The popularization of information technologies led to an economy based on consumer surveillance and the exploitation of personal data. In view of this it's necessary to analyze the role of consent and its effectiveness in the protection of the data holder from abusive and invasive practices that threaten the free development of personality of the individual.

**Keywords:** Consent; Informational Self-determination; Direct Marketing; Protection of Personal Data; Consumer; Vulnerability.

## SUMÁRIO

<b>1. INTRODUÇÃO</b>	<b>7</b>
<b>2. O USO DOS DADOS PESSOAIS DO CONSUMIDOR NO MARKETING DIRETO</b>	<b>10</b>
2.1. Os dados pessoais como ativo financeiro na sociedade da informação	10
2.2. A transformação do marketing na era digital e utilização dos dados pessoais	14
2.3. Técnicas de obtenção e processamento dos dados pessoais	17
<b>3. O DESENVOLVIMENTO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS</b>	<b>23</b>
3.1. Da privacidade ao surgimento e evolução da matéria de proteção de dados pessoais	23
3.2. A evolução geracional da proteção dos dados pessoais e sua estruturação fundamentada no protagonismo do indivíduo	27
3.3. A Lei Geral De Proteção de Dados Pessoais brasileira: objetivo, fundamentos, princípios e bases legais	32
<b>4. O CONSENTIMENTO DO CONSUMIDOR COMO INSTRUMENTO DE AUTODETERMINAÇÃO INFORMACIONAL NO MARKETING DIRETO</b>	<b>41</b>
4.1. O papel do consentimento	41
4.2. A (in)efetividade do consentimento como cerne único da autodeterminação informacional na esfera do marketing (ou nas relações de consumo)	45
4.3. Novos pilares da autodeterminação informacional: privacidade contextual e a autoridade nacional de proteção de dados pessoais	49
<b>5. CONCLUSÃO</b>	<b>53</b>
<b>REFERÊNCIAS</b>	<b>55</b>

## 1.INTRODUÇÃO

Na vida online, o fornecimento de informações pelo usuário para acessar e usar um serviço oferecido é corriqueiro. O compartilhamento de dados pessoais é constante, instantâneo e permanente. Seja de maneira consciente, ao preencher o cadastro de um site. Inconsciente, por meio da localização utilizada pelo aplicativo de celular. Ou, ainda, desconhecida, com a transferência entre os bancos de dados. O fato é: a cada segundo uma quantidade gigantesca de dados é gerada, colhida e analisada por algum banco de dados, de modo que concentrados em um mesmo local e confrontados entre si resultam em uma base de informações detalhada dos titulares.

Dentro dessa dinâmica, a capacidade de formular perfis de consumidores com base na análise combinada de dados pessoais transformou-se em um dos principais ativos do comércio digital e do marketing. Os dados pessoais passaram a ter uma expressiva valorização econômica e profunda influência na dinâmica capitalista consumerista da sociedade mercadológica. Assim, surgiu a necessidade de proteger o titular e regular a coleta, acesso, distribuição e armazenamento dos seus dados pessoais.

No Brasil, a Lei Geral de Proteção de Dados – LGPD (Lei 13.709 de 14 de agosto de 2018) busca regulamentar o tratamento dos dados pessoais e garantir ao cidadão os seus direitos fundamentais, a sua privacidade e o livre desenvolvimento de sua personalidade. A normativa adota como principal base legal o consentimento pelo titular. No entanto, a eficácia do consentimento é questionada quando o controle do usuário sobre seus dados pessoais é limitado ao “eu concordo com a política de privacidade” assinalado ao se registrar em um site.

Diante desse questionamento, nota-se que sem o desenvolvimento de um método que possibilite um processo genuíno de decisão acerca do tratamento de dados, "*o cidadão-consumidor está exposto a uma (hiper)vulnerabilidade que mistifica sua prometida capacidade de controle de dados.*" (BIONI, 2019). Desse modo, a problemática a ser desenvolvida passa por dois pontos: o efeito prático do consentimento na proteção do uso de dados pessoais e como possibilitar uma autodeterminação informacional ao titular.



O objetivo do presente trabalho é compreender a função e o limite do consentimento na proteção de dados na atualidade, o funcionamento e as consequências provenientes do processamento dos dados pessoais como ativo econômico no comércio digital pela área de publicidade e propaganda. Além de pontuar elementos essenciais para assegurar a autonomia do titular-consumidor. Além de esclarecer conceitos relacionados à temática e ampliar o debate para além da esfera jurídica.

Este estudo justifica-se dada a relevância e o crescimento do comércio digital na esfera global<sup>1</sup>, que é baseado na ideia de personalização do anúncio para o indivíduo e na (re)formulação do produto de acordo com o público-alvo, por meio do intercâmbio informacional. Embora possa ser algo positivo, o *e-commerce* estimula a economia de vigilância e o crescimento de práticas econômicas discriminatórias. Portanto, promover a cultura jurídica de proteção de dados pessoais é essencial para tutelar a personalidade e privacidade do consumidor.

A metodologia adotada no trabalho é o critério hipotético-dedutivo, abrangendo também o modelo analítico de pesquisa. Na revisão bibliográfica serão utilizados como base para a pesquisa: livros, artigos científicos, revistas, *guidelines* e outros meios de informação julgados necessários. Na pesquisa documental, serão considerados a legislação nacional e internacional, jurisprudência, pareceres e portarias. Além do mais, casos concretos serão utilizados como exemplo e para uma melhor compreensão do tema. O marco espacial centra-se no ordenamento jurídico brasileiro, mas em razão da profundidade do debate técnico-jurídico presente na

---

<sup>1</sup> Verifica-se que o comércio digital ou *e-commerce* vem crescendo significativamente no Brasil nos últimos anos, com um aumento do número de consumidores ativos – pessoas que compraram ao menos uma vez no ano pela internet – e do faturamento do *e-commerce* brasileiro. LUNARDI, Guilherme. 12 dados que comprovam o crescimento do e-commerce no Brasil. E-Commerce Brasil, 12 jun. 2018. Disponível em: <https://www.ecommercebrasil.com.br/artigos/12-dados-que-comprovam-o-crescimento-do-e-commerce-no-brasil/>. Acesso em: 4 ago. 2020. GAVIOLI, Allan. E-commerce brasileiro fatura R\$ 61,9 bilhões em 2019, crescimento de 16,3% ante 2018. InfoMoney, 20 fev. 2020. Disponível em: <https://www.infomoney.com.br/consumo/e-commerce-brasileiro-fatura-r-619-bilhoes-em-2019-crescimento-de-163-ante-2018/>. Acesso em: 4 ago. 2020. Além disso, o fechamento do comércio físico e o isolamento devido a pandemia atuaram como fortes incentivadores para a ascensão do comércio digital. Mais de 5 milhões de brasileiros realizaram sua primeira compra pela internet no período de abril e junho de 2020. SOPRANA, Paula. Comércio digital ganha 5,7 milhões de consumidores e varejo diz que eles vieram para ficar. Folha de São de Paulo, 22 jul. 2020. Disponível em: <https://www1.folha.uol.com.br/mercado/2020/07/comercio-digital-ganha-57-milhoes-de-consumidores-e-varejo-diz-que-eles-vieram-para-ficar.shtml>. Acesso em: 4 ago. 2020.

Regulação Geral de Proteção de Dados da União Europeia (*General Data Protection Regulation - GDPR*), a normativa é adotada como um referencial jurídico.

Esta monografia está estruturada em três capítulos. O primeiro procura tratar dos dados pessoais na economia digital, especialmente a utilização dos dados pessoais dos consumidores pelo marketing para criação de perfis. Explica-se por que a informação hoje é considerada um ativo econômico. Além de diferenciar o marketing tradicional e o marketing direto, baseado na conectividade entre o mundo on-line e off-line e no tratamento de dados pessoais, com intuito de desenvolver relações e influenciar o cliente. Logo, busca entender como se desenvolvem esses perfis, relacionamentos e a influência na esfera privada do ser humano pelo tratamento de dados pessoais, bem como quais mecanismos utilizados.

O segundo capítulo limita-se a mostrar o processo de construção do direito à proteção de dados pessoais, bem como sua evolução geracional, apresentando uma linha histórica considerando aspectos sociais, econômicos e jurídicos. Aborda a divergência acerca da efetividade e eficácia na proteção de dados pessoais centrada no protagonismo do titular dos dados pessoais, através do consentimento e sua autodeterminação informativa. Apresenta-se, ao fim, em linhas gerais, a Lei Geral de Proteção de Dados Pessoais brasileira, ao decorrer sobre o objetivo do legislador ao promulgá-la, seus fundamentos, princípios e bases legais.

No terceiro capítulo, busca-se analisar o papel do consentimento na proteção de dados pessoais, considerando os seus efeitos práticos e pretende-se provar que o mero consentimento é insuficiente para proteger e concretizar a autodeterminação informativa dos titulares de dados dentro da atividade publicitária instituída pela economia de vigilância. Por fim, apresentar outros elementos que devem ser considerados na efetivação do direito de autodeterminação informacional, como a privacidade contextual e a Autoridade Nacional de Proteção de Dados - ANPD.

## 2. O USO DOS DADOS PESSOAIS DO CONSUMIDOR NO MARKETING DIRETO

### 2.1 O dado pessoal como ativo financeiro dentro do comércio digital na Sociedade da Informação

Em uma análise histórica, nota-se que apesar de a erudição tradicionalmente ser associada à riqueza, o conhecimento só se tornou fonte geradora quando a evolução tecnológica permitiu a manipulação da informação<sup>2</sup>. Antes, os principais propulsores da economia eram a terra, a máquina a vapor, a eletricidade ou, ainda, a mão de obra humana pela oferta de serviços. No entanto, com o desenvolvimento da capacidade computacional, a fonte de produtividade passou a residir na organização de dados, processamento de informações e geração de conhecimento<sup>3</sup>.

A virtualização da informação<sup>4</sup> gerou um aumento das possibilidades de utilização e armazenamento da informação, por conseguinte fez com que esta assumisse o papel de principal elemento estruturante da sociedade<sup>5</sup> e se transformasse no mais novo insumo econômico da sociedade pós-industrial<sup>6</sup>. O tratamento de dados por computadores representou por si só uma mudança quantitativa, pelo crescimento do volume de informações processadas em menos tempo, bem como qualitativa, com o surgimento dos algoritmos e técnicas sofisticadas capazes de auferir resultados mais significativos<sup>7</sup>. Logo, a expressão Sociedade da Informação surge no século XX para identificar o desenvolvimento de novas formas de organização da informação, com o objetivo de extrair cada vez mais conhecimento, capaz de influenciar nas relações humanas.

---

<sup>2</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019; p. 136-137.

<sup>3</sup> CASTELLS, Manuel. A sociedade em rede. 3 ed. São Paulo: Paz e Terra, 2000.

<sup>4</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019; p. 6-9. “(...) os bits desmaterializaram a informação, permitindo a sua introdução em computadores. [...] Tal revolução binária não somente comprimiu tangivelmente o armazenamento da informação, mas, igualmente, permitiu a ela um acesso mais facilitado. Houve, portanto, um progresso quantitativo e qualitativo do processamento informacional. É a conjunção destes dois fatores – aliados e complementados pela criação da internet – que virtualizaram a informação, rompendo com o modelo fordista de produção para instaurar um novo “padrão sócio-técnico-econômico”.”.

<sup>5</sup> Ibidem; p.5.

<sup>6</sup> BARBOSA, Marco Antonio; SANTOS, Marco Aurelio. O direito na sociedade da informação e perspectivas para a sociedade do conhecimento. Direitos Fundamentais e Justiça – ano 8, nº 28, p. 82/99, julho/setembro. 2014.

<sup>7</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019; p. 150-151.

A máxima “saber é poder” passou a ser entoada como um mantra e traduziu de maneira trivial a dinâmica da Economia da Informação. Os dados pessoais dos consumidores como explicita Bruno Bioni<sup>8</sup>, converteram-se em ativos financeiros, principalmente para a área de marketing e publicidade. Identificar os interesses pessoais de um indivíduo, formular perfis de consumidores e até mesmo, calcular a probabilidade de um fato ou evento ocorrer tornou-se primordial para o funcionamento eficiente da economia. Somente conhecendo e compreendendo profundamente os clientes e quais suas demandas, as marcas e empresas terão sucesso em alcançar seu público e tornar eficazes as propagandas, quando estas aparecem na rede social, no e-mail ou na aba do aplicativo para o usuário.

A capacidade de formação de perfis e segmentação de consumidores foi intensificada com a automatização dos bancos de dados, os quais segundo Danilo Doneda “*consistem, basicamente, em conjuntos de informações organizadas segundo uma determinada lógica*”<sup>9</sup>. Esclarece-se que eles podem ser informatizados ou não, como uma agenda telefônica que pode existir no celular ou em um caderninho físico. Entretanto a tutela de proteção de dados pessoais não pode ser igual para os bancos de dados que façam uso dos recursos tecnológicos e para aqueles que não o fazem, visto a potencialidade de tratamento de informações pessoais das bases de dados virtuais<sup>10</sup>. Doneda explana muito bem essa diferença ao explicar a funcionalidade dos bancos de dados informatizados:

*“O banco de dados informatizado, produto da tecnologia aplicada ao tratamento de informações pessoais, possui potencial antes inimaginável: é capaz de armazenar um grande volume de informações, de processá-las rapidamente, agrega-las e combiná-las dos mais diversos modos, em tempo irrisório se comparado com o tratamento manual – que muitas vezes sequer possível seria – funcionando como um elemento catalisador de um novo perfil de utilização da informação”*<sup>11</sup>

---

<sup>8</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019; p.12-13.

<sup>9</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.p.140-141.

<sup>10</sup> Apesar dessa diferenciação entre os bancos de dados informatizados e não informatizados, esclarece-se que a LGPD tutela o tratamento de dados pessoais inclusive quando não automatizado. Nesse sentido MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). *Lei Geral de Proteção de Dados Comentada*. 2ª ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. p. 20: “*questão que merece destaque no art. 1º, por mais que vivencemos a era digital, em que dados pessoais usualmente já nascem, são coletados, utilizados e descartados diretamente por meios digitais, de forma dinâmica, é a aplicabilidade da Lei também ao tratamento de dados em estado físico ou off-line, migrando ou não, posteriormente, para o meio digital ou on-line.*”

<sup>11</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.p.141.

Somando-se o fornecimento consensual pelo próprio usuário ao preencher um cadastro, a colheita automática, por meio dos *cookies*, por exemplo, e os bancos de dados, conclui-se que existe uma enorme quantidade de informações pessoais<sup>12</sup> disponíveis para o comércio e o marketing digital explorarem. Em outros termos, existe uma enorme base virtual de arquivos que podem ser organizados e cruzados de inúmeras maneiras com o objetivo de revelar padrões de consumo e os mais diversos aspectos da personalidade e do comportamento de compra dos consumidores<sup>13</sup>, para benefício e satisfação da atividade mercantil e publicitária.

Os dados pessoais passaram a integrar a operação econômica, de modo que o titular, na qualidade de consumidor, transforma-se em um dos produtos comercializados. Estabelece-se uma exploração econômica do conhecimento obtido por meio do rastreamento e observação do usuário. Por conseguinte, estrutura-se uma economia baseada na vigília permanente do usuário<sup>14</sup> e no compartilhamento de informações pessoais, independente do conhecimento, compreensão e consentimento do titular.

A denominada Economia de Vigilância<sup>15</sup> ou Economia de Informação consolidou a ideia de um modelo econômico fundamentado na flexibilização, especialização, customização e diversificação de produtos. Uma economia de produção flexível permite uma estabilidade comercial e aumento da lucratividade através da oferta de uma menor quantidade de produtos, porém mais especializados, qualificados e passíveis de personalização com o fim de atender um

---

<sup>12</sup> Uma informação pessoal é aquela que está vinculada a um indivíduo, desnecessário que a própria pessoa seja responsável pela sua produção. Nesse sentido Pierre Catala (1983, p.20) esclarece: “*Mesmo que a pessoa em questão não seja a ‘autora’ da informação, no sentido de sua concepção, ela é a titular legítima dos seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade*” (apud DONEDA, p. 139)

<sup>13</sup> MIRAGEM, Bruno. A Lei Geral de Proteção de dados (Lei 13.709/2018) e o Direito do Consumidor. Revista dos Tribunais. Vol.: 1009/2019. Thomson Reuters Brasil. Novembro/2019. p. 1.

<sup>14</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019.p. 48/50

<sup>15</sup> Termo adotado por Bruno Bioni para identificar a economia sustentada pela exploração da informação pessoal. Ele define e caracteriza a Economia de Vigilância como “*a observação permanente do comportamento dos indivíduos que a movimenta, sendo as suas informações pessoais a matéria-prima a ser explorada para a geração de riqueza. [...] Para a operacionalização desse modelo de negócio, há uma complexa rede de atores que transaciona as informações pessoais dos consumidores, agindo cooperativamente para agregar mais e mais dados*”. BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019.p. 49.

nicho de consumidores<sup>16</sup>. Afinal, há uma significativa redução do risco de fracasso se a empresa investe em ofertar aquilo que é desejado.

Logo, o setor privado passa servir-se da técnica de tratamento de dados pessoais para ter uma maior previsibilidade mercadológica, formular perfis e segmentar consumidores, diferenciar produtos, customizar serviços, aprimorar a comunicação publicitária e, em vista disso, diminuir riscos. A colheita de dados como método de gerenciar riscos, contudo, impõe um círculo vicioso de vigilância. A sensação de insegurança é ampliada com o conhecimento acerca da existência de perigos e ameaças, de modo a provocar mais vigilância e coleta de dados pessoais.

Institui-se desse modo um imperativo de vigilância<sup>17</sup>, o qual é explorado economicamente, em especial pelo marketing. O marketing acompanha esse modelo econômico que utiliza ostensivamente da informação. O dado pessoal passa a ter valor comercial, como também vira um insumo econômico para atividade publicitária. O profissional de marketing passa a além de persuadir ao ato da compra, a acompanhar o cliente em todo o processo de consumo. Philip Kotler, Hermawan Kartajaya e Iwan Setiawan descrevem como os dados pessoais permitem conduzir o consumidor tanto no espaço virtual, como no espaço físico:

*“Saber por onde os clientes caminham e em que gastam seu tempo dentro da uma loja permite aprimorar a disposição dos produtos e merchandising visual da loja. Entender qual promoção funciona para cada cliente individual permite ajustar as mensagens de forma compatível e evitar o envio de spams irrelevantes. Ser capaz de saber exatamente onde os clientes estão em qualquer momento permite seduzi-los com ofertas em tempo real. Além disso, os profissionais de marketing podem usar os dados coletados para análise preditiva. Rastrear padrões históricos de transações ajuda a prever o que os clientes comprarão em seguida. Em última análise, fornece a oportunidade de prever necessidades futuras dos clientes e gerir estoques.”<sup>18</sup>*

---

<sup>16</sup> MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. Revista de Direito do Consumidor. vol. 102. ano 24. nov.-dez. 2015; p. 20/23.

<sup>17</sup> SAMARAJIVA, Rohan, 1997, p. 279 Apud, MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. Revista de Direito do Consumidor. vol. 102. ano 24. nov.-dez. 2015; p. 26 “Marketing efetivo para um grande número de consumidores dispersos no espaço requer a habilidade de diferenciar o consumidor em perspectiva e de formar distintas audiências para as mensagens de marketing; para alcançar essas audiências com diferentes mensagens persuasivas sobre bens, serviços e compactos. [...] Produção customizada relaciona-se ao marketing customizado, que, por sua vez, relaciona-se à vigilância do cliente. Esse é o imperativo da vigilância”

<sup>18</sup> KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. Marketing 4.0: Do tradicional ao digital. Rio de Janeiro: Sextante, 2017; p 173

O dado pessoal transformou-se no principal insumo do marketing da Economia de Vigilância. Enquanto o novo modelo de economia flexível, personalizado e diversificado levou a uma transformação do marketing e da publicidade.

## 2.2 A transformação do marketing na era digital e utilização dos dados pessoais

Na estruturação da Economia da Informação, os dados pessoais dos consumidores tornaram-se um instrumento essencial na promoção dos bens de consumo e na geração de valor sobre um produto, serviço ou marca, com o objetivo de criar um relacionamento valioso com os consumidores. As informações geradas sobre os clientes influenciam estrategicamente o desenvolvimento da ciência mercadológica e a mudança da atividade publicitária no mundo digital<sup>19</sup>.

Tradicionalmente, a atividade publicitária é baseada em uma comunicação em massa, com o objetivo de atingir uma coletividade de possíveis consumidores e induzi-los ao ato de comprar. No processo de elaboração da propaganda existe uma segmentação do mercado, segundo critérios geográficos, demográficos, psicográficos, comportamentais e a identificação do seu público-alvo, segundo os perfis de consumidores desenvolvidos. A identificação desses elementos promove um direcionamento na campanha publicitária, de modo a alcançar e se aproximar de pessoas efetivamente interessadas e predispostas à aquisição do bem ofertado<sup>20</sup>.

A canalização da comunicação é denominada publicidade direcionada<sup>21</sup>, que se ramifica em publicidade contextual, segmentada e comportamental. Sob o foco da publicidade online, a publicidade contextual<sup>22</sup> é baseada no conteúdo acessado ou pesquisado na internet, a

---

<sup>19</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019; p.12-15.

<sup>20</sup> KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. Marketing 4.0: Do tradicional ao digital. Rio de Janeiro: Sextante, 2017; p. 63/65.

<sup>21</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019; p.17: “A *publicidade direcionada* é uma prática que procura personalizar, ainda que parcialmente, tal comunicação social, correlacionando-a a um determinado fator que incrementa a possibilidade de êxito da indução ao consumo. Essa prática subdivide-se em *publicidade (direcionada) contextual, segmentada e comportamental – espécies do gênero publicidade direcionada*”.

<sup>22</sup> COMISSÃO EUROPEIA. Article 29 Data Protection Working Party: Opinion 2/2010 on online behavioural advertising. p. 5: “*Contextual advertising is advertising that is selected based on the content currently being viewed*”.

segmentada<sup>23</sup> é desenvolvida segundo características conhecidas dos indivíduos, e por fim, a comportamental<sup>24</sup> é quando a abordagem publicitária é cirurgicamente precisa com relação aos interesses do potencial consumidor. A publicidade comportamental corrobora para uma economia baseada na análise de comportamento do consumidor, visto que o desejo de alinhar ao máximo a propaganda com o perfil do consumidor, acaba por incentivar um rastreamento extensivo do usuário a fim de identificar suas preferências, sua localização, os sites acessados, suas opiniões, e até mesmo emoções.

A publicidade comportamental é amplamente adotada por modelos de negócios como o *zero-price advertisement business model*, nos quais diversos produtos e serviços online são ofertados sem a exigência de uma contraprestação pecuniária dos usuários, por conseguinte apresentando-se como gratuito. Todavia, a ideia da gratuidade é ilusória, pois ainda que inexistente o pagamento em dinheiro, o consumidor paga com a concessão dos seus dados pessoais. Nesse sentido, Bioni é preciso ao explicar a lógica da equação econômica de monetização da “gratuidade”:

*“Trata-se de um modelo de negócio que é financiado ou suportado predominantemente pela publicidade comportamental. Em um primeiro momento, atrai-se o usuário para que ele usufrua um serviço e/ou produto para, em um segundo momento, coletar seus dados pessoais e, então, viabilizar o direcionamento da mensagem publicitária, que é a sua fonte de rentabilização.”*<sup>25</sup>

Percebe-se que há uma alteração de papéis nesse modelo de negócio, no qual o principal cliente não é mais o usuário do serviço, mas sim o anunciante. O usuário vai assumir a condição de um objeto passivo de técnicas de vendas<sup>26</sup>, uma vez que o seu envolvimento perpassa pela mineração dos seus dados pessoais para aperfeiçoamento da mensagem publicitária. Sem poder

---

*by the data subject. In the case of a search engine, content may be derived from the search keywords, the previous search query or the user's IP address if it indicates their likely geographical location.”*

<sup>23</sup> Idem, p. 5: “Advertising selected based on known characteristics of the data subject (age, sex, location, etc.), which the data subject has provided at the sign up or registration stage.”

<sup>24</sup> Idem, p. 4: “Behavioural advertising is advertising that is based on the observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests.”

<sup>25</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019; p. 26

<sup>26</sup> KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. Marketing 4.0: Do tradicional ao digital. Rio de Janeiro: Sextante, 2017; p. 68.



de decisão, o consumidor transforma-se em alvo e passa a ser bombardeado com propagandas, independente do seu consentimento. Estabelece-se um relacionamento vertical entre a empresa e o consumidor, comparável ao existente entre o caçador e a presa<sup>27</sup>, pois o usuário passa a ser observado e vigiado sem seu conhecimento, ao mesmo tempo que é perseguido por anúncios e ações publicitárias.

Ressalta-se, contudo, que o papel do consumidor/usuário no comércio digital não se limita a de um agente passivo que apenas absorve mensagens publicitárias. No desenvolvimento do marketing direto dentro da Economia de Informação o consumidor apropria-se também da posição de agente ativo, uma vez que suas opiniões, impressões, avaliações, reações e preferências são responsáveis por moldar não só campanhas de marketing de uma marca, mas influir também em produtos, serviços e precificação. A participação do consumidor passa a ter valor comercial à medida que as empresas e marcas percebem que podem ampliar o seu lucro se adequarem-se às necessidades e interesses de seus clientes.

É a lógica do *prosumer*, na qual o consumidor não se limita apenas a consumir (*consumption*), mas também elabora o bem de consumo (*production*)<sup>28</sup>. A tecnologia da informação permite que o consumidor assuma simultaneamente a posição de um objeto passivo de técnicas de vendas e de um agente ativo na economia, porque o marketing digital é centrado no indivíduo e baseado em seu comportamento<sup>29</sup> a fim de compreender e satisfazê-lo. Os renomados autores do livro *Marketing 4.0*<sup>30</sup> transmitem bem a ideia ao dizerem que “*As marcas podem usar a análise de big data para entender o comportamento e a preferência de um cliente*

---

<sup>27</sup> KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. *Marketing 4.0: Do tradicional ao digital*. Rio de Janeiro: Sextante, 2017, p. 64

<sup>28</sup> BIONI, Bruno. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Editora Forense. 2019.p.15.

<sup>29</sup> TORRES, Claudio. *A Bíblia do Marketing Digital: tudo que você queria saber sobre marketing e publicidade na Internet e não tinha a quem perguntar*. São Paulo: Novatec Editora, 2009. p. 68

<sup>30</sup> Philip Kotler é professor de marketing da Kellogg School of Management da Northwestern University. Detentor de diversos prêmios e títulos de honra concedidos por várias instituições de ensino ao redor do mundo, é doutor em economia pelo MIT. Considerado pelo *The Wall Street Journal* um dos 10 pensadores mais influentes da área de negócios, Kotler é autor de mais de 50 obras traduzidas para mais de 20 idiomas, incluindo o mundialmente renomado *Administração de marketing*. Hermawan Kartajaya é fundador e CEO da MarkPlus, Inc., a maior empresa de consultoria de marketing da Indonésia. Foi considerado pelo *Chartered Institute of Marketing* um dos “50 gurus que moldaram o futuro do marketing”. Iwan Setiawan é o executivo-chefe de operações da MarkPlus, Inc. e realiza trabalhos de consultoria sobre estruturas e planejamento de marketing.

*individual. Assim, elas podem fornecer aos clientes o que eles desejam, quando desejam e onde desejam*<sup>31</sup>.

Os profissionais de marketing começaram a explorar essa troca de informação e conhecimento acerca do sujeito não só na elaboração das campanhas publicitárias, mas também na construção do processo comunicativo entre a marca e o cliente, com o objetivo de criar uma relação de identificação com o consumidor. Uma compreensão maior a respeito do comportamento, dos desejos, do estilo de vida, das preferências pessoais, dos hábitos de consumo, dos receios e anseios do ser humano se transformou em um importante fator de influência no sucesso e na lucratividade de uma marca ou empresa.

### **2.3 Técnicas de obtenção e processamento dos dados pessoais**

No processo de personalização do marketing digital, os primeiros passos são focados em obter os dados pessoais e compreender as preferências e hábitos de navegação do usuário. Mas como desenvolver perfis tão detalhados e específicos de grupos e indivíduos? A construção de perfis começa com a colheita dos dados pessoais, que na maioria das vezes é fornecido de forma consensual pelo consumidor, mas não verdadeiramente consciente, uma vez que este, na maioria das vezes, tem acesso a informações incompletas. E ainda, o sujeito desconhece os personagens envolvidos na mineração de dados, não compreende as formas de utilização, não sabe se serão compartilhados, além de não entender as políticas de privacidade. Além disso, o processo humano de decisão não é um ato racional perfeito, como o praticado por uma máquina, mas sim influenciado pelas percepções pessoais de privacidade<sup>32</sup>.

---

<sup>31</sup> KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. Marketing 4.0: Do tradicional ao digital. Rio de Janeiro: Sextante, 2017; p. 105

<sup>32</sup> ACQUISTI, Alessandro; GROSSKLAGS, Jens. Economics of Information: Security Privacy and Rationality in Individual Decision Making. IEEE Security & Privacy, Jan/Feb. 2005; p. 24-30 *“The individual decision process with respect to privacy is affected and hampered by multiple factors. Among those, incomplete information, bounded rationality, and systematic psychological deviations from rationality suggest that the assumption of perfect rationality might not adequately capture the nuances of an individual’s privacy-sensitive behavior.”*

Em um processo de decisão rápido sobre o fornecimento dos dados pessoais, vários fatores são considerados pelo titular<sup>33</sup>, desde a confiança no *software* até as possíveis vantagens e desvantagens decorrentes da concessão dos dados pessoais. Fatores estes que contribuem para a normalização do fornecimento de informações pessoais, apesar do desconhecimento do titular acerca do que será feito com as informações concedidas. Não obstante naturalizou-se o ato de informar o nome, data de nascimento, telefone, sexo, endereço, filiação e o número de documentos, como o CPF, ao preencher um cadastro na internet. É normal conceder acesso à sua câmera e galeria do seu dispositivo aos aplicativos de transporte privado ou de navegação por satélite, a sua localização para o software de mensagens instantâneas, chamadas de voz e vídeo ou, ainda, a sua agenda telefônica e registro de chamadas para poder utilizar redes sociais.

Reflexo prático disso é o fato de que na maioria das situações de colheita de dados pessoais há a participação ativa do titular. Uma quantidade gigantesca de dados é coletada a partir de transações comerciais, nas quais além dos dados bancários, são registradas outras inúmeras informações pessoais a título de segurança. Derivados de uma estratégia de marketing, os cartões fidelidade ou programas de pontuação são métodos populares para obtenção de dados sobre o consumidor. Eles permitem uma individualização maior do cliente, possibilitando a empresa classificá-lo segundo seu hábito de compra e, à vista disso, promover tratamentos desiguais em relação aos seus clientes<sup>34</sup>.

Os censos, registros públicos, pesquisas de mercado e estilo também são fontes de dados de consumidores. Inclusive são amplamente utilizados pelo marketing direto para fins de segmentação do consumidor de acordo com um mapeamento demográfico e comportamental. O setor privado utiliza ainda de sorteios e concursos para recolher dados pessoais. Recurso o qual é

---

<sup>33</sup> ACQUISTI, Alessandro; GROSSKLAGS, Jens. Economics of Information: Security Privacy and Rationality in Individual Decision Making. IEEE Security & Privacy, Jan/Feb. 2005; p. 24-30 “*Many factors affect privacy decision making, including personal attitudes, knowledge of risks and protection, trust in other parties, faith in the ability to protect information, and monetary considerations. Our preliminary data show that privacy attitudes and behavior are complex but are also compatible with the explanation that time inconsistencies in discounting could lead to under-protection and over-release of personal information*”.

<sup>34</sup> MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental*. Edição do Kindle. São Paulo: Saraiva, 2014. Paginação incorreta. Posição 1903. “*a partir desses dados de transações comerciais, que são dados comportamentais, a empresa pode avaliar e classificar o consumidor em relação à sua frequência, à última vez que esteve na loja e ao seu valor monetário (recency, frequency and monetary value – RFMV). As consequências dessa classificação podem ser indesejáveis, tais como a possibilidade de exclusão do consumidor de menor capacidade financeira.*”

no mínimo duvidoso, uma vez que o consumidor ao se inscrever pode não perceber que a premiação tem como fim a coleta de dados, bem como não é informado abertamente para quais finalidades estes estão sendo coletados<sup>35</sup>.

Além do fornecimento comissivo pelo usuário, a obtenção dos dados pessoais também acontece sem a participação ativa do titular. Uma das principais ferramentas utilizadas para tal finalidade são os *cookies*. Os *cookies* são associados a um navegador particular, de modo que conseguem registrar o histórico de navegação, códigos e senhas, armazenar as preferências dos usuários, permitindo recuperar uma pequena quantidade de informação quando o visitante regressa ao site usando o mesmo computador e *browser*<sup>36</sup>. A função primordial de um *cookie* simples é armazenar dados no formato de arquivo de texto e, posteriormente, em um novo acesso ao site pelo mesmo computador e navegador, recuperar as informações armazenadas da máquina do cliente<sup>37</sup>.

Existem, ainda, outras categorias de *cookies*. O mais conhecido é o *tracking cookie*, também chamado de *tracker*, que tem a capacidade de acompanhar e compartilhar hábitos de navegação de um usuário. Segundo o Article 29 Working Party<sup>38</sup> na Opinion 2/2010, o *tracker* é o principal instrumento adotado para monitorar as pessoas na internet<sup>39</sup>, porque consegue obter uma expressiva quantidade de informações acerca do usuário, provenientes até mesmo de

---

<sup>35</sup> MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental*. Edição do Kindle. São Paulo: Saraiva, 2014. Paginação incorreta. Posição 1945/1956.

<sup>36</sup> PRATES, Cristina Cantú. Privacidade e Intimidade na Internet: A legalidade dos Cookies e Spam. *Revista FMU Direito*, São Paulo, ano 28, n. 42, p. 29-45, 2014. ISSN: 2316-1515. “Um cookie armazena em seu próprio disco rígido informações sobre as preferências pessoais exclusivamente referentes ao sítio que o enviou e teoricamente serve para tornar a navegação mais confortável e proveitosa. [...] Eles são usados para ligar o consumidor à informação armazenada sobre sua visita na página da internet, tais como preferências, compras e outras ações.”

<sup>37</sup> NOJIRI, Sérgio. O direito à privacidade na era da informática algumas considerações. *Revista Jurídica UNIJUS*, Uberaba-MG, V.8, nº 8, maio/2005; p. 99/106.

<sup>38</sup> O Article 29 Working Party era o órgão consultivo, existente enquanto vigorava a antiga Diretiva Europeia de Proteção de Dados (EC 95/46), e tinha como função principal interpretar o texto da diretiva. O Working Party 29 (WP 29) reunia representantes de todas as autoridades de proteção de dados pessoais dos países-membros da União Europeia. Com a aprovação pela União Europeia do Regulamento Geral de Proteção de Dados 2016/679 – a GDPR – a WP29 foi extinta, e em seu lugar instituiu a European Data Protection Board (EDPB), que tal qual sua antecessora, tem a função de interpretar a nova regulamentação, porém as *guidelines* e *opinions* emitidas pelo órgão antecessor são dotadas de força vinculante.

<sup>39</sup> COMISSÃO EUROPEIA. Article 29 Data Protection Working Party: Opinion 2/2010 on online behavioural advertising; p. 6.

domínios diferentes, a depender das configurações adotadas por cada domínio. Os *tracking cookies* além de armazenar e restaurar, também realizam a função de vigilância.

Conforme explicado pelo Grupo de Trabalho do Artigo 29 na referida orientação, o *tracker* é a principal tecnologia de controle adotada, pois permite a identificação e verificação de todos os passos do usuário no espaço virtual. O documento europeu esclarece ainda a dinâmica de funcionamento dos *trackers*, especificadamente em relação à publicidade online comportamental:

*“Normalmente funciona da seguinte forma: os provedores de rede de publicidade instalam um tracking cookie no computador do titular dos dados, quando o indivíduo acessa um site que contém anúncios que fazem parte da sua rede. O cookie é uma espécie de texto alfanumérico que será armazenado (e depois restaurado) no equipamento do indivíduo por um provedor de rede. No contexto da publicidade comportamental, o cookie permitirá que o fornecedor de rede de publicidade reconheça um antigo visitante, seja por regressar ao site previamente visitado ou qualquer outro que seja parceiro da rede de propagandas. Essas visitas repetidas permitirão que o provedor crie um perfil do visitante que será utilizado para fornecer um conteúdo publicitário personalizado.”<sup>40</sup>*

Somando às técnicas de obtenção de dados pessoais, há também os métodos de processamento. Enquanto os primeiros têm o objetivo de reunir o máximo de dados, estes têm a finalidade de refinar e aperfeiçoá-los. O dado somente transforma-se em uma informação depois que passa por avaliação crítica, que lhe adiciona valor pela combinação de conhecimento<sup>41</sup>. É o dado valorado que permitirá a segmentação e criação de nichos de consumidores, classificá-los segundo a frequência de compra e valor para empresa, flexibilizar, especializar e diversificar a produção, adequar e customizar serviços e, por conseguinte, aprimorar o marketing e reduzir riscos.

---

<sup>40</sup> COMISSÃO EUROPEIA. Article 29 Data Protection Working Party: Opinion 2/2010 on online behavioural advertising; p. 6. *“It usually works as follows: typically, the ad network provider places a tracking cookie on the data subject's terminal equipment, when he/she first accesses a website serving an ad of its network. The cookie is a short alphanumeric text which is stored (and later retrieved) on the data subject's terminal equipment by a network provider. In the context of behavioural advertising, the cookie will enable the ad network provider to recognise a former visitor who returns to that web site or visits any other website that is a partner of the advertising network. Such repeated visits will enable the ad network provider to build a profile of the visitor which will be used to deliver personalised advertising.”*, tradução livre.

<sup>41</sup> O dado é fato bruto, sem qualquer análise valorativa ou adição de conhecimento, enquanto a informação deriva da valoração do dado em seu estado primitivo.

As distintas técnicas de processamento, tais quais *data mining*, *Online Analytical Processing* (OLAP), *profiling*, dentre outras, buscam satisfazer objetivos diferentes ao fornecerem resultados que abarcam os mais diversos pontos estratégicos passíveis de serem trabalhados pelo marketing. Logo, como regra geral, as técnicas de processamento são usadas em conjunto, de modo a completarem uma a outra.

A técnica de *data mining* ou mineração de dados consiste na utilização de *softwares* capazes de combinar e cruzar de diversas maneiras dados brutos, de modo a produzir novas informações e conhecimentos estatísticos. A mineração de dados fornece padrões de comportamento e levantamentos estatísticos empregados para diferenciar grupos de consumidores<sup>42</sup>. Enquanto o *Online Analytical Processing* (OLAP)<sup>43</sup>, um aprimoramento da técnica de *data mining*, utiliza de bases de dados para prover prognósticos de mercado e prever tendências.

O *profiling* é o método de formulação de perfis, no qual os dados pessoais são organizados com o propósito alcançar um retrato completo da personalidade de uma pessoa. Através do *profiling* obtém-se uma imagem detalhada e confiável das preferências, hábitos, opiniões, estilo de vida e interesses do consumidor. A autoridade europeia ao discorrer sobre a construção de perfis identifica dois principais: perfil preditivo ou perfil explícito<sup>44</sup>. O perfil explícito é formulado com base nos dados pessoais fornecidos ativamente pelos próprios titulares a um serviço da internet. Enquanto o perfil preditivo advém da observação do comportamento individual e coletivo do usuário ao longo do tempo, particularmente por meio do monitoramento dos sites visitados e anúncios visualizados.

---

<sup>42</sup> *Ibidem*, posição 2112; “O objetivo da mineração de dados é a extração de inteligência significativa e de padrões de conhecimento, partindo de um banco de dados, por meio de sua ordenação e transformação. Geralmente, a mineração de dados tem como finalidade gerar regras para a classificação de pessoas ou objetos.”

<sup>43</sup> *Ibidem*, posição 2133; “Com essa técnica, as empresas são capazes de realizar uma análise de dados de forma dinâmica e multidimensional, obtendo novas relações entre os dados e diferentes variáveis.”

<sup>44</sup> COMISSÃO EUROPEIA. Article 29 Data Protection Working Party: Opinion 2/2010 on online behavioural advertising; p. 7, “There are two main approaches to building user profiles: i) Predictive profiles are established by inference from observing individual and collective user behaviour over time, particularly by monitoring visited pages and ads viewed or clicked on. ii) Explicit profiles are created from personal data that data subjects themselves provide to a web service, such as by registering.”

Por fim, há o *scoring*, um sistema de pontos para identificar os clientes com maior valor para empresa, para que esses sejam alvos de promoções e estratégias de fidelização. O marketing faz uso deste sistema avaliativo para identificar bons e maus consumidores. Àqueles considerados bons serão ofertadas mais vantagens econômicas a fim de desenvolver um relacionamento longo. Aos identificados como maus consumidores, no entanto, pouco ou nenhum benefício, como promoções e descontos, serão lhes direcionados. O *scoring* também é muito usado para avaliação de crédito. No Brasil, há o caso do Serasa Score<sup>45</sup> que serve para demonstrar a probabilidade de um indivíduo pagar contas em dia no período futuro de doze meses. A pontuação creditícia pode influir na concessão de financiamentos, empréstimos, cartões, na fixação de taxa de juros, na realização de negócios<sup>46</sup>.

O problema reside no fato que os meios de coleta e métodos de processamento de dados pessoais utilizados na economia de vigilância para estruturação de uma inteligência de marketing personalizada ao cliente, ameaçam à esfera privada e o desenvolvimento da personalidade do indivíduo. Práticas de marketing sustentadas por uma vigilância do cliente, análises estatísticas e probabilidades, em conjunto com métodos de construção de perfil e classificação de consumidores podem ser invasivas e discriminatórias, tendo como efeito influir no âmbito íntimo das relações humanas e reduzir o acesso a oportunidades e benefícios pelo titular, na qualidade de consumidor, trabalhador ou cidadão. Impondo se, assim, a necessidade de tutela do consumidor contra os riscos que o tratamento indevido de dados pessoais acarreta.

---

<sup>45</sup> Cabe pontuar que apesar de a LGPD prever no art. 7º, X, a hipótese legal de tratamento de dados pessoais para a proteção de crédito, existe no ordenamento jurídico brasileiro a Lei do Cadastro Positivo (Lei 12.414 de 9 de junho de 2011) a qual regula de forma específica os sistemas de avaliação e análise sobre crédito no Brasil. Ademais, tem o Código de Proteção e Defesa do Consumidor que também legisla acerca do tema.

<sup>46</sup> A finalidade e o funcionamento do Serasa Score é explicado no site do serasa, bem como critérios para aumentar e reduzir a pontuação. As informações podem ser encontradas em <<https://ajuda.serasa.com.br/hc/pt-br/articles/360030706011-Como-funciona-o-Serasa-Score->>> e <<https://www.serasa.com.br/ensina/aumentar-score/score-de-credito/>>.

### 3. O DESENVOLVIMENTO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

#### 3.1 Da privacidade ao surgimento e evolução da matéria de proteção de dados pessoais

No final do século XIX, Samuel Warren<sup>47</sup> e Louis Brandeis publicaram na Harvard Law Review o famoso artigo *The Right to Privacy*<sup>48</sup>, dando início à construção da disciplina moderna de direito à privacidade, na qual a fundamentação ao direito de privacidade deixa de perpassar pela ideia de propriedade, mas é embasada na tutela da personalidade<sup>49</sup>. À época, fotografias de famosos, políticos ou pessoas consideradas poderosas em situações íntimas espalhavam-se por jornais e revistas<sup>50</sup>. Essa exposição da intimidade representava uma ameaça à privacidade, bem como à personalidade, nome e honra das celebridades expostas.

Os autores defendiam o direito à privacidade como uma proteção à inviolabilidade da personalidade diante dos riscos que os avanços tecnológicos geravam à vida íntima e doméstica do cidadão. Logo, ao definirem no artigo os limites para proteção à privacidade, descrevem um direito fortemente individualista e negativo, com a defesa da não interferência do Estado e baseado no direito a ser deixado só (*right to be let alone*) formulado pelo Juiz Cooley em *Treatise of the law of torts* em 1888.<sup>51</sup>

No século XX, todavia, a sociedade mundial passa por profundas transformações socioeconômicas e políticas acompanhadas de uma revolução da tecnologia da informação. Em um primeiro momento, o tratamento de dados pessoais vai ser uma tecnologia restrita ao Estado,

---

<sup>47</sup> A presença constante de sua família nos noticiários, muita das vezes na forma de notícias jocosas, devido a envolvimento político do seu sogro, Senador Thomas Franklin Bayard, e as inúmeras publicações na imprensa local descrevendo ao mínimos detalhes o casamento de sua filha foram as principais motivações para Warren escrever e publicar o referido artigo com seu colega de curso de direito de Harvard e sócio, Brandeis. DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados*. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 123.

<sup>48</sup> O artigo encontra-se disponível em <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>

<sup>49</sup> DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados*. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 124.

<sup>50</sup> Danilo Doneda explica que o direito à privacidade no início é associado a burguesia, uma vez que os primeiros casos judiciais são de celebridades, como o caso do Príncipe Albert e Rainha Vitória (Inglaterra, 1848), da atriz Elisa Rachel Félix (França, 1858), do tenor Erico Caruso (Itália, 1953) e de Benito Mussolini e sua amante Clara Petacci (Itália, 1953). DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados*. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. pp. 30-32.

<sup>51</sup> MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental*. Edição do Kindle. São Paulo: Saraiva, 2014. Paginação Incorreta. Posição 476-496.



que a utilizará com base na justificativa de uma maior eficiência da administração pública e como instrumento de controle social dos seus cidadãos. Ao decorrer do tempo, o barateamento do ato de coleta, armazenamento, processamento e o surgimento de novas maneiras de utilização dos dados pessoais no âmbito econômico, vai viabilizar a utilização dessa tecnologia da informação na esfera privada.

À medida em que ocorre o desenvolvimento técnico da informática, aumenta-se a utilidade e importância em controlar e deter informações pessoais do cidadão, pois significa uma maior potencialidade de influenciar as estruturas de poder e manipular a sociedade.<sup>52</sup> Logo, o risco à privacidade não é mais somente das celebridades ou poderosos, mas torna-se real também para a população como um todo<sup>53</sup>.

Abandona-se a ideia de privacidade<sup>54</sup> como um direito negativo e individual. O direito à privacidade assume um caráter positivo, passa a ser reconhecido internacionalmente como um direito fundamental e pressuposto de uma sociedade democrática moderna<sup>55</sup>. O conceito de privacidade começa a ser associado ao controle do indivíduo sobre suas informações, ao passo que os avanços da tecnologia possibilitam o tratamento informatizado de dados pessoais, em detrimento da ideia de privacidade como o direito a ser deixado só<sup>56</sup>.

Nesse sentido, Alan Westin (1970, p. 7)<sup>57</sup> definiu privacidade como a *“reivindicação de indivíduos, grupos ou instituições para determinar, quando como e em que extensão, informações sobre si próprios devem ser comunicadas a outros”*. Noção de privacidade que foi

---

<sup>52</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. pp. 34-35.

<sup>53</sup> Ibidem, p. 33

<sup>54</sup> Danilo Doneda explica que a concepção do conceito de privacidade ou mesmo de vida íntima e intimidade é moldado segundo fatores sociais, culturais, políticos e econômicos de cada contexto histórico, de modo a privacidade é condicionada pela tecnologia existente em cada época. Ibidem, p. 69.

<sup>55</sup> FONTENELLE NETO, José Edilson Cunha. O direito à proteção de dados pessoais (informatizados) enquanto direito fundamental autônomo. 2019. Dissertação (Mestrado em Ciência Jurídica) – Universidade do Vale do Itajaí, Santa Catarina, 2019. p. 109: *“A violação de Dados pessoais (mesmo aqueles que não individualizem uma pessoa em particular) pode ser um instrumento apto a viciar o processo democrático legítimo, motivo pelo qual, por vezes, a violação do direito à proteção de dados redundará, também, na violação do direito difuso à democracia substancial”*

<sup>56</sup> MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental. Edição do Kindle. São Paulo: Saraiva, 2014. Paginação Incorreta. Posição 507.

<sup>57</sup> Apud. BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019; p. 115. *“the claim of individuals, groups, or institutions to determine for themselves when, how, and what extent information about them is communicated to others”*

reforçada por Stefano Rodotà (1996, p. 122)<sup>58</sup> ao estabelecer o direito à privacidade como “o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada”.

Diante da popularização da tecnologia de tratamento de dados pessoais em uma esfera governamental e privada, a tutela da privacidade é essencial como forma de proteção do próprio indivíduo, pois é responsável por alimentar a individualidade e autonomia do ser humano, no exercício da sua cidadania, dos seus direitos políticos e de liberdade de maneira ampla. Ademais, proteger a privacidade significa garantir ao indivíduo um ambiente privado no qual consiga desenvolver livremente a sua personalidade sem influências externas ou qualquer forma de controle social<sup>59</sup>.

Deve-se compreender que os dados pessoais retratam a própria personalidade do indivíduo e é por meio deles que o ser humano apresenta suas mais diversas características a outrem, bem como seus posicionamentos políticos, sua religião, sua cultura àqueles que não o conhecem. O tratamento desses dados pessoais compartilhados permite a construção de perfis os quais podem ser adotados para rotular, agrupar e segregar indivíduos, ocasionando a adoção de práticas discriminatórias. Além disso, a coleta, armazenamento, organização, cruzamento e compartilhamento de dados, resulta na obtenção de novas informações acerca do sujeito que influenciam no processo de tomada de decisões de governos e empresas e, por conseguinte, interferem na vida de toda a sociedade.

O processamento indevido dos dados pessoais representa uma ameaça ao livre desenvolvimento da personalidade das pessoas, bem como impacta substancialmente nas liberdades individuais e na igualdade entre os cidadãos. Manifesta-se claramente, portanto, a necessidade de amparar os dados pessoais juridicamente para proteger a personalidade, a liberdade e igualdade do titular contra os riscos sociais, econômicos e políticos que o

---

<sup>58</sup> Apud DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 132

<sup>59</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 129

processamento indevido gera. Assim, o direito à privacidade passa a se transformar para o surgimento do direito à proteção de dados pessoais.

Trata-se agora de uma privacidade informacional baseada no controle do cidadão sobre o seu fluxo de informações, de modo a permitir que ele defina quem e a quais informações sobre si terá acesso, com o objetivo de impedir a utilização dos dados pessoais sem o conhecimento e participação do titular<sup>60</sup>. Surge aqui o conceito da intitulada autodeterminação informativa como o poder do cidadão para administrar os seus dados pessoais, instituindo limites para o uso dos mesmos no tratamento automatizado<sup>61</sup> e reflexamente definindo o consentimento como uma das principais hipóteses legais para tutela dos dados pessoais<sup>62</sup>.

O direito à proteção de dados pessoais nasce, portanto, para preservar a pessoa humana e sua esfera privada de forma a garantir o livre desenvolvimento da personalidade. O intuito é impedir o tratamento indevido dos dados pessoais, bem como a adoção de práticas econômicas segregacionistas ou que afetem as oportunidades sociais de cada indivíduo. Laura Mendes destaca que o objeto tutelado na proteção de dados pessoais é o sujeito e sua personalidade, não o dado em si:

*“A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados per se, mas a pessoa que é titular desses dados”*<sup>63</sup>

A proteção de dados pessoais estabelece-se, portanto, não mais somente como um instrumento na proteção da privacidade, mas sim como um novo direito fundamental da

---

<sup>60</sup> MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental. Edição do Kindle. São Paulo: Saraiva, 2014. Paginação Incorreta. Posição 547

<sup>61</sup> A expressão autodeterminação informativa foi cunhada na decisão do Tribunal Constitucional Alemão no julgamento da Lei do Censo para indicar o controle que titular deve ter sobre os seus dados pessoais e acerca de como suas informações pessoais são utilizadas. No entanto a ideia da autonomia informacional já existia na doutrina estadunidense através de Alan Westin. DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 168.

<sup>62</sup> MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental. Edição do Kindle. São Paulo: Saraiva, 2014. Paginação Incorreta. Posição 776: *“O exercício dessa liberdade de controle de dados pessoais baseia-se no consentimento do titular, que possibilita à pessoa, em tese, determinar o nível de proteção dos dados a ela referentes”*

<sup>63</sup> Ibidem, Paginação Incorreta. Posição 558

personalidade. Isso porque, os dados pessoais representam como o titular apresenta-se e é visto pelo mundo digital. A síntese dos dados pessoais resulta na personalidade do usuário.

Logo, a proteção dos dados pessoais ultrapassa a ideia de proteção à privacidade. Trata-se de uma nova variante do direito da personalidade. A tutela não se limita a somente resguardar a intimidade, sem embargo se propõe igualmente a garantir o desenvolvimento da pessoa humana e da sua personalidade. Assegurar a proteção de dados significa abarcar toda e qualquer atividade relacionada ao tratamento de dados capaz de influenciar a vida das pessoas.

### **3.2 A evolução geracional da proteção dos dados pessoais e sua estruturação fundamentada no protagonismo do indivíduo**

Cumprir destacar que esta monografia não tem como objetivo realizar uma profunda análise histórica do direito a proteção de dados pessoais ou um estudo comparado, mas apenas pretende, neste momento, apresentar de maneira rápida o seu processo evolutivo devido os avanços tecnológicos da vida contemporânea. Entender essa evolução é importante para compreender os princípios e as bases legais que fundamentam e regulam a proteção dos titulares e o tratamento dos dados pessoais em uma esfera mundial, visto a transnacionalidade<sup>64</sup> do tema, e que influenciaram o ordenamento jurídico brasileiro na promulgação da LGPD.

A matéria de proteção de dados pessoais no seu processo de construção atravessa quatro fases geracionais. As quatro gerações são diretamente influenciadas pela capacidade técnica existente à época e pelos riscos e medos os quais ela gera, bem como pela ideia de privacidade e personalidade adotada pelo direito.

Prova disso é que as primeiras leis refletem o desconhecimento e o medo acerca das tecnologias da informação, suas consequências e possíveis ameaças à liberdade do cidadão. A

---

<sup>64</sup> A transnacionalidade aqui deve ser percebida como uma consequência da globalização e conectividade proporcionada pela tecnologia da informação, uma vez que as fronteiras geográficas são transpostas no ambiente virtual. O tratamento de dados pessoais é realizado em escala global, empresas dos mais diversos países processam informações pessoais de indivíduos espalhados pelo mundo, portanto, independentemente do local onde encontra-se a sede da empresa ou o titular dos dados é importante uma regulamentação mínima na utilização dos dados pessoais e uma tutela jurídica da pessoa.

primeira fase geracional é voltada para o uso dos dados pessoais pelo Estado. Nela busca-se regulamentar os bancos de dados, instituindo a necessidade de autorização estatal para a criação e posteriormente de fiscalização<sup>65</sup>. Neste primeiro momento, o foco é a regulamentação das bases de dados, não há uma preocupação com a privacidade em si, nem com a promoção de qualquer tipo de participação do cidadão no processo.

A popularização do uso da tecnologia da informação na esfera privada, conseqüentemente o aumento do número de bancos de dados existentes e a difusão da atividade de processamento de dados, provoca uma alteração do foco regulatório. A segunda geração não mais tenta controlar a tecnologia, autorizando e fiscalizando o funcionamento de bancos de dados através de mecanismos estatais, mas atribui ao cidadão a responsabilidade de tutelar os próprios dados<sup>66</sup>. As novas normas advêm da insatisfação da população com uso indevido de seus dados pessoais por terceiros, portanto, elaboram uma estrutura na qual cabe ao titular, através do consentimento, controlar a sua utilização e protegê-los.

No entanto, à medida que as informações pessoais começaram a ser utilizadas de maneira intensa pelo Estado e entes particulares para viabilizar o seu funcionamento, a negativa na concessão dos dados pessoais pelo indivíduo passou a implicar a sua exclusão social. Assim, a segunda geração vai iniciar o debate acerca de qual a real eficácia do consentimento como instrumento de proteção dos dados pessoais e da liberdade individual de escolha, quando a recusa no fornecimento ocasiona prejuízos sociais à pessoa. Ou, ainda, quando o fornecimento dos dados sociais é atrelado à promoção de benefícios econômicos e facilidades no mercado de consumo<sup>67</sup>.

---

<sup>65</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 176. No mesmo sentido BIONI, Bruno. Proteção de dados pessoais.... p. 114: “*Em suma, o que marca a primeira geração de proteção dos dados pessoais é o seu foco na esfera governamental, bem como na premissa em se estabelecer norma rígidas que domassem o uso da tecnologia.*”

<sup>66</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019; p. 115: “*A segunda geração de leis transfere para o próprio titular dos dados a responsabilidade de protegê-los. Se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais.*”

<sup>67</sup> MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental. Edição do Kindle. São Paulo: Saraiva, 2014. Paginação Incorreta. Posição 683-694: “*Por um lado no âmbito do Estado Social, é muito difícil assegurar-se a liberdade informacional sem comprometer as funções dessa complexa burocracia que necessita de dados dos cidadãos para planificar. Por outro, também na*

Considerando a controvérsia suscitada na geração anterior, a terceira geração tem a intenção de garantir um real controle do cidadão sobre suas informações e uma autonomia no processo de escolha. Busca-se agora uma autodeterminação informativa do titular como instrumento de garantia de sua liberdade. O protagonismo do indivíduo na defesa dos seus dados pessoais é ainda maior, estendendo a participação do titular para todas as etapas do tratamento, desde a coleta, passando pelo armazenamento e até a transmissão, incluindo garantias como o dever de informação.

A decisão do Tribunal Constitucional alemão, no julgamento da Lei do Censo<sup>68</sup> alemã em 1983, marcou a terceira fase geracional, além de ser um referencial histórico e jurídico na tutela dos dados pessoais. A corte declarou a inconstitucionalidade das cláusulas da referida lei que permitiam o cruzamento e o compartilhamento entre os órgãos da administração pública dos dados coletados para outros fins que não fossem o de recenseamento. Todavia, a importância do julgamento reside no reconhecimento da proteção de dados pessoais como um direito de personalidade autônomo<sup>69</sup> e na construção do direito à autodeterminação informativa como um direito fundamental do qual não se pode dispor<sup>70</sup>, que ultrapassa a ideia de consentimento. Ademais, destaca os limites do consentimento e a essencialidade de vinculação ao princípio da finalidade na coleta de dados.

---

*relação entre privados é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca de suas informações pessoais.*

<sup>68</sup> A referida lei determinava a coleta por pesquisadores de uma série de dados pessoais com objetivo de realizar um levantamento estatístico acerca do crescimento populacional, das atividades econômicas realizadas no país e da distribuição espacial e geográfica da população. Cada cidadão deveria responder a um questionário, que depois seria submetido ao tratamento informatizado. Além disso, permitia a possibilidade de contrastar as respostas com registros públicos prévios para eventuais correções, o compartilhamento dos dados coletados, de maneira anônima, entre a administração pública alemã, além da existência de multa aos que se negassem a responder, bem como incentivos para que as pessoas denunciassem aqueles que se negaram.

<sup>69</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019; p. 101.

<sup>70</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 169. “*Concebido como um direito fundamental, na esteira do direito geral de personalidade, o direito à autodeterminação informativa proporciona ao indivíduo o controle sobre suas informações[...] “Os direitos fundamentais não são concedidos ao cidadão para que deles disponha livremente, porém na sua condição de membro da comunidade e também no interesse público”.*

O Tribunal Constitucional alemão admite que a capacidade técnica empregada no processamento de dados é capaz de transformar qualquer dado pessoal em um dado sensível, gerar perfis detalhados sobre os quais o cidadão não tem controle e, por conseguinte, impor novos riscos ao livre desenvolvimento da personalidade, à liberdade e à igualdade. A decisão afirma, portanto, que informar a finalidade para qual se destina a colheita dos dados e limitá-la a este fim específico, independente do consentimento, é necessário para não reduzir o indivíduo a uma mera fonte de informação a ser explorada<sup>71</sup>.

Compreende-se do julgamento que a ampliação do propósito inicial, com base no argumento do consentimento, gera uma distorção da ideia da autodeterminação informativa, corrompendo a lógica da proteção de dados pessoais baseada no controle do titular sobre seus dados e escolhas individuais.

*“A conclusão que se extrai da releitura do julgado é de que o consentimento poderia servir às avessas para a desproteção dos dados pessoais, na medida em que tornaria ilimitada a coleta e o processamento dos dados pessoais, tornando a pessoa, intermediada por seus dados, a um objeto a ser ilimitadamente explorado.”<sup>72</sup>*

Apesar das ressalvas sobre o consentimento, as leis da terceira geração aprofundaram ainda mais o protagonismo do indivíduo na tutela dos dados pessoais, com a defesa da autodeterminação informativa. Entretanto, a proteção dos dados baseada na escolha individual, no controle do cidadão sobre suas informações e participação no procedimento de mineração de dados mostrou-se inviável, porque poucas pessoas estão dispostas a arcar com os custos, sociais e econômicos<sup>73</sup>, junto às consequências desvantajosas de exercer esta tutela<sup>74</sup>. Logo, a observância

---

<sup>71</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019; p. 105: *“O que se extrai do julgado não é só a construção do princípio da especificação dos propósitos que orienta e limita a coleta e utilização dos dados pessoais (finalidade estatística), mas, sobretudo, a sua prevalência em um contexto no qual o consentimento dos titulares de dados pessoais não teve um papel de protagonismo. Caso contrário, a pessoa poderia ser transformada em m “objeto de informação” decorrente da sua relação de assimetria de poder”*

<sup>72</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019; p. 107.

<sup>73</sup> Em pesquisa realizada nos Estados Unidos pela Universidade de Carnegie Mellon, afirmou-se existir uma divergência entre o comportamento real das pessoas e aquele necessário para proteção da privacidade. Apesar dos inúmeros estudos indicarem que a população estadunidense está mais preocupada com a privacidade, as pesquisas também demonstraram que as pessoas estão mais que dispostas a ceder seus dados pessoais em troca de pequenos benefícios e recompensas. Além de serem pouco propensas a adotarem tecnologias de proteção de dados. ACQUISTI, Alessandro; GROSSKLAGS, Jens. Economics of Information: Security Privacy and Rationality in Individual Decision Making. IEEE Security & Privacy, Jan/Feb. 2005; p. 24-30.

do dever de informação, obrigatoriedade de respeitar o princípio da finalidade e a mera primordialidade do consentimento não são suficientes para salvaguardar o cidadão contra o tratamento indevido dos seus dados pessoais.

Por fim, a quarta e atual geração de leis tenta solucionar os problemas relacionados ao consentimento e a autodeterminação informativa ao compreender a desigualdade de poder existente entre o titular dos dados e os organismos que tratam seus dados. Na tentativa de evitar a desvirtuação do consentimento, surge o princípio da limitação dos propósitos. De acordo com o princípio, a finalidade informada para justificar a coleta ou fornecimento de dados pessoais vincula o tratamento ao propósito especificado, assim na eventualidade de um uso diverso ao autorizado é necessário um novo consentimento. Logo, se há a persecução de diversos propósitos com objetivos finais diferentes, o titular de dados deve consentir expressamente para cada um deles. O consentimento não pode ser único, deve ser granular e específico a cada fim<sup>75</sup>.

O objetivo da limitação dos propósitos é impedir a ampliação do consentimento, ao ponto de legitimar uma utilização secundária do dado coletado, sem a participação e o conhecimento do titular. No entanto, em confronto com a realidade, algumas críticas surgiram em relação ao princípio da limitação dos propósitos. A primeira é que o requerimento repetitivo e constante do consentimento levaria a uma exaustão do titular, de modo que ele não mais se daria ao trabalho de se informar e analisar o porquê e para que fim seus dados estão sendo coletados, apenas consentiria de forma automática – o que foi chamado de “fadiga do consentimento”. Outro ponto criticado é que a vinculação restritiva do consentimento às finalidades explicitamente especificadas no momento em que foi concedido, provocaria um bloqueio no fluxo de informações e atrapalharia a inovação e o desenvolvimento da tecnologia de informação.

---

<sup>74</sup> MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental. Edição do Kindle. São Paulo: Saraiva, 2014. Paginação incorreta. Posição 716: “*o ideal participativo dos cidadãos no controle das informações pessoais, consubstanciado na ideia de autodeterminação informativa, provou-se não ser factível no mundo real. Isso porque, semelhante ao que ocorreu com a segunda geração das normas de proteção de dados pessoais, os cidadãos não estavam dispostos a arcar com os altos custos monetários e sociais de exercer o seu direito e, por consequência, ser privado do acesso a bens e serviços ou a benefícios*”.

<sup>75</sup> Nesse sentido Guidelines 05/2020 on consent under Regulation 2016/679 “*If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom.[...] When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose.*”



Ademais, devido a vulnerabilidade do titular dos dados, passou-se a defender a necessidade de uma tutela coletiva jurídica mínima dos dados pessoais, uma vez que a proteção de dados pessoais não pode ser limitada ou fundamentada apenas pela decisão individual<sup>76</sup>. Assim, são instituídas autoridades independentes para fiscalizar o cumprimento das leis, são impostas proibições ao tratamento de dados pessoais considerados sensíveis e além da existência de uma lei geral, são criadas normas setoriais para regulamentar setores específicos.

A adoção de proteção coletiva, contudo, não afastou o protagonismo do indivíduo na defesa dos seus dados. Ao contrário, a evolução geracional confirma a construção do direito à proteção de dados centrada na promoção da autonomia informativa e estruturada ao redor da ideia do consentimento como mecanismo de controle do indivíduo. Verifica-se isso na Diretiva Europeia de Proteção de Dados (EC 95/46)<sup>77</sup>, que estabeleceu princípios, distinguiu dados pessoais, sensíveis e anônimos, apresentou conceitos, definiu um escopo de aplicação amplo, criou a autoridade de proteção de dados da União Europeia e abordou a transferência internacional de dados, mas ainda tinha em sua medula, como vetor principal, a participação do indivíduo na tutela dos seus dados.

O protagonismo do indivíduo permaneceu ainda no novo Regulamento Geral de Proteção de Dados 2016/679, a *General Data Protection Regulation* (GDPR), aprovado pela União Europeia em 2016. A normativa que entrou em vigor em 2018, decorre de uma atualização da Diretiva Europeia de Proteção de Dados (EC 95/46) e tornou-se referência para as novas normativas com relação a proteção de dados. Inclusive sendo uma das principais influências na formulação e aprovação da lei brasileira de proteção de dados.

### **3.3 A Lei Geral de Proteção de Dados Pessoais brasileira: objetivo, fundamentos, princípios e bases legais**

---

<sup>76</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 179.

<sup>77</sup> MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental. Edição do Kindle. São Paulo: Saraiva, 2014. Paginação Incorreta. Posição 738.

No Brasil, a Lei 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais – LGPD, aprovada em agosto de 2018, é a primeira lei brasileira a regulamentar de forma específica o tratamento de dados pessoais<sup>78</sup>. Anteriormente, a regulamentação sobre a matéria era de forma esparsa, com base na Constituição, no Código Civil, no Código de Defesa do Consumidor e no Marco Civil da Internet, em razão da ausência de uma cultura brasileira de defesa da privacidade. A normativa além do objetivo primário de regulamentação, surge também para gerar uma mudança cultural na proteção de dados no Brasil e, principalmente, fomentar o debate sobre o tema segundo uma perspectiva econômica.

Ao mesmo tempo que há um esforço do legislador em formular normas que incentivem o intercâmbio de dados entre os mais diversos setores produtivos de maneira segura, existe o anseio de proteger o titular, sua personalidade e privacidade, apesar das atividades cotidianas nas quais é exigido o fornecimento dos seus dados pessoais, seja para o setor privado ou público<sup>79</sup>. Assim, incorpora princípios constitucionais e estabelece no primeiro artigo que a lei tem “*o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural*”<sup>80</sup> e, ao mesmo tempo, determina no dispositivo seguinte como um dos seus fundamentos “*o desenvolvimento econômico e tecnológico e a inovação*”<sup>81</sup>. Ainda que distintos, esses pontos não são opostos e compatibilizá-los significa incentivar um desenvolvimento tecnológico responsável e um ambiente digital seguro, uma vez que reconhece a interferência realizada pelo tratamento de dados pessoais no âmbito privado do ser humano.

---

<sup>78</sup> MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). Lei Geral de Proteção de Dados Comentada. 2ª ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. p. 19.

<sup>79</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019. p. 109.

<sup>80</sup> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

<sup>81</sup> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Na tentativa de possibilitar a proteção do titular de dados, a LGPD estabelece princípios e hipóteses legais para o tratamento de dados pessoais. Os princípios enumerados nos incisos do art. 6º<sup>82</sup> da normativa refletem a evolução das leis geracionais e são compartilhados por diversas normas em vigor atualmente, como o GDPR. Destaca-se que todos os princípios devem ser sempre observados no tratamento de dados pessoais, independente da base legal adotada<sup>83</sup>. Dentre eles se sobressai o princípio da finalidade, o qual se relaciona profundamente com os princípios da adequação, necessidade e transparência. Em conjunto eles buscam reduzir a chance de aplicação dos dados pessoais em desacordo com o propósito informado sem a existência de um legítimo interesse, além do necessário e sem a devida comunicação prévia, de forma clara, específica e acessível ao indivíduo. De maneira semelhante a GDPR<sup>84</sup> estabelece que os titulares de dados devem ser tratados de maneira justa e transparente e que a colheita ocorra segundo finalidades legítimas, específicas, explícitas, de modo que o tratamento não pode ser incompatível com as finalidades informadas, é o *Purpose Limitation* ou princípio da limitação dos propósitos.

---

<sup>82</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; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; 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; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

<sup>83</sup> MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). Lei Geral de Proteção de Dados Comentada. 2ª ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. p. 138

<sup>84</sup> Art. 5 GDPR Principles relating to processing of personal data

1. Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with [Article 89\(1\)](#), not be considered to be incompatible with the initial purposes ('purpose limitation');

Além do cumprimento dos princípios, há a indispensabilidade da observância das bases legais, pois são elas as responsáveis por legitimar o processamento dos dados pessoais e sensíveis. Sem a adequação a pelo menos uma das hipóteses legais, o tratamento dos dados pessoais não é considerado legítimo. A LGPD dedica-se a listá-las em um rol taxativo no art. 7 no caso de dados pessoais, enquanto o art. 11 trata dos dados sensíveis.

O art. 7º dispõe que o tratamento de dados pessoais poderá ser realizado: mediante o consentimento do titular (I); para o cumprimento de obrigação legal ou regulatória pelo controlador (II); pela administração pública, quando necessário para a execução de políticas públicas (III); para a realização de estudos por órgãos de pesquisa (IV); quando necessário para a execução de contrato de qual seja parte o titular, a pedido do titular dos dados (V); para o exercício regular de direitos em processo judicial, administrativo ou arbitral (VI); para a proteção da vida ou incolumidade física do titular ou terceiro (VII); para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (VIII); para atender aos interesses legítimos do controlador ou de terceiros, salvo no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (IX) e para a proteção ao crédito (X). As hipóteses relacionadas aos dados sensíveis enumeradas no art. 11<sup>85</sup> se assemelham muito as bases legais previamente elencadas no art. 7º, excluindo apenas as duas últimas hipóteses, legítimo interesse e proteção de crédito. Ademais, diferenciam-se pontualmente na concessão do consentimento, que no caso de dados sensíveis deve ser para uma finalidade determinada e de forma específica e destacada.

---

<sup>85</sup> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Assim como a normativa europeia<sup>86</sup>, a lei brasileira define que para o consentimento ser válido, ele deve ser expresso por meio de uma manifestação livre, informada e inequívoca<sup>87</sup>. Em termos ideais, o consentimento somente será legalmente válido quando o usuário deter a capacidade mínima de compreensão técnica associada a possibilidade de aceitar ou declinar os termos estabelecidos para o recolhimento e processamento dos seus dados pessoais sem sofrer qualquer prejuízo de ordem econômica ou social, ou seja, quando o consentimento efetivamente representar uma escolha<sup>88</sup>, uma vez que o tratamento automatizado dos dados pessoais não pode afetar o livre desenvolvimento da personalidade.

A LGPD empenha-se em positivar uma participação ativa do indivíduo em todas as etapas do processamento dos dados pessoais, que inclui a coleta, o acesso, a distribuição, o armazenamento, a eliminação, dentre outras. A lei define diversos direitos do titular no Capítulo III, dentre os quais destacam-se alguns especificados no art. 18, como a possibilidade de acesso aos dados (II); correção de dados incompletos, inexatos ou desatualizados (III); eliminação dos dados pessoais tratados com o consentimento do titular (VI); informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (VIII); revogação do consentimento (IX); opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento (§2º). Além de dispor no artigo 9º que 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.

Embora não exista uma hierarquia entre as hipóteses legais elencadas e que o consentimento não seja necessário para legitimar o tratamento de dados pessoais, nota-se que o consentimento possui um destaque maior na Lei Geral de Proteção de Dados Pessoais brasileira.

---

<sup>86</sup> Art. 4 GDPR Definitions. For the purposes of this Regulation:

(11) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

<sup>87</sup> 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;

<sup>88</sup> A Working Party 29 esclarece que o consentimento apenas será válido quando o tratamento dos dados não for condição para que o usuário possa usar ou acessar o serviço. Caso contrário, o controle obtido através do consentimento é apenas ilusório e o tratamento dos dados será ilegal. Ressalta, ainda, que deve ser uma escolha reversível, nunca uma decisão definitiva que não pode ser alterada. Nesse sentido é a Guidelines on consent under Regulation 2016/679.

Princípios centrados na participação do indivíduo, a adjetivação do consentimento, além de inúmeros mecanismos na lei que concretizam, orientam e reforçam a ideia do consentimento e o protagonismo do titular<sup>89</sup>. Comprovação disso é o fato de a LGPD adotar a autodeterminação informativa como fundamento, reafirmando a construção de um direito de proteção de dados pessoais baseado na participação da pessoa e no seu controle sobre os próprios dados.

Um controle que se estende além do seu âmbito particular e íntimo, englobando informações de natureza pública<sup>90</sup>. Informações pessoais públicas por força de lei, como dados acerca de servidores públicos e a filiação partidária de um candidato, ou aquelas tornadas públicas voluntariamente, tal qual a publicação em uma rede social ou canal de vídeos. Compreender esse controle de maneira abrangente é essencial para permitir a liberdade de pensamento, informação e expressão, de modo que o ser humano consiga externalizar seus interesses, ideologias, crenças e gostos sem nenhum tipo de manipulação pela desinformação e/ou censura, e se comunicar livremente.

O problema é que hoje em dia a tecnologia de rede e algoritmos são capazes de manipular estruturas de poder, tanto na esfera pública, como privada. Exemplos reais e significativos dessa manipulação são como a eleição presidencial de 2016 dos Estados Unidos foi afetada com o processamento de dados dos usuários do Facebook<sup>91</sup> e as *fakes news* na pandemia transformaram-se uma potente ameaça à saúde pública<sup>92</sup>. Na economia, o produto mais bem-sucedido vai ser aquele que agrada o algoritmo do Google e aparecer nos primeiros tópicos de pesquisa<sup>93</sup>. Os consumidores são influenciados não somente pelos mecanismos de busca, mas também pelas comunidades digitais, tais quais o Trip Advisor, Yelp e grupos em redes sociais, nos quais

---

<sup>89</sup> TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*. Rio de Janeiro, a. 9, n. 1, 2020; p. 5.

<sup>90</sup> TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*. Rio de Janeiro, a. 9, n. 1, 2020; p. 12 “*Entende-se não ser razoável admitir que dados disponíveis publicamente possam ser tratados sem uma base legal específica, pois isso seria o mesmo que autorizar que qualquer informação publicada, por exemplo, por força de uma obrigação legal, pudesse ser utilizada para uma finalidade distinta sem que o novo controlador precisasse demonstrar que existia uma base legal que autorizava o tratamento de tal dado, especialmente quando ele não foi tornado público por seu titular*”

<sup>91</sup> BBC NEWS BRASIL (Brasil). Como os dados de milhões de usuários do Facebook foram usados na campanha de Trump. 2018. Disponível em: < <https://www.bbc.com/portuguese/geral-43705839> >. Acesso em: 09 set. 2020.

<sup>92</sup> DE PIERRO, Bruno. Epidemia de fake news: Organização Mundial da Saúde chama atenção para grande circulação de notícias falsas sobre o novo coronavírus. *Revista Pesquisa FAPESP*, 7 abr. 2020. Disponível em: <https://revistapesquisa.fapesp.br/epidemia-de-fake-news/>. Acesso em: 9 set. 2020.

<sup>93</sup> HARARI, Noah Yuval. 21 lições para o século 21. *Companhia das Letras*. p. 43.

compartilham suas experiências, opiniões sobre marcas e avaliam produtos<sup>94</sup>. Estas informações são amplamente coletadas e utilizadas para fins publicitários.

No ambiente da economia digital, dados pessoais de consumidores representam verdadeiros ativos econômicos devido à capacidade de criar perfis, identificar interesses, padrões de comportamento, customizar produtos e produzir publicidade direcionada. O consumidor fica exposto e suscetível à uma ingerência dos algoritmos, à uma inteligência artificial e/ou a terceiros desconhecidos, pois parte de um ponto de vulnerabilidade, no qual negar-se a conceder os dados pessoais implica sua exclusão social e prejuízos econômicos, conforme explicitado anteriormente. Logo, é imprescindível a defesa do consumidor como um dos fundamentos na proteção de dados pessoais<sup>95</sup>.

A defesa do consumidor no comércio digital perpassa ainda pela inibição de atos de abuso de poder, decorrentes de uma grande concentração de poder informativo por uma mesma empresa ou grupo empresarial<sup>96</sup>, e repreensão de práticas discriminatórias. No Brasil, um caso importante na proteção de dados pessoais e do consumidor é o da Decolar. A empresa de turismo foi condenada a pagar R\$ 7,5 milhões em razão da prática de *geopricing* e *geoblocking*, as quais consistem na utilização da localização geográfica do consumidor, respectivamente, para promover uma diferenciação de preços, impedindo ofertas ou uma espécie de desconto a uma pessoa, e no bloqueio de acomodações em hotéis e pousadas<sup>97</sup>. O Departamento de Proteção e Defesa do Consumidor (DPDC), em nota técnica, esclareceu que a utilização da localização geográfica, um dado pessoal, para precificar deve ser justificada (como no caso do frete) e não

---

<sup>94</sup> KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. *Marketing 4.0: Do tradicional ao digital*. Rio de Janeiro: Sextante, 2017; p. 27/29.

<sup>95</sup> MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). *Lei Geral de Proteção de Dados Comentada*. 2ª ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. p. 48: “A necessidade da defesa dos interesses do consumidor diante da sua vulnerabilidade, fragilidade e exposição na era digital ganhou a expressão “consumidor de vidro”, pois praticamente toda atividade humana atual deixa rastro. Assim, a ausência do cumprimento de todas as novas disposições legais que buscam equilibrar a relação de consumo, os consumidores estarão suscetíveis a decisões imperceptíveis pautadas em seus próprios comportamentos, mas não necessariamente de acordo com os seus interesses.”

<sup>96</sup> Idem, p. 42: “A EDPB (European Data Protection Board) considera essencial avaliar as implicações a longo prazo para proteção econômica e garantia de direitos do consumidor sempre que uma fusão significativa for proposta, pois o aumento da concentração de mercado no ambiente digital tem o potencial de ameaçar o nível de proteção de dados e a liberdade que beneficiam os consumidores de serviços digitais.”

<sup>97</sup> VENTURA, Ivan. *Geoblocking e geopricing: os bastidores da disputa pelo turismo online no Brasil*. Consumidor Moderno, 1 ago. 2018.

pode ser utilizada para desfavorecer um grupo, pois caso contrário caracteriza-se uma discriminação em relação ao consumidor e gera um desequilíbrio nas relações de consumo<sup>98</sup>.

Todavia, o caso evidencia um problema maior ainda: a dificuldade de identificação de práticas discriminatórias decorrentes do tratamento indevido de dados pessoais pelos órgãos de fiscalização e regulamentação. A constatação da prática abusiva e discriminatória só foi possível graças à representação de uma empresa concorrente, a Booking, no DPDC, pois o consumidor ou órgãos responsáveis pela fiscalização não foram capazes de identificá-la<sup>99</sup>. Nota-se que, apesar da utilização preconceituosa dos dados pessoais do consumidor, ele sequer tem o conhecimento sobre como se dá o uso dos seus dados e muito menos tem a capacidade técnica de defender a si mesmo. Letícia Canut e Heloísa Gomes Medeiros<sup>100</sup> afirmam que existe uma opacidade sobre como se dá o funcionamento do algoritmo no comércio eletrônico, visto que, no processamento automatizado, dificilmente sabe-se o porquê dos resultados obtidos<sup>101</sup>. Então como identificar a violação ao direito do titular dos dados, na qualidade de consumidor ou ainda cidadão, se as violações e o procedimento de decisão não são conhecidos?

O desamparo jurídico do titular de dados, na qualidade de consumidor, é ainda mais evidente no caso do marketing direto. Fundamentado na construção de um relacionamento entre a empresa e o cliente, o marketing dedica-se a conhecer de maneira profunda o consumidor, ao ponto de por meio do processamento de dados pessoais montar um dossiê digital do consumidor e

---

<sup>98</sup> MINISTÉRIO DA JUSTIÇA. Departamento de Proteção e Defesa do Consumidor. Nota Técnica n.º 92/2018/CSA-SENACON/CGCTSA/GAB-DPDC/DPDC/SENACON/MJ. 15 jun. 2018.

<sup>99</sup> VENTURA, Ivan. Geoblocking e geopricing: os bastidores da disputa pelo turismo online no Brasil. *Consumidor Moderno*, 1 ago. 2018. “A *Booking.com*, inclusive, não apenas deu início ao processo administrativo, mas também contribuiu com evidências para o governo. Um exemplo foi a pesquisa de simulação simultânea de reserva de hospedagem, feito pela empresa, dentro o site da *Decolar*. Isso ocorreu por meio de computadores localizados nas cidades de São Paulo (Brasil) e Buenos Aires (Argentina). Nessa pesquisa foram registrados valores diferentes para as mesmas reservas.”

<sup>100</sup> CANUT, Leticia; MEDEIROS, Heloísa Gomes. Os algoritmos nas relações de consumo eletrônicas: Análise do Direito do Consumidor à Informação. XI Congresso de Direito de Autor e Interesse Público, Curitiba, p. 1039-1061, 2017.

<sup>101</sup> A LGPD prevê como um direito do titular o direito à explicação no caso de decisões automatizadas, podendo ser solicitado a revisão da decisão em si, bem como informações claras acerca dos critérios e procedimentos adotados. “Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.”



conseguir influir em sua esfera pessoal<sup>102</sup>. O mais conhecido e referenciado dos casos é o da Target, uma varejista do *e-commerce*, que foi capaz, por meio de análises estatísticas e tratamento de dados pessoais, identificar o comportamento de compra de clientes grávidas. Assim, ao direcionar campanhas específicas para gestantes a uma adolescente, o pai reclamou alegando que ação poderia incentivar sua filha engravidar. No entanto, o homem descobriu um tempo depois o que a Target já sabia, sua filha estava grávida<sup>103</sup>.

O marketing direto centra-se em explorar o comportamento, sentimentos, gostos, desejos do consumidor, que são facilmente identificáveis com o tratamento dos dados pessoais, de modo a desenvolver um relacionamento e uma comunicação eficaz com o cliente<sup>104</sup>. A problemática reside no desequilíbrio existente na relação, pois a quantidade de informação que cada parte detém um sobre o outro é desigual, enquanto empresa muito sabe sobre seu consumidor, este nada ou pouco sabe sobre a empresa. O titular de dados está em uma posição de vulnerabilidade, em razão da sua desinformação e desconhecimento, portanto passível de ser manipulado e suscetível a uma tecnologia persuasiva das campanhas publicitárias. Logo, como pode o ser humano por meio do consentimento realizar um efetivo controle dos seus dados e tutelar sua personalidade contra o marketing?

---

<sup>102</sup> MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental. Edição do Kindle. São Paulo: Saraiva, 2014. Paginação Incorreta. Posição 1843. *“A vulnerabilidade do consumidor nesse processo de coleta e tratamento de dados pessoais é tão patente que se cunhou a expressão “consumidor de vidro” para denotar a sua extrema fragilidade e exposição no mercado de consumo, diante de inúmeras burocracias privadas que tomam decisões e influenciam as suas oportunidades, a partir das informações pessoais armazenadas em bancos de dados.”*

<sup>103</sup> O caso foi relatado e analisado por Charles Duhigg, com contribuições de Andrew Pole, cientista de dados da Target, em uma matéria publicada no jornal New York Times. Disponível em: <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&r=1&hp>.

<sup>104</sup> TORRES, Claudio. A Bíblia do Marketing Digital: tudo que você queria saber sobre marketing e publicidade na Internet e não tinha a quem perguntar. São Paulo: Novatec Editora, 2009. p. 66-67.

## 4. O CONSENTIMENTO DO CONSUMIDOR COMO INSTRUMENTO DE AUTODETERMINAÇÃO INFORMACIONAL NO MARKETING DIRETO

### 4.1 O papel do consentimento

Diante da exploração econômica que os dados pessoais estão submetidos articular a tutela dos dados pessoais como um direito fundamental da personalidade é primordial. No desenvolvimento do direito a proteção de dados pessoais a ideia do consentimento estruturou-se como um dos pilares fundamentais da matéria, sob os argumentos de promover um maior controle do indivíduo sobre seu fluxo de informações e viabilizar uma autodeterminação informativa, conforme pontuado anteriormente. Faz necessário promover uma análise do papel do consentimento e sua efetividade na inserção dos dados pessoais na economia da informação à medida que garante a proteção do cidadão.

O fato é que o consentimento não é um instituto novo e carrega consigo uma definição e compreensão semântica originária do direito civil. Neste âmbito, o consentimento é um reflexo do princípio da autonomia privada, pois é a competência atribuída ao cidadão de alterar sua esfera jurídica por meio da manifestação da sua vontade. O consentimento assume a dupla função de ser uma expressão do querer, correspondente às intenções íntimas da pessoa, e de legitimar o negócio jurídico, expressando concordância com as condições e com a situação jurídica.

No entanto, a utilização do consentimento na sistemática de tutela dos dados pessoais, afastado da dogmática do direito civil, sem a devida observância dos efeitos práticos da sua aplicação nos casos concretos, ocasiona uma distorção da finalidade e funções do instituto. Na condição de manifestação da vontade o consentimento apresenta-se como elemento essencial na construção da esfera privada e da autonomia informacional do titular na tutela dos dados pessoais. Na instrumentalização da autodeterminação, o consentimento será sempre revogável sob o argumento de proteger os elementos da personalidade<sup>105</sup>. A revogabilidade incondicional

---

<sup>105</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019; p. 303. *“A ideia da sua revogabilidade incondicional encontra fundamento no fato de se estar protegendo a própria personalidade, entre cujos atributos estaria a*

do consentimento teoricamente é o instrumento de garantia do livre desenvolvimento da personalidade, como um direito essencial do titular.

Em aspectos práticos, o cidadão no exercício da sua autonomia privada emprega o consentimento para relativizar a indisponibilidade dos direitos da personalidade. Quem consente atua moldando a esfera jurídica para conceder o direito de uso e gozo da sua imagem, do seu nome, dos seus dados pessoais em favor a quem foi consentido. Sob o foco do marketing digital, ter o poder de fruição sobre os dados e informações pessoais do consumidor de forma ampla e extensiva é um importante diferencial capaz de determinar o êxito da campanha publicitária, mas não é condição primordial para desenvolvimento da atividade de marketing<sup>106</sup>. Logo, o consentimento dado pelo titular não pode ser incorporado como definitivo, mas deve ser feito observando a possibilidade de reversibilidade.

Todavia, se o indivíduo utiliza do direito de revogação, que foi institucionalizado pela LGPD em seu artigo 8º, §5º, de maneira abusiva, impõe-se um risco alto e dispendioso a quem recebeu e depende do consentimento. Condutas abusivas em razão da possibilidade de revogação do consentimento de forma incondicionada constitui uma esfera de insegurança para o desenvolvimento das tecnologias da informação e estabelecimento de relações negociais fundamentadas no processamento de dados pessoais. Efeito completamente contrário ao propagado pelo movimento mundial de crescimento das técnicas de bioinformática, de ampliação do comércio digital e democratização da internet.

O estabelecimento de uma esfera de incerteza e insegurança a ciência da informação não beneficia o ser humano na proteção da sua personalidade. Isso porque dificulta uma regulamentação eficaz da tecnologia, do seu uso e suas consequências, que cada vez mais estão integradas ao cotidiano humano.

---

*indisponibilidade. Por este ponto de vista, tal consentimento será sempre revogável e a sua caracterização como ato jurídico unilateral serve a reforçar essa revogabilidade”.*

<sup>106</sup> Importante compreender que a revogação como exercício da autodeterminação informacional só é viável e discutível no tratamento dos dados pessoais que aconteça sob a hipótese legal do consentimento, pois nos casos de processamento de dados pessoais justificado sobre uma outra base legal como o legítimo interesse do controlador e na necessidade para execução e satisfação do contrato não há porque se falar em revogabilidade, incondicionada ou condicionada, como um instrumento de tutela da personalidade disponível ao titular tutelar.

Em contrapartida, na função legitimadora, o consentimento atua validando o uso dos dados pessoais para fins econômicos por terceiros, como uma hipótese legal do tratamento de dados pessoais. Trata-se de um consentimento negocial, de natureza jurídica fortemente contratual, pois inseridos no mercado, os dados pessoais assumem a condição de ativos econômicos e são amplamente explorados, enquanto é oferecido vantagens e benefícios econômicos aos titulares pela concessão da informação.

Na realidade, o consentimento, segundo uma visão meramente negocial, é ineficiente para tutelar o desenvolvimento da personalidade, a liberdade e a igualdade. Isso porque, os modelos econômicos fundamentados na informação valem-se dos dados pessoais como uma moeda de troca. Na *práxis*, a concessão e validação da coleta dos dados pessoais, por meio da concordância com políticas de privacidade, é uma condição de acesso a determinado serviço. Contra quem é demandado o consentimento não é concedida efetiva possibilidade de escolha, mas apenas a opção de conceder ou recusar-se e, conseqüentemente, usufruir ou não do serviço.

Além do mais, o processamento de dados pessoais fora da esfera coletiva e difusa aparenta-se inofensivo, pois é difícil a identificação individualizada dos males que a colheita, armazenamento, tratamento e compartilhamento de informações pessoais pode ocasionar na vida do ser humano. É inviável que o homem sozinho compreenda de maneira prévia as conseqüências advindas do processamento de dados pessoais e, à vista disso, exerça a concessão do consentimento como um instrumento da tutela da sua privacidade.

Soma-se ainda o que alguns autores chamam de paradoxo de privacidade, no qual apesar do usuário anunciar uma efetiva preocupação com a sua privacidade, não toma atitudes que traduzam esta apreensão e consome uma falsa sensação de segurança baseada na impessoalidade das relações virtuais. Na lógica do paradoxo, primeiro o indivíduo expõe-se, muitas das vezes por vontade própria com a publicação periódica da sua vida cotidiana em redes sociais, para depois efetivamente proteger sua privacidade. Assim, observa-se que

*“quando o consentimento centraliza a disciplina, o interessado somente poderá obter a tutela em um momento posterior ao consentimento, valendo-se da arguição de algum*

*defeito desse – o que implica que a pessoa tenha que, primeiro, concordar em revelar seus dados para somente depois se valer da tutela*<sup>107</sup>

A inserção da ideia de consentimento negocial, segundo uma dogmática do direito civil, dentro da matéria de proteção de dados pessoais confere um papel ficcional ao consentimento, denominado de mito do consentimento. A principal crítica se dá em razão da tentativa de moldar o instituto do consentimento do direito civil, no qual este representa um verdadeiro instrumento de consumação da autonomia privada e de escolha, ao ambiente virtual do *e-commerce* e das redes sociais<sup>108</sup>.

É ilusória a semelhança existente entre o consentimento legislado pelo Código Civil e aquele adotado, conceituado e caracterizado pelas normativas de regulamentação da tecnologia de tratamento de dados pessoais, como a LGPD. A dupla função do consentimento assume outros contornos quando observadas suas consequências dentro da realidade da economia da informação e do direito a proteção de dados pessoais. Logo, deve ser revisto o papel do consentimento, de modo a serem estabelecidos parâmetros, além da sua mera adjetivação<sup>109</sup>, para sua concessão e critérios de ponderação contextuais de fácil observância, tais quais o campo de aplicação, as finalidades e os interesses em jogo.

O consentimento sozinho, desvinculado dos princípios, afastado das garantias advindas dos direitos fundamentais e sem uma análise contextual fática, é incapaz de empoderar, o (hiper)vulnerável, titular de dados ao ponto deste alcançar uma autonomia informacional privada mínima dentro do mercado informacional<sup>110</sup>. Instrumentalizado o ato de concessão, concordância, anuência, cessão, este se limita a um papel pro forma, para pura satisfação procedimental do sistema legal arquitetado pelo direito de proteção de dados pessoais.

---

<sup>107</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019; p. 299.

<sup>108</sup> DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019; p. 301.

<sup>109</sup> A LGPD adjetiva e caracteriza o consentimento no seu art. 5, XII, como devendo este ser uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada para que seja considerado válido, no entanto não estabelece ou informa quais requisitos devem ser satisfeitos para que o consentimento seja explícito, verdadeiramente informado e advindo de uma manifesta expressão da vontade do titular.

<sup>110</sup> BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense. 2019; p. 209

## 4.2 A (in)efetividade do consentimento como cerne único da autodeterminação informacional na esfera do marketing

Verifica-se que na prática o consentimento se dá pela anuência aos termos e condições gerais de um serviço e na demarcação de caixas pré-definidas para configuração de *cookies*. Por certo a concordância do indivíduo com uma política de privacidade não é capaz de promover uma autonomia informacional mínima. Entretanto o capítulo não se destina a adentrar no debate sobre a forma adequada de obtenção do consentimento, mas sim evidenciar a ineficácia do consentimento como cerne único da autodeterminação informal.

No direito de proteção de dados pessoais, o consentimento é o instituto jurídico adotado por meio do qual *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*<sup>111</sup>. Assim, a autodeterminação informacional está associada ao controle de acesso aos dados pessoais, por meio da limitação do fluxo de informação. O titular decide a quem concede, para que concede, por quanto tempo concede seus dados, visto o direito de revogabilidade.

Em teoria, o consumidor tem autonomia informacional quando de maneira consciente<sup>112</sup>, por meio de uma manifestação livre<sup>113</sup> dá o seu consentimento informado<sup>114</sup>, para organizações privadas colher, processar, armazenar e compartilhar seus dados pessoais para fins de publicitários e de marketing. Nesta circunstância, o titular consegue exercer segundo o seu livre-

---

<sup>111</sup> Mendes, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. Revista de Direito do Consumidor. vol. 102. ano 24. São Paulo: Ed. RT, nov.-dez. 2015, p. 29

<sup>112</sup> MIRAGEM, Bruno. A Lei Geral de Proteção de dados (Lei 13.709/2018) e o Direito do Consumidor. Revista dos Tribunais. Vol.: 1009/2019. Thomson Reuters Brasil. Novembro/2019; p 19 “*a lei define que a manifestação deve ser inequívoca. Assume o sentido de que o consentimento, quando expresso pelo consumidor, deve ser compreendido por ele como tal. Visa-se impedir a manipulação da vontade daquele do titular dos dados*”

<sup>113</sup> TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civillistica.com. Rio de Janeiro, a. 9, n. 1, 2020. p. 7. “*Livre significa que o titular pode escolher entre aceitar ou recusar a utilização de seu bem, sem intervenções ou situações que viciem o seu consentimento.*”

<sup>114</sup> MIRAGEM, Bruno. A Lei Geral de Proteção de dados (Lei 13.709/2018) e o Direito do Consumidor. Revista dos Tribunais. Vol.: 1009/2019. Thomson Reuters Brasil. Novembro/2019; p 18 “*a noção de consentimento informado firma-se em termos amplos não apenas com o reconhecimento de um dever de repassar informações àquele que deve manifestar seu consentimento, mas um autêntico dever de esclarecimento (esclarecer = tornar claro), de modo a reconhecer o dever daquele a quem compete informar, de tornar estas informações compreensíveis para o destinatário.*”

arbítrio a tutela da sua personalidade, pois está em condições ideais. Não foi constrangido ao fornecimento dos seus dados para obter vantagens ou não sofrer prejuízos econômicos. Tem acesso às informações completas, bem como compreende as etapas e os atores envolvidos no tratamento de dados pessoais. É capaz, portanto, de instituir limites para o tratamento automatizado dos seus dados pessoais.

Na prática, no entanto, existe um desequilíbrio de poder que é incapaz de ser suprimido pelo consentimento, em razão de uma assimetria de recursos técnicos, no sentido de processamento de informações, e econômicos entre o operador/controlador e o titular de dados, na qualidade de consumidor<sup>115</sup>. A democratização das técnicas de coleta e processamento de dados, devido ao desenvolvimento da tecnologia da informação, aumentou a capacidade de produção de conhecimento especializado em larga escala. Aprofundou-se, assim, o desequilíbrio prévio na medida em que um dos polos da relação sabe demasiadamente mais sobre a outra, enquanto a outra detém pouco ou quase nenhum conhecimento.

Os dados pessoais na economia de vigilância são utilizados como uma moeda de troca, visto que o acesso ao produto ou serviço somente é concedido depois que o titular cede e faculta o uso deles como ativo na atividade publicitária. Desta forma, impõe-se ao consumidor a obrigação de avaliar o custo social da privacidade. Fator este que afasta por completo a crença que o consentimento é dado segundo um processo genuíno de tomada de decisão de um sujeito racional<sup>116</sup> e livre de constrangimentos externos.

Além disso, há a falta de transparência do processo decisivo das inteligências artificiais responsáveis por tratar os dados pessoais. Os critérios relacionados pelo software para decisão automatizada são um mistério para o usuário, que não detém o conhecimento técnico suficiente para compreender os elementos decisivos impostos ao tratamento de dados. A opacidade dos critérios da tomada de decisão automatizadas ficam mais evidentes nos *machines learning*, que conseguem estabelecer novos parâmetros de análise independentes dos estipulados pelo

---

<sup>115</sup> O Código de Defesa do Consumidor reconhece em seu art. 4, I a vulnerabilidade do consumidor no mercado de consumo, visto o desequilíbrio intrínseco existente na relação entre fornecedor e consumidor.

<sup>116</sup> BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019, p. 148

programador. Os próprios estudiosos da área de TI e computação, como programadores, desenvolvedores não possuem uma compreensão integral do funcionamento dos mecanismos de autonomia dos *machines learning*. A inteligência artificial com capacidade de aprendizagem possui uma autonomia contra a qual o instituto jurídico do consentimento é absolutamente ineficaz.

A fragilidade do consentimento fica ainda mais evidente quando considerado o tratamento de dados pessoais sensíveis<sup>117</sup>. É característico do dado sensível seu alto potencial lesivo ao titular, por tratar-se de informações que por si só são capazes de gerar discriminação e incitar costumes sexistas, racistas, xenofóbicos e outras práticas preconceituosas. O processamento de dados sensíveis, portanto, deve ser mais rigoroso, visto o risco maior impostos aos direitos de liberdade e igualdade e a potencialidade de violar a personalidade e intimidade do usuário.

Importante ressaltar que os efeitos do tratamento de dados pessoais não são limitados a uma esfera econômica, mas afetam também de forma significativa as relações humanas sociais e políticas<sup>118</sup>. O escandaloso caso da Cambridge Analytica, empresa de análise de dados que participou da campanha de Trump em sua corrida à Presidência dos EUA em 2016, comprova o poder da tecnologia de informação de manipular a sociedade e o futuro humano<sup>119</sup>. A companhia utilizou da análise de dados pessoais, coletados por meio de um teste psicológico realizado no Facebook, para direcionar uma publicidade negativa da opositora Hillary Clinton e pró-Trump na mesma rede social. O direcionamento do marketing político fundamentado no comportamento do usuário influenciou de maneira gradativa e não notável na percepção política do cidadão estadunidense. Principalmente em relação aos eleitores em dúvida, a implementação de uma publicidade comportamental política na rede social levou-os a ter posicionamentos políticos que normalmente não possuem.

---

<sup>117</sup> A LGPD considera dados pessoais sensíveis aqueles que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; relativos à vida sexual ou orientação sexual; biometria e genética, para simples identificação conforme o art. 5, II.

<sup>118</sup> MIRAGEM, Bruno. A Lei Geral de Proteção de dados (Lei 13.709/2018) e o Direito do Consumidor. Revista dos Tribunais. Vol.: 1009/2019. Thomson Reuters Brasil. Novembro/2019; p. 2.

<sup>119</sup> ENTENDA o escândalo político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. BBC News, 20 de março de 2018. Disponível em: < <https://www.bbc.com/portuguese/internacional-43461751>>. Acesso em: 20 out. 2020.



Destaca-se que, embora ilegítima a compra dos dados pessoais dos usuários do Facebook e indevido o processamento pela Cambridge Analytica, a coleta foi legal e ocorreu de acordo com a política de privacidade da rede social, a qual prevê e permite em seus termos a utilização da informação dos seus usuários para fins científicos<sup>120</sup>. O teste de personalidade que foi realizado por um pesquisador da Universidade de Cambridge, no Reino Unido, aconteceu com o consentimento das pessoas, que à época da pesquisa inclusive chegaram a ser pagas para responder as perguntas e concordaram expressamente com a coleta dos seus dados para propósito acadêmico.

Diante do fornecimento, o marketing beneficia-se de todos os métodos de processamento de dados pessoais, com o fim de caracterizar e desenvolver um retrato detalhado e fiel da personalidade do sujeito, ao ponto de ter ingerência na em sua esfera pessoal. Uma vez que os dados pessoais constituem uma projeção da personalidade, portanto expõe a própria identidade do indivíduo. Ainda que não se saiba com certeza quem é, o consumidor é segmentado em nichos conformes suas particularidades, de modo a ficar sujeito aos riscos de decisões automatizada, de práticas discriminatórias ilícitas e as manipulações de uma tecnologia persuasiva.

Constata-se, que, não há um encontro entre a sistemática do direito de proteção de dados pessoais e a realidade fática que possibilite a autodeterminação informacional fundamentada somente no consentimento. É necessário estabelecer outros pilares capazes de promover um equilíbrio na relação de consumo da economia de informação e, conseqüentemente, viabilize ao cidadão exercer de maneira efetiva sua autonomia informacional. É o que Bruno Bioni denomina de arquitetura de vulnerabilidade<sup>121</sup>, a qual é operacionalizada por meio de mecanismos que superem a assimetria de poder presente no fluxo informacional de dados pessoais, e defende que:

---

<sup>120</sup> A justificação de pesquisas com base no argumento que o usuário ao concordar com os termos de uso do Facebook consentiu com a utilização dos seus dados para fins científicos não é novidade. Em 2014, o Facebook realizou uma pesquisa de cunho emocional, na qual as *timelines* eram manipuladas com notícias e postagens com uma carga emocional positiva ou negativa para saber qual o efeito destas nos usuários. A pesquisa concluiu que emoção expressada por terceiros no Facebook influencia como o indivíduo se sente, os posts feitos pelos os usuários refletiam a carga emocional do conteúdo consumido. Ela foi justificada com base na concordância do usuário a política de privacidade da rede social. Mais informações disponíveis em: <https://www.pnas.org/content/111/24/8788>.

<sup>121</sup> BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019, p.206 “*A arquitetura da rede deve, assim, funcionalizar tal habilidade, tomando-se como ponto de partida que o titular dos dados pessoais é um sujeito vulnerável de fato. É o que chamamos em outra oportunidade de arquitetura de vulnerabilidade, pela qual se deve aparelhá-lo com mecanismos que lhe permitam superar a sua debilidade com relação ao fluxo de suas informações pessoais.*”

*“Somente desta forma se superará parte do drama da proteção dos dados pessoais, que é a sublinhada falta de correspondência entre o programado direito da autodeterminação informacional e uma arquitetura que lhe dê vazão. Trata-se, portanto, de promover o encontro entre o arranjo jurídico-normativo da privacidade informacional com a realidade que lhe é subjacente, buscando-se novas formas para o venerado consentimento do titular dos dados pessoais, nutrindo-se, em última análise, a sua capacidade (autonomia) em controlá-los”<sup>122</sup>*

A eficácia do controle por meio do consentimento é condicionada a um empoderamento do titular, por meio do qual o exercício da autonomia informacional ultrapasse o momento e o ato de concessão do consentimento. Mas como garantir que o controle do sujeito sobre seus dados pessoais após o consentimento, frente a assimetria de poder existente entre o cidadão e as organizações privadas?

#### **4.3 Novos pilares da autodeterminação informacional: privacidade contextual e a Autoridade Nacional de Proteção de Dados Pessoais**

Primeiramente, deve ocorrer uma mudança sobre a percepção do exercício da autonomia informativa. A autodeterminação informacional deve ser compreendida como a previsibilidade do indivíduo sobre o seu fluxo informacional dentro de uma conjuntura concreta, com o intuito de preservar um fluxo de informações pessoais ético e adequado a valores sociais. Não se abandona, todavia, a ideia de autodeterminação informativa como o poder de limitar determinar quais dados podem ser tratados, para que fins podem ser tratados, com quem podem ser compartilhados.

Defende-se uma privacidade contextual na qual o controle informacional deve ocorrer sobre uma análise contextual caso a caso, a qual permitirá verificar a integridade do fluxo de informações pessoais<sup>123</sup>. O objetivo é condicionar a validade do processamento de dados pessoais ao contexto em que este acontece, de modo a estabelecer restrições ao fluxo de dados de acordo

<sup>122</sup> BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019, p.207

<sup>123</sup> BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019, p.212. *“Dessa conjunção (contexto + integridade) é que se arquiteta uma alternativa normativa em que a proteção dos dados pessoais não se baseia única e exclusivamente nos desígnios do próprio titular dos dados pessoais. Pelo contrário, as chamadas normas informacionais impõem restrições ao fluxo informacional que independem do controle (consentimento) exercido pelo indivíduo. [...] É o produto (normas constitucionais) dos citados elementos (contexto e integridade) dessa equação que governar o trânsito de dados.”*

com as motivações, finalidades e consequências identificadas em uma configuração social específica. Para tanto, a análise contextual deve ser dividida em um estudo da relação que justifica a coleta primária e o tratamento dos dados pessoais, o que seria o fluxo interno, e o compartilhamento da informação com terceiros, denominado de fluxo externo do trânsito de dados pessoais presente na sociedade de informação.

No fluxo interno busca-se identificar os personagens envolvidos, o vínculo entre eles, o motivo que dá causa ao processamento de dados pessoais e, por último, a esfera social na qual estão postos. Enquanto no exame do fluxo externo, analisa-se o envolvimento de terceiros no fluxo informacional e a disseminação da informação. Por exemplo, uma relação médico–paciente o compartilhamento do histórico de saúde do paciente é esperado, porém o médico compartilhar informações acerca do estado de saúde do seu paciente com o empregador deste é indevido<sup>124</sup>, ou ainda, com um plano de saúde, seria ilegítimo e errado.

No caso de uma relação de consumo, o fornecimento de informações pessoais como nome, dados bancários e endereço é essencial para concretização da transação comercial, logo, apropriado. Se a empresa utiliza das informações fornecidas para direcionar sua publicidade com o objetivo de sugerir produtos e informar promoções ao consumidor há um fluxo informacional legítimo, porque o cliente espera por esse tipo de marketing. Entretanto, se os dados pessoais coletados são utilizados para realizar a diferenciação de preços, praticando *geopricing*, o cliente não espera este tipo de prática, portanto, o fluxo informacional é indevido e ilegítimo.

Isso porque ao fornecer os dados e consentir com tratamento destes, o consumidor carrega uma expectativa sobre o seu fluxo de informação concernente a esfera social que está inserido. Esta legítima expectativa do titular deve vincular o tratamento de dados pessoais, de modo a garantir um fluxo informacional íntegro. Caso contrário, o consentimento, ainda que livre, informado e inequívoco, poderia ser utilizado para legitimar o tratamento abusivo e ofensivo dos dados pessoais, de maneira a ameaçar o livre desenvolvimento da personalidade do titular.

---

<sup>124</sup> BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019, p. 214/215.

Nesta lógica, o consentimento passa ser contextual, à medida que condiciona a utilização dos dados pessoais a um conjunto de ações passíveis de execução dentro de contexto limitado por costumes sociais e práticas de conduta<sup>125</sup>. Sem vincular e limitar, concomitantemente, o tratamento de dados pessoais as finalidades especificadas no momento em que se deu o consentimento. A privacidade contextual permite uma ampliação elástica do consentimento, que promove dinamicidade ao fluxo informacional e evita a sobrecarga do cidadão pela exigência constante de se manifestar para consentir com a coleta dos seus dados pessoais, a denominada fadiga do consentimento.

Pautado na legítima expectativa do cidadão e em uma relação de confiança, o processamento de dados pessoais na privacidade contextual deve ser orientado pelo princípio da boa-fé objetiva. Impõe-se o dever de lealdade e cooperação entre as partes. É segurança de uma conduta proba, honesta, adequada, leal que fundamental a privacidade contextual.

*“A privacidade contextual reside justamente na fidelidade depositada pelo emissor de uma informação ao(s) seu(s) recipiente(s), na legítima expectativa de que seus dados pessoais serão usados e compartilhados de acordo com o contexto de um relação preestabelecida ou a razão pela qual foi publicizado um dado; particularmente, na esperança de que o trânsito das suas informações pessoais não minará e trairá sua capacidade de livre desenvolvimento da personalidade e de participação social.”<sup>126</sup>*

Nota-se que a privacidade contextual reduz o protagonismo do consentimento como instrumento de estruturação da autonomia informacional do titular de dados. A legítima expectativa da privacidade do indivíduo e o dever de observância do princípio da boa-fé objetiva pelo operador e controlador estabelecem-se como novos pilares do direito à autodeterminação informacional.

Embora a privacidade contextual estruture uma dinâmica fática que propicie o direito à autodeterminação informacional, ela não diminui a assimetria de força das relações de consumo perpetuas na economia de vigilância. O cidadão continua a ocupar uma posição de desvantagem informacional, técnica e econômica. Logo, faz-se necessário a intervenção de um terceiro

---

<sup>125</sup> BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019, p. 243

<sup>126</sup> BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019, p. 247

elemento na relação, o Estado, que reequilibre os poderes entre as partes, atribuindo poder ao (hiper)vulnerável titular de dados.

No Brasil, a Autoridade Nacional de Proteção de Dados Pessoais – ANPD assume esse papel de intervir para operacionalizar o direito à autodeterminação informacional e garantir ao titular o controle não só dos seus dados pessoais, mas também sobre seu fluxo de informações. Em atenção a vulnerabilidade do consumidor, a autoridade de dados recebe a função de verificar a observância da boa-fé objetiva pelo controlador/operador e das legítimas expectativas do consumidor no tratamento de dados pessoais dentro de um modelo de privacidade contextual.

Tarefa à qual ganha embasamento jurídico diante das competências da ANPD, estabelecidas pelo art. 55-J da LGPD, de promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança (VI); estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais (VIII); garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento (XIX) e implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais (XXIV). Observa-se que a própria normativa reconhece a deficiência informacional da população acerca da temática, a dificuldade do indivíduo de controlar os seus dados pessoais e busca oferece recursos para minimizar esses problemas.

Por fim, conclui-se que a operacionalização de um direito à autodeterminação informacional exige uma tutela estatal. Uma atuação administrativa previa que abarque diferentes frentes como a promoção de uma cultura brasileira de privacidade, por meio da conscientização da população e o estabelecimento de políticas públicas, e a regulamentação de tecnologias que favoreçam o controle e proteção dos dados pessoais, tais quais as *privacy enhancing technologies –PETs*. É a intervenção paternalista do Estado que reequilibra a relação, empodera o (hiper)vulnerável titular de dados e estabelece condições mínimas para que o indivíduo exerça sua autonomia informacional.

## 5. CONCLUSÃO

O instituto-jurídico do consentimento no direito de proteção de dados pessoais assume contornos diferentes daqueles presentes na carga dogmática do Direito Civil. Na tutela do titular dos dados, o consentimento assume a função tripla de (i) legitimar a inserção dos dados pessoais na economia de informação na qualidade de ativos econômicos, (ii) facultar ao indivíduo o controle do fluxo de seus dados dentro do mercado informacional e (iii) proteger o desenvolvimento da personalidade do titular contra os riscos provenientes da coleta, processamento e compartilhamento dos dados pessoais. A multiplicidade de dimensões é essencial para viabilizar a autodeterminação informacional do consumidor, ao mesmo tempo que fiscaliza a legitimidade do tratamento de dados pessoais.

No entanto, em um estudo de situações fáticas que permeia as relações comerciais, compreende-se a (hiper)vulnerabilidade do consumidor na economia de vigilância. A discrepância de força existente entre os organismos privados, que utilizam da tecnologia da informação para conduzir seus negócios, e o consumidor, que é submetido as decisões provenientes do tratamento de dados pessoais, impossibilita que o consentimento seja um instrumento eficiente na operacionalização da autonomia informativa do consumidor. O consentimento é ineficaz ao promover a liberalidade de escolha efetiva sobre o destino dos seus dados pessoais ao indivíduo.

Ademais, o conceito de autodeterminação informacional limitada a uma mera concessão ou não do dado pessoal poderia legitimar práticas discriminatórias ou, extremamente, invasivas pelo marketing direto. Seja por meio da diferenciação de preços em razão do endereçamento do consumidor ou a qualificação do consumidor com base em sua capacidade financeira. Ou ainda, pelo sugestionamento de produtos, marcas, conteúdos e até ideologias e posicionamento políticos capazes de manipular e influir no âmbito privado do indivíduo. Conclui-se que a sistemática do direito de proteção de dados pessoais não produz reflexos na realidade.

Faz-se necessário, assim, a construção de uma arquitetura de empoderamento do (hiper)vulnerável que dê efetividade ao controle dos dados pessoais pelo consumidor e proteja-o,

na qual o direito à autodeterminação informacional é concebido como controle do fluxo informacional e que extrapola o momento do consentimento. Nesta nova estrutura jurídica, além do pilar do consentimento, delinea-se os pilares da privacidade contextual e a ANPD. A privacidade contextual impondo um controle subjetivo do fluxo informacional, de modo a manter-lhe íntegro por meio do dever de observância da legítima expectativa do consumidor e o tratamento de dados pessoais segundo a boa-fé objetiva. A autoridade de dados promovendo uma tutela estatal capaz exercer um controle objetivo da atividade de processamento de dados, cabendo-lhe fiscalizar, educar a população e regular novas tecnologias que possibilitam uma proteção maior da privacidade do consumidor.

## REFERÊNCIAS

ARTICLE 29 DATA PROTECTION WORKING PARTY: Opinion 2/2010 on online behavioural advertising, de 22 de junho de 2010. Disponível em: <[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf)>. Acesso em: 9 set. 2020

\_\_\_\_\_. Opinion 03/2013 on purpose limitation, de 2 de abril de 2013. Disponível em: <[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf)>. Acesso em: 10 de set. 2019

\_\_\_\_\_. Guidelines on consent under Regulation 2016/679, de 28 de novembro de 2017. Disponível em: [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=623051](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051). Acesso em: 8 ago. 2019.

ACQUISTI, Alessandro; GROSSKLAGS, Jens. Economics of Information: Security Privacy and Rationality in Individual Decision Making. **IEEE Security & Privacy Magazine**, p. 24-30, jan/fev. 2005

BARBOSA, Marco Antonio; SANTOS, Marco Aurelio. O direito na sociedade da informação e perspectivas para a sociedade do conhecimento. **Direitos Fundamentais e Justiça** – ano 8, nº 28, p. 82/99, julho/setembro. 2014. Disponível em: <<http://dfj.emnuvens.com.br/dfj/article/view/209/787>>. Acesso em: 12 ago. 2020

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

BRASIL. Constituição (1988). Proposta de Emenda Constitucional nº 17, de 12 de março de 2019. Poder legislativo, Brasília, DF, 03 de julho de 2019. Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1560427715849&disposition=inline>>. Acesso em: 8 ago. 2018.

\_\_\_\_\_. Lei nº 13.709, de 14 de agosto de 2018. **Lex**: legislação federal e marginalia, Brasília, 14 ago. 2018.

\_\_\_\_\_. Lei nº 8.078, de 11 de setembro de 1990. **Lex**: legislação federal e marginalia, Brasília, 11 set. 1990

\_\_\_\_\_. Departamento de Proteção e Defesa do Consumidor. Processo administrativo. Consumidor. Ofensa à liberdade de escolha nas contratações, pelos consumidores. Diferenciação de preço de acomodações e negativa de oferta de vagas, quando existentes, de acordo com a localização geográfica do consumidor. Técnicas de geopricing e geoblocking. Aplicação de sanção de multa no valor de r\$ 7.500.000,00 (sete milhões e quinhentos mil reais). Nota Técnica n.º 92/2018/CSA-SENACON/CGCTSA/GAB-DPDC/DPDC/SENACON/MJ. PROCESSO Nº 08012.002116/2016-21. Representante: Booking.com. Representada: Decolar.com. **Lex** – Notas



técnicas da SENACON/ Ministério da Justiça e Segurança Pública, Brasília, 15 jun. 2018. Disponível em: <[https://www.cmlagoasanta.mg.gov.br/abrir\\_arquivo.aspx/PRATICAS\\_ABUSIVAS\\_DECOLARCOM?cdLocal=2&arquivo=%7BBBCA8E2AD-DBCA-866A-C8AA-BDC2BDEC3DAD%7D.pdf](https://www.cmlagoasanta.mg.gov.br/abrir_arquivo.aspx/PRATICAS_ABUSIVAS_DECOLARCOM?cdLocal=2&arquivo=%7BBBCA8E2AD-DBCA-866A-C8AA-BDC2BDEC3DAD%7D.pdf)>. Acesso em: 18 out. 2020.

\_\_\_\_\_. Averiguação preliminar. Suposto desvio de tráfego de internet para fins publicitários. Prática abusiva. Publicidade abusiva. Sugestão de instauração de processo administrativo. Nota Técnica n.º 108/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ. Processo Nº 08012.000723/2018-19. Representante: Departamento de Proteção e Defesa do Consumidor (Ex officio). Representado: Facebook Inc. e Facebook Serviços Online do Brasil Ltda. **Lex** - técnicas da SENACON/ Ministério da Justiça e Segurança Pública, Brasília, 11 mar. 2019. Disponível em: <[https://www.defesadoconsumidor.gov.br/images/Notas\\_T%C3%A9cnicas/Nota\\_T%C3%A9cnica\\_108.pdf](https://www.defesadoconsumidor.gov.br/images/Notas_T%C3%A9cnicas/Nota_T%C3%A9cnica_108.pdf)>. Acesso em: 19 out. 2020.

CANUT, Leticia; MEDEIROS, Heloísa Gomes. Os algoritmos nas relações de consumo eletrônicas: Análise do Direito do Consumidor à Informação. **XI Congresso de Direito de Autor e Interesse Público**, Curitiba, p. 1039-1061, 2017. Disponível em: <[http://www.gedai.com.br/wp-content/uploads/2018/04/xi-codaip-2017-gedai.pdf?fbclid=IwAR3YSUO\\_607WimhSo091bfvVKCpUShB0Nagdh\\_pOEet0vULvodtiCMm-ng8](http://www.gedai.com.br/wp-content/uploads/2018/04/xi-codaip-2017-gedai.pdf?fbclid=IwAR3YSUO_607WimhSo091bfvVKCpUShB0Nagdh_pOEet0vULvodtiCMm-ng8)>. Acesso em: 29 ago. 2020.

COMO os dados de milhões de usuários do Facebook foram usados na campanha de Trump. **BBC News Brasil**, 9 de abril de 2018. Disponível em: <<https://www.bbc.com/portuguese/geral-43705839>>. Acesso em: 09 set. 2020.

DE PIERRO, Bruno. Epidemia de fake news: Organização Mundial da Saúde chama atenção para grande circulação de notícias falsas sobre o novo coronavírus. **Revista Pesquisa FAPESP**, 7 abr. 2020. Disponível em: <https://revistapesquisa.fapesp.br/epidemia-de-fake-news/>. Acesso em: 9 set. 2020.

DONEDA, Danilo. **Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados**. 2ª ed. São Paulo: Editora Thomson Reuters Brasil, 2019

DUHIGG, Charles. How Companies Learn Your Secrets. **The New York Times**, Nova York, 16 de fevereiro de 2012. Disponível em: <[https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&\\_r=1&hp](https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp)>. Acesso em: 02 out. 2020.

ENTENDA o escândalo político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **BBC News**, 20 de março de 2018. Disponível em: <<https://www.bbc.com/portuguese/internacional-43461751>>. Acesso em: 20 out. 2020.

EUROPEAN DATA PROTECTION BOARD. Guidelines 05/2020 on consent under Regulation 2016/679, de 4 maio de 2020. Disponível em: <[https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679\\_pt](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt)>. Acesso em: 10 de out. de 2020.

FEIGELSON, Bruno; LEITE, Luiza. ANPD - Autoridade autoritária de dados. **JOTA**, Rio de Janeiro, 01 jan. 2019. Disponível em: <<https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/anpd-autoridade-autoritaria-de-dados-01012019>>. Acesso em: 08 ago. 2019.

FONTENELLE NETO, José Edilson Cunha. **O direito à proteção de dados pessoais (informatizados) enquanto direito fundamental autônomo**. 2019. 138 f. Dissertação (Mestrado em Ciência Jurídica) – Universidade do Vale do Itajaí, Santa Catarina, 2019.

GAVIOLI, Allan. E-commerce brasileiro fatura R\$ 61,9 bilhões em 2019, crescimento de 16,3% ante 2018. **InfoMoney**, 20 fev. 2020. Disponível em: <<https://www.infomoney.com.br/consumo/e-commerce-brasileiro-fatura-r-619-bilhoes-em-2019-crescimento-de-163-ante-2018/>>. Acesso em: 4 ago. 2020.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Parte Geral**. 10. ed. São Paulo: Saraiva, 2012. v. 1.

HARARI, Noah Yuval. **21 lições para o século 21**. São Paulo: Companhia das Letras, 2018.

MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). **Lei Geral de Proteção de Dados Comentada**. 2ª ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. 2008. 156 f. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2008.

\_\_\_\_\_. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. **Revista de Direito do Consumidor**. vol. 102. ano 24. p. 19-43. São Paulo: Ed. RT, nov/dez. 2015.

\_\_\_\_\_. **Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental**. Edição do Kindle. São Paulo: Editora Saraiva, 2014.

KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. **Marketing 4.0: Do tradicional ao digital**. Rio de Janeiro: Editora Sextante, 2017.

LUNARDI, Guilherme. 12 dados que comprovam o crescimento do e-commerce no Brasil. **E-Commerce Brasil**, 12 jun. 2018. Disponível em: <<https://www.ecommercebrasil.com.br/artigos/12-dados-que-comprovam-o-crescimento-do-e-commerce-no-brasil/>>. Acesso em: 4 ago. 2020.

MIRAGEM, Bruno. A Lei Geral de Proteção de dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais Online**, vol. 1009, novembro. 2019. Disponível em: <<http://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf>>. Acesso em: 20 ago. 2020.

NOJIRI, Sérgio. O direito à privacidade na era da informática algumas considerações. **Revista Jurídica UNIJUS**, Uberaba, v.8, nº 8, p. 99-106, maio/2005.

PRATES, Cristina Cantú. Privacidade e Intimidade na Internet: A legalidade dos Cookies e Spam. **Revista FMU Direito**, São Paulo, ano 28, n. 42, p. 29-45, 2014.

RAMER, Adam D. I.; GUILLORY, Jamie E.; HANCOCK, Jeffrey T. Experimental evidence of massive-scale emotional contagion through social networks. **PNAS**, California, p. 1-3, 17 jun. 2014. Disponível em: <<https://www.pnas.org/content/111/24/8788>>. Acesso em: 18 out. 2020.

SOPRANA, Paula. Comércio digital ganha 5,7 milhões de consumidores e varejo diz que eles vieram para ficar. **Folha de São de Paulo**, 22 jul. 2020. Disponível em: <<https://www1.folha.uol.com.br/mercado/2020/07/comercio-digital-ganha-57-milhoes-de-consumidores-e-varejo-diz-que-eles-vieram-para-ficar.shtml>>. Acesso em: 4 ago. 2020.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**. Rio de Janeiro, a. 9, n. 1, 2020. p. 5. Disponível em: <<http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/>>. Acesso: 9 set. 2020.

TORRES, Claudio. **A Bíblia do Marketing Digital**: tudo que você queria saber sobre marketing e publicidade na Internet e não tinha a quem perguntar. São Paulo: Novatec Editora, 2009.

VENTURA, Ivan. Geoblocking e geoprícing: os bastidores da disputa pelo turismo online no Brasil. **Consumidor Moderno**, 1 ago. 2018. Disponível em: <<https://www.consumidormoderno.com.br/2018/08/01/geoprícing-geoblocking-novo-desafio-consumidor/>>. Acesso em 09 set. 2020.