Comércio digital e proteção de dados: a era do Big Data

Digital trade and data protection: the age of Big Data

Giselle Borges Alves[*]
Rodrigo Teixeira de Souza[**]

Resumo: O desenvolvimento das relações de consumo em meios digitais estava crescendo nas últimas décadas, mas no último ano em decorrência da pandemia provocada pela Covid-19, observamos uma mudança paradigmática em todas as relações humanas com o uso da tecnologia. O Big Data, fenômeno muito estudado nas últimas décadas, ganha uma percepção maior diante da grande variedade de dados e informações que são diariamente deixadas por milhões de usuários da internet. Neste sentido, o estudo buscou analisar as mudanças desencadeadas nas relações de consumo, diante do intenso compartilhamento e coleta de dados, bem como verificar como a recente Lei Geral de Proteção Dados pode contribuir, juntamente com os demais diplomas normativos, para uma nova compreensão e o aprimoramento da defesa dos direitos básicos do consumidor e quais os desafios a serem enfrentados. Para tanto foram utilizados o método de raciocínio dedutivo e as técnicas de pesquisa bibliográfica e documental. Os resultados da pesquisa informam que a lei de proteção de dados brasileira, mesmo tendo aplicação subsidiária ao Código de Defesa do Consumidor, trouxe uma nova perspectiva sobre os direitos básicos, conferindo uma nova interpretação dos direitos à privacidade, igualdade nas contratações, oposição às práticas abusivas, bem como maior segurança nas relações comerciais.
Palavras-chave: proteção de dados, direito do consumidor, comércio eletrônico, big data.

Abstract: The development of consumer relations in digital media was growing in the last decades, but in the last year due to the pandemic caused by Covid-19, we observed a paradigmatic change in all human relations with the use of technology. The Big Data, a phenomenon that has been studied a lot in the last decades, gains a greater perception in view of the great variety of data and information that are left daily by millions of internet users. In this sense, the study sought to analyze the changes triggered in consumer relations, in face of the intense data sharing and collection, as well as verifying how the recent General Data Protection Law can contribute, together with the other normative diplomas, to a new understanding and the improvement of the defense of basic consumer rights and what are the challenges to be faced. For this purpose, the deductive reasoning method and bibliographic and documentary research techniques were used. The results of the research inform that the Brazilian data protection law, despite having subsidiary application to the Consumer Protection Code, brought a new perspective on basic rights, giving a new interpretation of the rights to privacy, equality in hiring, opposition to abusive practices, as well as greater security in commercial relations.
Keywords: data protection, consumer rights, e-commerce, big data.

Recebido em: 27/03/2021
Aprovado em: 29/03/2021

Como citar este artigo: ALVES, Giselle Borges; SOUZA, Rodrigo Teixeira de. Comércio digital e proteção de dados: a era do Big Data. Revista da Defensoria Pública do Distrito Federal, Brasília, vol. 3, n. 1, 2021, p. 99/122.

[*] Mestra em Direito pela Universidade de Brasília (UnB). Especialista lato sensu em Direito Processual Civil. Advogada inscrita na OAB/MG. Professora de cursos de graduação em Direito.

[**] Bacharel em Direito. Faculdade CNEC Unaí/MG.

Introdução

O crescimento do comércio eletrônico no Brasil foi sentido fortemente nos últimos anos, mas acentuado pelos últimos acontecimentos relacionados a pandemia de saúde pública advinda da COVID-19. Segundo o 42º Relatório *Webshoppers* divulgado pela Ebit, o faturamento do comércio eletrônico no primeiro semestre de 2020 foi 9% maior que no segundo semestre de 2019. Ao mesmo tempo o varejo *off line* cresceu os mesmos 13% do ano de 2019 (EBIT NIELSEN COMPANY, 2020).

Apenas no primeiro semestre de 2020, o varejo *on line* foi responsável por 38,8 bilhões em vendas. Enquanto no primeiro semestre de 2019, os valores de vendas *on line* ficaram no patamar de 26,4 bilhões. Assim, houve uma variação crescente de 47% nas vendas no *e-commerce* se comparado o primeiro semestre de 2019 e o primeiro semestre de 2020. Além disso, o comércio eletrônico em 2020 trouxe muitos consumidores que realizaram pela primeira vez compras *on line*. De acordo com os dados divulgados houve uma média de 38% de novos consumidores *on line*, o que gerou uma contribuição de 18% no crescimento do comércio eletrônico brasileiro no ano de 2020 (EBIT NIELSEN COMPANY, 2020).

Ainda de acordo com o Relatório, o crescimento se intensificou durante a pandemia com uma variação crescente de 57% no número médio de pedidos *on line* no primeiro semestre de 2020, sendo que apenas no mês de abril houve um pico de 77% de crescimento nos pedidos *on line*. O maior destaque foi para as regiões norte e nordeste do país que contribuíram com mais de um terço do crescimento das vendas *on line* no primeiro semestre de 2020 (EBIT NIELSEN COMPANY, 2020).

O Relatório também destaca a participação do *Marketplace*, ou seja, lojas *on line* que permitem a venda de produtos de lojas parceiras, sendo que durante o 1º semestre de 2020 os varejistas do *Marketplace* tiveram uma participação de 78% no faturamento total do *e-commerce*, o que representou uma média de R$ 30 bilhões em vendas, o que equivale a um percentual 56% maior frente ao mesmo período em 2019. Também houve uma crescente utilização de aplicativos de entrega, sendo que, segundo os dados divulgados, cerca de 72% dos consumidores nacionais começaram a utilizar ou estão utilizando mais aplicativos de *delivery* para não precisar sair de casa durante a pandemia (EBIT NIELSEN COMPANY, 2020).

Em um período de acentuadas transformações, temos, então, o crescente uso da internet para compras por meio de sites de venda, aplicativos e redes sociais *on line* (RSOs), e o consumidor

que pelas regras gerais possuía vulnerabilidade presumida, agora se vê diante de novas incertezas relacionadas não apenas ao comércio, mas aos dados que coloca à disposição e que produz durante a utilização dos recursos tecnológicos cada vez mais acessíveis. Se antes a vulnerabilidade estava na própria troca, relacionando-se a qualidade, quantidade, oferta, publicidade, características, prazos e preços, hoje o consumidor também precisa se preocupar com a segurança de dados expostos e na forma como estes dados são utilizados pelas próprias empresas, tanto fornecedores diretos de bens e serviços, como as empresas que atuam no setor de tecnologia que tratam os dados ofertando valor econômico.

Diante desse cenário, o Brasil viu entrar em vigor no mês de agosto de 2020, a Lei nº 13.709/2018, que promete ser um diploma diretamente relacionado à cidadania e garantia de direitos mínimos aos titulares de dados individuais, para uma nova era digital em expansão. Sob essa proposta, a partir da utilização do método de raciocínio dedutivo e das técnicas de pesquisa bibliográfica e documental, este estudo buscou averiguar quais os desafios da proteção do consumidor do *e-commerce* na era do Big Data e qual o papel da recente Lei Geral de Proteção de Dados brasileira nesse caminho que começamos a trilhar na proteção de direitos mínimos dos usuários das redes e consumidores.

1. A era digital e as transformações no comércio

A sociedade atual, marcada pela intercomunicação e a conectividade, difere substancialmente daquela existente há um século ou até mesmo poucos anos atrás. Conforme relata Kunsch (2007), a evolução trouxe profundas mudanças na sociedade com a saída do mundo analógico para o digital, gerando mudanças econômicas, sociais e políticas. Castells (2003) sinalizava em suas análises no início deste século, que estaríamos vivenciando uma sociedade em rede estruturada pela internet e que esta não seria apenas uma tecnologia, mas um meio de comunicação que organiza a sociedade, assim como foram as fábricas e as grandes corporações durante a Era Industrial[1].

E foram justamente as empresas que movimentaram o crescimento da utilização dos meios digitais, investindo em tecnologia tanto na produção de bens e serviços, como na comercialização destes. Foram elas que promoveram a expansão e disseminação das redes, popularizando a

[1] Neste sentido, Castells (2003, p. 287) já afirmava: "A internet é o coração de um novo paradigma sociotécnico, que constitui na realidade a base material de nossas vidas e de nossas formas de relação, de trabalho e de comunicação. O que a internet faz é processar a virtualidade e transformá-la em nossa realidade, constituindo a sociedade em rede, que é a sociedade em que vivemos".

comunicação com foco na lucratividade, através da economia informacional que passou a enxergar os sinais e os rastros deixados pelos usuários como *commodities* (CASTELLS, 2006). Rifikin (2016) ressalta que as empresas se viram pressionadas a buscar novas tecnologias para estimular a produtividade, diminuir preços e serem mais competitivas no mercado. Neste sentido, travaram guerras contra si mesmas, inclusive aquelas que atuavam em mercados monopolizados verificaram a necessidade de melhora da produtividade e redução de custos com o uso da tecnologia.

Em vista disso, as empresas migraram com o decorrer dos anos para o comércio *on line*, investindo inicialmente em publicidade e em coletas de dados a partir de pesquisas de mercado (LUCIANO; FREITAS, 2003). No entanto, com o avanço dos processos de comunicação, as empresas perceberam a necessidade de expandir o uso das redes e possibilitar novas formas de aquisição de bens e serviços pelos usuários (GALINARI et al., 2015). Destaca-se, assim, a consolidação do comércio por via eletrônica.

O comércio eletrônico (*e-commerce*) de acordo com Albertin (2000, p. 95) é "a realização de toda a cadeia de valores dos processos de negócio em um ambiente eletrônico, por meio da aplicação intensa das tecnologias de comunicação e de informação, atendendo aos objetivos do negócio". Neste sentido, para o autor esse processo pode ser realizado tanto de forma completa ou parcial, utilizando os meios digitais com uma infraestrutura de acesso fácil, livre e de baixo custo.

A utilização do *e-commerce* possui pontos positivos e negativos amplamente vivenciados pelos consumidores ao longo das últimas décadas. Conforme destaca Galinari et al. (2015) temos atualmente novos modelos de negócios que comercializam produtos digitais (*e-books*, músicas, filmes, imagens, base de dados, softwares), que diminuem custos com o transporte, a estocagem de mercadorias e representam, ainda, economia de capital humano devido a necessidade de menos funcionários e menor investimento em lojas físicas. Neste sentido, o *e-commerce* também gera impacto no mercado de trabalho, que observa novas transformações diante do surgimento de novas profissões e a diminuição na oferta de vagas em outras, o que gera também uma grande mudança de ordem social, conforme explica Galinari et al. (2015, p. 143):

> As perdas ou a desaceleração da criação de postos de trabalho tende a ocorrer em ocupações que geram um grande número de empregos, no entanto, relativamente mal remunerados – o que pode ser um problema para países que se encontram com altas taxas de desemprego, mas um benefício para os que necessitam liberar mão de obra para trabalhos mais qualificados. Os ganhos tendem a ocorrer em setores que geram menos postos de trabalho, mas que contratam pessoas com melhores níveis educacionais e que recebem salários relativamente altos, como analistas de sistemas, engenheiros e gestores.

Quando são analisados os pontos de vista dos clientes do *e-commerce*, verificamos que os aspectos positivos estão atrelados a uma maior e mais ampla oferta de produtos e serviços, maior comodidade na busca de bens com qualidade e preços competitivos sem a necessidade de saírem de suas residências, podendo, inclusive, adquirir produtos customizados e sob medida. Há também uma vasta quantidade de informações disponíveis na internet sobre os bens e serviços que se deseja adquirir e podem ajudar na tomada de decisão desde que as informações sejam realmente qualificadas. Conforme destaca Galinari et al. (2015), as ferramentas de busca e comparação de preços e produtos na internet, auxiliam o consumidor a partir da experiência de outros usuários e ofertam recursos que podem mitigar os efeitos negativos das transações realizadas a distância.

No entanto, os pontos negativos ou desvantajosos do comércio eletrônico não podem ser descartados, como a insegurança dos usuários-consumidores em relação ao recebimento do produto conforme condições estipuladas e a segurança dos sites de compra, notadamente quanto à disponibilização dos dados pessoais para empresas, tornando a privacidade de dados pessoais uma preocupação incipiente. Entretanto, no cenário atual a preocupação do uso de dados dos usuários deve ir além da disponibilização para as empresas do *e-commerce*.

Esse processo de desenvolvimento de relações comerciais e pessoais na internet, principalmente pelas redes sociais, fez surgir o interesse da utilização de megadados tanto para fins públicos de interesse coletivo, como para finalidades comerciais. Rifikin (2016), ao tratar do surgimento e utilização da Internet das Coisas[2], cita como exemplo a atual forma de gestão e administração dos ecossistemas terrestres, com a utilização de sensores para identificação de desastres como incêndios, erupções vulcânicas, movimentações no solo ou como meios de prevenção de danos ambientais. Também temos a utilização da internet das coisas como meio de monitorar tráfego em estradas e rodovias, entre outras aplicações.

> Somente nos Estados Unidos, 37 milhões de medidores digitais inteligentes fornecem informações sobre o uso de eletricidade. Dentro de dez anos, todo prédio ou casa nos Estados Unidos e na Europa, assim como em outros países do mundo, terá um medidor inteligente instalado. E cada dispositivo – termostato, linhas de montagem, equipamentos nos armazéns, TVs, lavadoras de roupa, computadores – terá sensores conectados a medidores inteligentes à plataforma da Internet das Coisas. Em 2007, havia 10 milhões de sensores conectando cada tipo de dispositivo humano à Internet das Coisas. Em 2013, estimou-se que este

[2] Rifikin (2016, p. 25) destaca que vivenciamos atualmente a internet das coisas que conecta tudo e todos em uma rede global que estimula a produtividade que ocorre por meio da conectividade e através do Big Data (megadados), que interliga empresas, lares, veículos, eletrodomésticos, entre outros produtos eletrônicos através de dados pessoais previamente cadastrados.

> número ultrapassaria os 3,5 bilhões e, mais impressionante ainda, em 2030 a projeção é que 100 trilhões de sensores estarão conectados à IdC (RIFIKIN, 2016, p. 93).

Assim, as ideias de Rifikin (2016) destacam que a Internet das Coisas está transformando o mundo em um único sistema operacional, aumentando a eficiência e a produtividade no gerenciamento de recursos e na distribuição de bens e serviços, tendo em vista que todas essas redes de informações estão interligadas de forma quase imperceptível ao cidadão comum, o que também gera desafios de ordem ética sobre a utilização econômica e discriminatória dos dados pessoais coletados.

O Big Data e os riscos à privacidade

Big Data é o conceito utilizado para descrever o grande volume de dados, estruturados ou não-estruturados, produzidos a cada segundo pelos usuários da internet e direcionados a criação de novos produtos e serviços através de um processo de marketing aprofundado a um determinado público-alvo. Esse processo de utilização de dados se relaciona ao cruzamento de informações disponibilizadas pelos potenciais consumidores através da internet e que são utilizadas como vantagens competitivas por fornecedores. As maiores fontes de dados utilizadas nesses processos são as redes sociais *on line* como Facebook, Twitter, Instagram, entre outras, em que há grande produção e coleta de dados utilizados com fins econômicos (NOVO; NEVES, 2013).

A extração ou mineração desses dados, apesar da complexidade da transformação em informações úteis, pode ser realizada nas mais diversas modalidades a partir de aparelhos conectados à internet, por meio de aplicativos, câmeras de segurança, usos de GPS, dados de voz, interações diversas realizadas pelos usuários e, até mesmo, dados de genoma de pesquisas biológica e medicinal, possibilitando grande variedade de informações sobre os indivíduos ou grupos de indivíduos, que após análise podem ser utilizadas em diversos segmentos de negócios (NOVO; NEVES, 2013).

Assim, o uso de dados traz grande diferencial competitivo no mercado uma vez que é possível identificar padrões de consumidores e hábitos de vida e consumo como gostos, formas de pagamento, satisfação ou insatisfação quanto ao produto ou serviço, inclusive, utilizando os dados coletados como forma de melhoria nos processos produtivos.

Neste sentido, é imperioso ainda diferenciar dado e informação. Veronese (2019, p. 386-387), de forma simples, afirma que o termo "dado" se relaciona a uma informação existente antes do tratamento, já o termo "informação" é o dado tratado e mensurado.

> O termo "dado" se refere a uma informação existente antes do seu tratamento. A legislação brasileira já vinha protegendo e regulando as informações pessoais. Assim, o inciso I do artigo 4º da Lei de Acesso à Informação (Lei 12.527/2011) definia que a informação seria composta de dados – tratados ou não – usados para produção ou para transmissão de conhecimentos. Essa definição jurídica é suficiente para explicar a proteção de dados. [...].
>
> A informação – nessa perspectiva – irá se referir aos dados tratados. Os dados são características dos objetos (documentos) – abstratos ou concretos – que, após a sua classificação (tratamento), dão origem às informações. A altura de uma pessoa, em si mesma, é um dado físico. Porém, uma vez que ela é mensurada, tornasse uma informação. [...] (VERONESE, 2019, p. 386 - 387).

Nesse processo o uso de algoritmos é a forma mais eficaz de minerar a grande quantidade dados e gerar informação a partir dos meios digitais, pois além de identificar dados relevantes, os algoritmos ainda estabelecem correspondências sobre esses dados e devolvem resultados potenciais a partir das funções descritiva ou preditiva, extraindo padrões úteis para antever comportamentos e até direcioná-los (REIS; NAVES, 2020).

Veronese (2019, p. 388-389) ainda destaca que diante a evolução tecnológica é necessária a proteção de dados brutos e não apenas das informações, como ocorria no passado: "Se a proteção for outorgada somente às informações, um vasto conjunto de dados – não classificados e não tratados – poderão estar desprotegidos. [...]". Diante deste cenário é cada vez mais incipiente o debate sobre o uso indevido de dados pessoais frente aos direitos de personalidade, notadamente o direito à privacidade.

> Riscos que envolvem a violação à privacidade e à personalidade dos cidadãos na sociedade da informação crescem exponencialmente, como a possibilidade de uso indevido dos dados pessoais, cadastro e classificação dos indivíduos, propagandas de marketing invasivas, publicidade comportamental, vigilância estatal, utilização indevida da Big Data, coleta de dados através da Internet das coisas, entre outros (FINKELSTEIN; FINKELSTEIN, 2019, p.285).

Sobre o direito à privacidade, o temos como uma garantia constitucional estabelecida no artigo 5º, inciso X da Constituição Federal de 1988, que informa a inviolabilidade da intimidade,

da vida privada, da honra e da imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988). Conforme ressaltado por Medina (2014), a Constituição Federal traz proteção à privacidade em dois níveis: vida privada e vida pública, uma oposta à outra. No que se refere a vida privada, temos como espécie o direito à intimidade, que conforme destaca o autor, são informações que se restringem "àquilo que é mais pessoal e reservado, a pensamentos, segredos, sentimentos e emoções que não são compartilhados ou são compartilhados apenas com aqueles com quem se mantém um relacionamento pessoal, normalmente afetivo" (MEDINA, 2014, p. 84).

Medina (2014, p. 85) também esclarece que a proteção à intimidade sofre limitações pela própria forma como o indivíduo utiliza suas informações. Neste sentido, se a pessoa utiliza informações íntimas em seu benefício, como na vida profissional, ela mesma "autolimita" a proteção à sua privacidade e intimidade, pois conforme relata o autor, tais atributos – características e qualidades pessoais – passam a integrar "o rol de qualidades relacionadas ao papel social exercido pela pessoa".[3]

Assim, a Constituição Federal de 1988 confere proteção para ambos os direitos, privacidade e intimidade, o último decorrente do primeiro. No entanto, atualmente a discussão sobre as limitações do uso de dados individuais expostos pelos usuários nas redes e diversas plataformas digitais, bem como as formas de utilização destes dados é sobressalente, diante dos níveis de imposição de coleta de dados que as empresas de tecnologia e até entidades públicas fazem aos usuários, coletando dados, inclusive, sem que os indivíduos tenham dimensão da forma e extensão da sua utilização. Rifikin (2016) é um dos autores que assinala, inclusive, que deverá ser observada a evolução do pensamento das gerações futuras sobre a importância das noções de privacidade e liberdade, bem como os direitos e limitações inerentes.

Facchini Neto e Demoliner (2019) destacam a necessária mudança de compreensão no conceito de privacidade. Para eles, a privacidade atualmente não pode ser compreendida como no passado, com limites conceituais tão estreitos, tendo em vista que os direitos da personalidade não se restringem à esfera material. Conforme ressaltam, muitas vezes, sequer conseguimos identificar quando fomos invadidos e quem são os invasores e ofensores de nossa esfera privada, e mesmo quando são identificáveis, as pessoas ficam dependentes de autorizações judiciais para evidenciar buscas e investigações tendentes a indicar os reais autores.

[3] No mesmo sentido Facchini Neto e Demoliner (2019, p. 125), na medida em que informam que a vida privada "[...] substancialmente envolve sua autonomia e liberdade para conduzir sua vida.[...]" e intimidade "[...] envolve um direito de autodeterminação".

Assim, a intimidade como direito de autodeterminação é defendida por Facchini Neto e Demoliner (2019, p. 137), sendo que a autodeterminação deve ser entendida hoje como "autodeterminação informativa", ou seja, o direito individual de decidir sobre o fornecimento dos dados e "a possibilidade de impedir que venham ser utilizados de forma incorreta ou para fins diversos daqueles para os quais foram coletados". A autodeterminação informativa compreende, ainda, conforme os autores, o direito de correção dos dados equivocados e a exclusão do armazenamento uma vez cumprida a finalidade ou atingido o tempo previsto de utilização.

Diante de todas essas transformações relativas as novas formas de exposição das características individuais e informações pessoais coletadas e de ter ficado evidenciada a necessária intervenção regulatória estatal sobre a coleta e uso de dados pessoais, nos últimos anos diversos ordenamentos jurídicos passaram a estabelecer novos regramentos para a proteção dos indivíduos-usuários, muitas vezes reiterando direitos mínimos de dignidade humana adaptados à Era Digital.

2. Aspectos regulatórios da proteção de dados no Brasil

Em vista das mudanças no cotidiano das pessoas, promovidas pelo uso intenso das tecnologias disponíveis e cada vez mais avançadas, é necessário pensar nos processos regulatórios que cercam a utilização de dados de consumidores e usuários.

Na Europa a proteção de dados pessoais remonta da Lei de Informática e Liberdades (*Loi de l'informatique et des libertés*), editada em 1978, que estabelecia o direito dos cidadãos franceses de solicitar explicação e de realizar oposição sobre decisões automatizadas (VERONESE, 2019). Ainda no cenário europeu podemos citar outras normas que tratavam da proteção de dados pessoais, como a Diretiva 95/45/CE do Parlamento Europeu e do Conselho, existente desde 24 de outubro de 1995 e posteriormente revogada pelo Regulamento Geral de Proteção de Dados (RGPD) – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, sendo estas apenas algumas das regulações existentes sobre o tema[4].

Nos Estados Unidos da América (EUA), conforme destaca Bessa (2012), a proteção de dados pessoais difere do sistema europeu porque não temos a figura de uma lei geral. As leis setoriais são prevalecentes e também não existe uma obrigatoriedade de ter uma autoridade

[4] Sobre a proteção de dados na União Europeia recomendamos a leitura do texto "Os direitos de explicação e de oposição frente às decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira", de Alexandre Veronese (2019, pp. 385-415).

específica para controlar empresas e entidades que realizam a coleta e o tratamento de dados pessoais. Na Europa, a existência de uma autoridade ou órgão é obrigatória desde a Diretiva 95/46/CE e deve ser constituída por cada país membro da União Europeia.

Nos EUA, em razão das leis serem setoriais, muitas vezes a proteção se evidencia de forma inconsistente, mas podemos citar como exemplo de legislação de proteção de dados o *Fair Credit Reporting Act* (FCRA), criado na década de 1970 para disciplinar os dados no mercado de crédito e que inspirou o artigo 43 do Código de Defesa do Consumidor brasileiro (BESSA, 2012). Posteriormente, tivemos a edição de inúmeras leis setoriais e estratificadas pelos Estados americanos, relacionadas a proteção de dados individuais. Em 2008, a *Biometric Information Privaccy Act* (Illinois, EUA) foi a primeira lei a regular a coleta e tratamento de dados biométricos nos EUA, trazendo exigências de informação, consentimento, proibição de transações, entre outras obrigações para as empresas que atuassem no setor em Illinois. Posteriormente, Washington (EUA) também regulou a coleta de dados biométricos, em 2018, com a edição da *HB 1493*, e o Estado do Texas trouxe a *Texas Business and Commerce Code – BUS & COM §503.001 Capture or Use of Biometric Indentifier* (BIONI; LUCIANO, 2019)[5].

No Brasil a doutrina tem destacado a fragmentação da atuação legislativa em matéria de proteção de dados (SOUZA; SILVA, 2019). Tivemos ao longo dos anos uma vasta produção legislativa que de alguma forma tentava proteger os dados e informações individuais privadas dos cidadãos brasileiros. Além da própria Constituição Federal de 1988, temos o Código de Defesa do Consumidor, a Lei do *Habeas Data*, o Código Civil, a recente Lei do Cadastro Positivo, a Lei de Acesso à Informação, entre outros diplomas, os quais passaremos a tratar dos aspectos básicos relacionados a proteção de dados e informações.

O Código de Defesa do Consumidor (Lei nº 8.078/1990), por exemplo, traz a proteção do consumidor frente aos bancos de dados e cadastros, conforme disciplina estabelecida na Seção VI, artigos 43 e 44, sendo esta tutela de importância reconhecida como primordial por grande parte da doutrina consumerista. Bessa (2012) é um dos autores que sempre afirmou essa necessidade de regulação sobre os arquivos de consumo, diante da ameaça à privacidade e honra das pessoas.

[5] Muitas outras normas setoriais podem ser verificadas no cenário norte-americano, tratando, por exemplo da regulação do reconhecimento facial e da aplicação sobre novos usos de tecnologias. Recomenda-se a leitura do texto de Bruno Ricardo Bioni e Maria Luciano, intitulado "O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada?", que trata da possibilidade do uso do princípio da precaução, comum no direito ambiental, para tutelar o uso da inteligência artificial. Os autores tratam das diversas normas norte-americanas, bem como do cenário de proteção europeu e fazem uma comparação com a recente lei geral de proteção de dados brasileira.

No entanto, a norma consumerista realiza a tutela sobre bancos de dados e cadastros sem diferenciá-los e, conforme ressalta Bessa (2012), a diferenciação apenas ocorreu por meio da doutrina formulada pelo Ministro do Superior Tribunal de Justiça, Antônio Herman V. Benjamin, que destacou em seus escritos e julgados que a distinção entre os bancos ocorre em razão da origem e do destino da informação. Pela formulação estabelecida, nos cadastros é o próprio consumidor que oferece os dados pessoais ao fornecedor. Assim, quem fornece o dado e a quem se destina o dado são conhecidos por ambas as partes. No entanto, nos bancos de dados as informações são em geral fornecidas pelos fornecedores e o destinatário final é o mercado. Portanto, há um grau de incerteza e vulnerabilidade maior dos dados dos consumidores quando inseridos em bancos de dados, principalmente quanto ao uso e aplicação dessas informações.

> Os bancos de dados, genericamente falando, podem possuir propósitos absolutamente diversos, que vão desde a obtenção de informações para fins históricos, estatísticos, passando pelos arquivos de proteção ao crédito, até aqueles que coletam informações úteis para as companhias seguradoras. Os bancos de dados de consumo são aqueles cujas informações são importantes para o mercado de consumo (BESSA, 2012, p. 295).

Assim, o Código de Defesa do Consumidor cumpriu papel preponderante no início dos anos 1990, diante da acentuada abertura comercial e o início do processo de globalização da economia brasileira. Ao longo dos anos, com o avanço dos meios e formas de negociação, o que acabou também ampliando a vulnerabilidade do consumidor frente ao poder do fornecedor de utilizar de forma incorreta e abusiva as informações e dados dos quais dispunha em seus bancos de dados e cadastros, o Código de Defesa do Consumidor se revelou como instrumento essencial de proteção da esfera íntima do cidadão.

A Lei do *Habeas Data* (Lei nº 9.507/1996) também foi um dos diplomas legais destinado a proteção de dados e informações dos indivíduos, entretanto, conforme ressaltado por Veronese (2019), a norma definiu de forma ambígua o que seriam dados e informações, mas a imprecisão não causou grandes problemas na efetivação de seus comandos. A Lei do *Habeas Data* tem como foco os dados públicos, o direito de acesso e de retificação desses dados pelos cidadãos.

A Lei do Cadastro Positivo (Lei nº 12.414/2011, com modificações substanciais realizadas pela Lei Complementar nº 166/2019), foi outra norma que veio disciplinar a formação e consulta aos bancos de dados com informação de adimplemento de contratos de consumo, estabelecendo, conforme destaca Bessa (2012, p. 293), um "forte diálogo com o Código de Defesa do Consumidor", pois a norma prevê a possibilidade de existência de um banco de dados com

histórico de crédito do consumidor, muito similar ao tradicional banco de dados de informações negativas, mas com uma diferença básica: ao invés de conter apenas a informação de inadimplemento, comum nos cadastros negativos, agora o fornecedor possui informações completas do consumidor no mercado[6].

Ainda no ano de 2011, foi promulgada a Lei de Acesso à Informação (Lei nº 12.527/2011) aplicada aos entes públicos, regulamentando o artigo 5º, inciso XXXIII da CF/1988. Em 2012, tivemos a edição de lei que tipificou os delitos informáticos, a Lei nº 12.737/2012, inserindo o crime de invasão de dispositivo informático no Código Penal brasileiro, acrescendo os artigos 154-A e 154-B, sancionando, assim, a divulgação de dados e imagens pessoais.

No entanto, foi em 2014, com a promulgação do Marco Civil da Internet (Lei nº 12.965/2014), que tivemos pela primeira vez uma norma voltada a regular o ambiente digital. De acordo com Souza e Silva (2019, p. 244), ainda uma proteção deficitária, na medida em que "substituiu o sistema de *notice and take down* que até então era aplicado pela jurisprudência a hipóteses semelhantes"[7].

Entretanto Finkelstein e Finkelstein (2019, p. 292), destacam que o Marco Civil da Internet, trouxe importantes dispositivos destinados a proteção da confidencialidade, à inviolabilidade da vida privada e aos fluxos de tráfego da internet. De acordo com os autores, a norma "além de garantir que a guarda e disponibilização de registros de conexão e de acesso a aplicações a internet", impôs a necessidade de resguardar a honra, a imagem e a intimidade dos usuários, na medida em que há necessidade de consentimento expresso para o armazenamento e tratamento dos dados pessoais, conforme estabelecido pelo artigo 7º, inciso IX da norma[8].

Assim, o Marco Civil da Internet foi a primeira norma que veio para preparar os aspectos regulatórios, com a construção de direitos civis para que, posteriormente, fosse criada uma proteção mais efetiva aos dados individuais (LEMOS, 2014). A Lei nº 12.965/2014 trouxe diretrizes e princípios destinados também a delimitar a livre-iniciativa e livre-concorrência também nas relações de consumo, mesmo não tratando diretamente destas, pois soma-se às demais

[6] Sobre o tratamento de dados para formação de cadastros de crédito, recomenda-se a leitura do texto "Tratamento de dados para a concessão de crédito", de Milena Donato Oliva e Francisco de Assis Viégas.

[7] A expressão em inglês, significa em tradução livre "aviso e retirada", onde a breve comunicação ou notificação era suficiente para que fosse retirado do conteúdo *on line*, o ilícito. Prática comum no direito americano em situações de aferição de responsabilidade dos provedores de internet (BOECHAT, 2012).

[8] "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] X - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; [...]" (BRASIL, 2014).

normas existentes para reforçar os direitos previstos no Código de Defesa do Consumidor, agora sobre os contratos celebrados em meios digitais (MARQUES; KLEE, 2014).

No entanto, em 14 de agosto de 2018, foi sancionada a Lei nº 13.709, denominada de Lei Geral de Proteção de Dados Pessoais – LGPD, que apenas entrou em vigor em agosto de 2020. Ainda em 2018, através da Medida Provisória nº 869/2018, foi estabelecida a criação da Autoridade Nacional de Proteção de Dados, órgão responsável por zelar pela aplicação da LGPD[9]. Assim, a forma como foi consagrada a proteção de dados no Brasil é muito similar as normas europeias, centralizando em um ente específico o poder de aplicar a norma administrativamente, bem como impor diretrizes para regulamentar a lei geral.

A Lei nº 13.709/2018 foi criada, portanto, com o objetivo de proteger e resguardar os direitos à privacidade e liberdade dos usuários sobre o armazenamento do fluxo de informações que produzem no meio digital, sendo aplicável tanto para os setores públicos como privados, estabelecendo diretrizes e penalidades para quem descumprir seus comandos.

Os direitos dos indivíduos consumidores

De forma antecedente, ressaltamos a função que o Código de Defesa do Consumidor exerceu como a primeira norma infraconstitucional voltada aos arquivos com dados pessoais de consumidores, através da regulação em caráter geral sobre bancos de dados e cadastros. Essa importância ocorreu, sobretudo, após a pulverização de bancos de dados de proteção ao crédito administrados por entidades que tem por objetivo não apenas a coleta e armazenagem, mas que realizam o compartilhamento de dados com terceiros interessados em saber sobre a análise de crédito de determinado consumidor, o que é feito pelo próprio histórico existente dentro destes bancos de dados alimentados por milhares de fornecedores[10].

A análise da jurisprudência ao longo das décadas posteriores, relacionada aos direitos individuais de consumidores frente a estes bancos de dados e cadastros, traz a dimensão de como essa regulação foi importante para o enfrentamento de abusos provocados tanto pelas entidades que administram esses bancos, como por fornecedores que inserem os dados e utilizam dados

[9] Toda a organização e estrutura da Autoridade Nacional de Proteção de Dados (ANPD) está contida no Decreto nº 10.474 de 26 de agosto de 2020 e seus anexos. Para mais informações sobre a atuação da ANPD, recomenda-se o acesso ao site governamental da entidade: <https://www.gov.br/anpd/pt-br>.

[10] Bessa (2012, p. 298) destaca que os bancos de dados de proteção ao crédito, como SPC, SERASA, entre outros, obtém informações fornecidas pelo comércio, mas também realizam permuta de informações com outros bancos de dados, pois existem algumas entidades que, por exemplo, coletam por iniciativa própria, informações de cartórios de distribuição de ações e de protesto de títulos.

expostos por terceiros[11]. Conforme destaca Bessa (2012), o CDC consagrou os direitos de acesso, retificação e comunicação ao consumidor sobre os dados existentes nos bancos de dados e cadastros, o que foi repetido pela Lei nº 12.414/2011 quando tratou da regulação sobre cadastro positivo.

Com o advento da LGPD, em vigor desde agosto de 2020, temos uma nova perspectiva de proteção de dados dos consumidores, agora para além dos bancos de dados e cadastros, mas sem descuidar destes[12]. Emerge uma proteção que também vai além da proteção da honra, privacidade e intimidade das pessoas, fortalecendo os direitos mínimos dos consumidores, insculpidos no artigo 6º do Código de Defesa do Consumidor, ofertando a eles novas dimensões de proteção e garantia.

Neste sentido, direitos básicos como o direito à segurança contra riscos provocados por práticas no fornecimento de produtos e serviços (inciso I, art. 6º), assume agora o direito à segurança dos dados individuais fornecidos, diante do evidente risco que representa a ausência de medidas efetivas para o resguardo dessas informações. Também engloba a verificação da dimensão atual do direito à liberdade de escolha e igualdade de contratação (inciso II e IV do art. 6º), combatendo práticas discriminatórias ou marketing abusivo por meio da coleta de dados, bem como o direito à informação completa sobre como os dados disponíveis estão sendo utilizados e o direito ao ressarcimento ou indenização na medida em que o uso dos dados individuais pelos fornecedores, provocarem prejuízos aos consumidores (inciso VI do art. 6º).

A respeito das práticas discriminatórias realizadas por meio da coleta de dados dos consumidores, podemos citar, exemplificativamente, o *geo-pricing* e o *geo-blocking*, que vem sendo investigadas e sancionadas pelos órgãos nacionais de defesa do consumidor, antes mesmo da entrada em vigor da LGPD, com fundamento em normas consumeristas e em prática de concorrência desleal (FRAZÃO, 2018). Em termos simples, o *geo-pricing* trata da discriminação de preços conforme a localização do consumidor-usuário e o *geo-blocking* trata da discriminação pelo próprio bloqueio de ofertas, conforme a região em que o consumidor-usuário reside. A prática de diferenciações de preço entre consumidores, fundada em aspectos meramente subjetivos, é

[11]Diversas súmulas foram editadas pelo STJ tratando dos bancos de dados e cadastros, podemos citar, exemplificativamente, as súmulas 323, 385, 404 e 548. Assim, como inúmeros julgados também tratam do tema de inserção de dados de consumidores em bancos de dados e cadastros negativos, tais quais o AgRg no Ag 959.364/DF (Relator Min. Humberto Gomes de Barros) e o REsp 442.483/RS (Relator Min. Barros Monteiro).

[12] Neste sentido, Oliva e Viégas (2019, p. 580-585) destacam que a LGPD veio para reforçar a proteção conferida pela Lei nº 12.414/2011 e pelo Código de Defesa do Consumidor, corroborando a necessidade de consentimento – mesmo, em alguma medida, disciplinando hipóteses de dispensa deste no art. 7º –, amplo acesso aos dados pelos consumidores e a exigência de transparência no uso destes dados, destacando os princípios da finalidade, adequação e necessidade do tratamento.

vedada pelo Código de Defesa Consumidor, no entanto, muitos consumidores não sabem que podem estar sendo vítimas de práticas discriminatórias de preços e ofertas de produtos e serviços apenas pela identificação do bairro, cidade ou região em que residem. Trata-se, conforme pontua Dias et al. (2020, p. 1916), de "uma relação assimétrica entre as plataformas digitais e os usuários", uma prática desleal, em que o poder de barganha é diminuído e os consumidores passam a acreditar que o preço informado pela plataforma é o preço real de mercado[13].

> Do ponto de vista consumerista, o controle de conteúdo consubstanciado nas práticas de *geo-blocking* e *geo-pricing* pode ser considerado abusivo. Isso porque esse controle pode representar uma ofensa à isonomia e à não-discriminação, já que o consumidor se encontra em posição manifestamente desigual nas plataformas em rede. Com efeito, as práticas podem possibilitar a criação de grupos de consumidores favorecidos em prejuízo de outros a depender de sua localização geográfica (DIAS et al., 2020, p. 1921).

Neste sentido, é preciso averiguar em que medida a LGPD poderá tutelar o consumidor, frente às práticas abusivas de mercado, baseadas na coleta de dados, como o *geo-pricing* e o *geo-blocking*, já que o referido diploma deverá ter aplicação subsidiária ao CDC para possibilitar maior proteção e defesa dos direitos do consumidor. Em alguma medida, às agências reguladoras de cada setor, a Autoridade Nacional de Proteção de Dados e demais órgãos públicos, deverão atuar de forma coordenada com a finalidade de coibir e sancionar adequadamente os abusos.

Outro aspecto importante sobre a LGPD em relação ao mercado de consumo é o fato de que, ao contrário do que possa parecer, a norma não realiza tutela dos dados individuais apenas para os usuários da internet. No seu artigo 1º, a norma deixa evidente que a proteção conferida ocorre sobre o tratamento dos dados "inclusive nos meios digitais" (BRASIL, 2018)[14]. Assim, não existe uma limitação de efeitos da LGDP aos dados provenientes da realidade virtual ou digital, conforme é ressaltado por Finkelstein e Finkelstein (2019), tendo em vista que a norma se aplica a qualquer meio de coleta e tratamento de dados, seja em armazenamento físico ou digital, com ou sem acesso à internet. Portanto, a LGPD é plenamente aplicável aos bancos de dados e aos

[13] Em 2018, a empresa *Decolar.com* teve que responder ação civil pública, ajuizada pelo Ministério Público do Rio de Janeiro, em que se apurava prática desleal ao consumidor e à livre concorrência em razão da discriminação por localização geográfica no mercado de turismo (DIAS et.al, 2020). Além disso, o Departamento de Proteção e Defesa do Consumidor da Secretaria Nacional de Relações de Consumo do Ministério da Justiça, em agosto de 2018, aplicou à Decolar.com uma multa de 7,5 milhões de reais pela prática de discriminação de preços aos consumidores (*geopricing*) ou pela negativa de ofertas (*geoblocking*) (FRAZÃO, 2018).

[14] "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".

cadastros de consumidores existentes de forma *on line* ou *off line*, sejam em entidades públicas ou privadas, de proteção ao crédito (cadastro negativo) ou de histórico de crédito (cadastro positivo), e sobre cadastros de consumidores de qualquer fornecedor de produtos ou serviços. A LGPD, assim, se transforma em outro grande instrumento de proteção aos direitos individuais dos consumidores neste século XXI.

Finkelstein e Finkelstein (2019) ressaltam uma outra potencialidade da norma: a sua perspectiva de aplicação transnacional (extraterritorialidade). Mesmo que os dados não sejam de brasileiros, mas coletados em âmbito nacional, poderão sofrer consequências da aplicação da LGPD, tendo em vista que o artigo 3º[15] afirma a possibilidade de tutela sobre operações de tratamento realizadas em território nacional, à exemplo de tratamento com o objetivo de troca comercial no Brasil ou se os indivíduos fornecedores ou receptores dos dados estiverem no Brasil. A importância deste dispositivo se revela diante da grandeza que assume o *e-commerce* em escala mundial e também pela constante utilização de redes sociais e sites pelo público brasileiro, pertencentes a empresas de tecnologia que realizam a coleta de dados no Brasil, mas que não possuem sede em território nacional.

Outro assunto que emerge a partir da LGPD – no entanto, antecedente à esta e um dos argumentos para sua existência – é a comercialização dos dados coletados. Um dos pontos centrais de discussão sempre foi a possibilidade ou não de empresas que coletam dados poderem comercializá-los para outras empresas ou entidades para as mais diversas finalidades. A LGPD surge em resposta a esta necessidade de proteção, conforme destacam Finkelstein e Finkelstein (2019), que salientam a discordância sobre a comercialização ou compartilhamento de dados coletados para empresas ou entidades que não estão coligadas à empresa que os coletou, diante da agressão à privacidade dos usuários. Ainda acerca da impossibilidade de monetização de dados pessoais e do tratamento como *commodities*, é importante trazer as considerações de Frazão (2019, p. 103), que destaca:

> [...] a LGPD pode, igualmente, ser vista como um freio e um agente transformador das técnicas atualmente utilizadas pelo capitalismo de vigilância, a fim de conter a maciça extração de dados e as diversas aplicações e utilizações

[15]"Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei".

> que a eles podem ser dadas sem a ciência ou o consentimento informado dos usuários.
>
> Tal aspecto é fundamental para a compreensão da LGPD, porque os valores e objetivos por ela reconhecidos representam um importante contraponto à tendência de monetização dos dados, considerando-os como commodities e objeto de livre-extração ou negociação. De forma contrária, os princípios da LGPD mostram que dados pessoais não são meros bens de cunho patrimonial, o que revela a insuficiência das soluções de mercado para qualquer disposição a respeito deles.

Conforme é possível verificar a LGPD assume uma complementaridade central na defesa do consumidor diante do avanço da tecnologia e da atual vulnerabilidade digital da grande maioria dos consumidores que realizam transações comerciais pela internet. Frazão (2019, p. 112), inclusive, destaca que os agentes econômicos "não mais trabalham com a perspectiva de incerteza ou mesmo de risco".

Existe uma concentração de conhecimento sobre gostos, forma de vida, padrões de consumo, preferências, que levam algumas empresas a deterem mais informações sobre os consumidores do que estes mesmos podem prever e essa assimetria informacional leva não apenas o consumidor ser subjugado e, de certa forma, dominado pelas práticas mercadológicas, mas também faz com que outros potenciais concorrentes aos *players* do mercado, não detenham o mesmo acesso às informações e fiquem fora da disputa em termos concorrenciais. O prejuízo pela coleta e tratamento indiscriminado de dados ocorre tanto a nível de consumo, como a nível concorrencial, o que atrai um prejuízo concreto para todos os agentes do mercado.[16]

3. O que esperar da LGPD

Em uma sociedade em que o dado e a informação por este produzida são vistos como produtos em escala comercial, a LGPD representa um esforço inicial e necessário para adequar as condutas que não são compatíveis com padrões mínimos de sociabilidade e de observância dos direitos fundamentais. Entra em vigor com o objetivo de estabelecer direitos mínimos de acesso e transparência como pilares normativos, posto que, conforme destacado por Monteiro Filho e Castro (2019, p. 325-331), o acesso aos dados é atualmente uma "*pedra angular para a proteção das informações pessoais*". Neste sentido, a proteção estabelecida pela norma abrange não apenas

[16] Neste sentido destaca Frazão (2019, p. 115): "As modificações recentes promovidas pelo Big Data mostram como o poder econômico, hoje associado ao poder da informação, da comunicação e mesmo ao poder político, apresenta riscos e custos ainda maiores para a preservação da competição nos mercados e para assegurar a liberdade econômica de todos os agentes envolvidos".

o acesso aos dados brutos, mas também o direito à informação sobre a forma de tratamento e de circulação das informações do indivíduo.

No entanto, percebe-se que a LGPD está longe de representar consenso doutrinário – o que em termos jurídicos é praticamente inalcançável –, principalmente em razão da vagueza de alguns conceitos e institutos[17]. Souza e Silva (2019, p. 261) afirmam que a LGPD "revela mais uma declaração de intenções" quando oferta protagonismo a concepção atual de privacidade, mas que a lei não traz uma "mudança efetiva na atribuição de direitos à pessoa humana", o que já estaria consagrado na cláusula geral da dignidade da pessoa humana e nas garantias e direitos fundamentais tratados pela Constituição Federal de 1988[18].

Entretanto, apesar dos posicionamentos expostos, compreendemos que a LGPD representa no cenário atual de consumo, uma possibilidade de buscar proteção mais ampla dos direitos já consagrados na norma geral consumerista. É uma importante salvaguarda frente às profundas mudanças nas relações comerciais que vivenciamos e de necessidade de aprimoramento de alguns institutos jurídicos. Consagra, conforme destacado por Monteiro Filho e Castro (2019, p. 326), uma nova perspectiva sobre o direito à privacidade, saindo de uma visão cunhada no dever que se assemelhava um direito de propriedade e passa a consagrar um direito de controle e titularidade em aspecto extrapatrimonial, controlando a manipulação, a coleta e o uso para finalidades legítimas.

Neste sentido, a LGPD aprimora a proteção sobre os dados mais recônditos do consumidor e dos usuários em geral de meios eletrônicos, pois traz a definição e exemplificação dos dados sensíveis sobre sua tutela.

> Os dados denominados sensíveis representam espécie de dado pessoal e se encontram presentes em todos os conjuntos informacionais do ser humano. Na LGPD, entendeu o legislador que a melhor forma de os proteger seria trazendo exemplos claros de dados assim considerados. Portanto, dados sensíveis versão sobre origem racial ou étnica, convicção religiosa, opinião política e filiação a

[17] Podemos citar como exemplo a discussão sobre qual espécie de responsabilidade é preponderante na LGPD, se subjetiva ou objetiva, tendo em vista que ainda não existe um consenso doutrinário a respeito, diante da vagueza da norma. Neste sentido, Capanema (2020) sustenta que a responsabilidade prevista na LGPD é de natureza objetiva, onde não há necessidade de averiguação do requisito de culpabilidade do agente. Em sentido contrário, Guedes e Meirelles (2019) sustentam a posição de incidência da responsabilidade subjetiva do agente, sendo necessária a perquirição sobre culpa.

[18] Os autores, ainda, destacam que da leitura do artigo 18, não se infere qualquer inovação "na medida em que apenas reproduz conteúdos que já eram atribuídos de longa data ao direito à privacidade" e que o dispositivo apenas traz "medidas e procedimentos que podem ser utilizados pelo titular de dados ou que devem ser implementados pelo agente de tratamento, com vistas a efetivar a tutela da privacidade e, mais do que isso, mensurar a extensão da tutela desse direito". Na visão dos autores, trata-se da simples exposição de "remédios para tutela da privacidade" (SOUZA E SILVA, 2019, p. 264).

> sindicato ou a organização de caráter religioso, filosófico ou político. São também sensíveis aqueles referentes à saúde ou à vida social e dados genéticos ou biométricos.
>
> Essa categoria integra o chamado 'núcleo duro' da privacidade, tendo em vista que, pelo tipo e natureza de informação que traz, ela apresenta dados cujo tratamento pode ensejar a discriminação de seu titular, devendo, por conseguinte, ser protegidos de forma mais rígida. Cuida-se de dados especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, cujo contexto propicia riscos significativos para o titular (TEPEDINO; TEFFÉ, 2019, pp. 306-307).

A proteção mais abrangente sobre os dados sensíveis, traça o próprio limite objetivo dos direitos fundamentais, conforme visão de Ruaro e Glitz (2019, p. 353), uma vez que a dignidade humana representa a vedação à instrumentalização do indivíduo e sua objetificação para finalidades coletivas:

> A eficácia dos direitos fundamentais, tanto nas relações públicas quanto privadas, atua como limite objetivo. O conteúdo da dignidade enuncia a compreensão de que o indivíduo é um fim em si mesmo, vedando-se a sua instrumentalização, o qual não pode ser tratado como meio para a consecução de objetivos ou metas de natureza coletiva.

Portanto, sob a perspectiva do diálogo das fontes que, conforme destaca Marques (2012), consagra uma eficiência funcional do sistema jurídico contemporâneo, marcado, sobretudo, pela pluralidade e complexidade, as normas de proteção de dados quando avaliadas sobre a ótica da defesa dos direitos individuais dos consumidores devem promover um diálogo conciliador e não excludente[19]. Assim, o objetivo do legislador não foi inovar na órbita jurídica sobre os institutos da privacidade, intimidade e sobre as responsabilidades inerentes a cada área de apuração de conduta, mas tão somente, possibilitar que diante dos avanços tecnológicos e do desconhecimento ou assimetria informacional dos usuários, incluindo os consumidores, estes tivessem o reconhecimento do direito a não ter seus dados utilizados de forma prejudicial a si ou à coletividade com ele integrada, bem como o direito de serem informados e de se reportar quanto à manutenção e guarda dos seus dados pessoais por qualquer agente, sem consentimento.

[19] Sobre a expressão "diálogo das fontes", cunhada por Erik Jayme, Marques (2012, p. 118) ressalta a amplitude de seu significado atualmente: " 'Diálogo' porque há influências recíprocas, 'diálogo' porque há aplicação conjunta das duas normas ao mesmo tempo e ao mesmo caso, seja complementarmente, seja subsidiariamente, seja permitindo a opção pela fonte prevalecente ou mesmo permitindo uma opção por uma das leis em conflito abstrato – uma solução flexível e aberta, de interpretação, ou mesmo a solução mais favorável ao mais fraco da relação (tratamento diferente dos diferentes)".

Nesta esteira, conforme destaca Frazão (2019, p. 108), não se pode olvidar que a proteção de dados pessoais também envolve uma proteção à cidadania e a própria democracia, uma vez que "o conhecimento excessivo que alguns agentes possuem dos titulares de dados pode ser utilizado para todo tipo de manipulação, inclusive para efeitos políticos". Assim, a proteção de dados extrapola os limites individuais e possui eficácia coletiva e, neste sentido, segue a importância de que a lei geral possa representar além de uma expectativa, a possibilidade de soluções concretas inviabilizando abusos à direitos fundamentais e expandido para os aspectos de soberania estatal sobre os dados dos seus cidadãos.

Portanto, o que se deve esperar da LGPD é um diploma conciliador de expectativas e direcionador das atividades realizadas por entes públicos e privados. Trata-se de um início bem-vindo para uma abertura interpretativa de institutos jurídicos, para além de uma eficácia meramente privada, apesar de não se descurar desta. Ao longo dos anos será inevitável seu aprimoramento, na medida que forem sendo verificadas a eficiência real do teor das normas, bem como em razão do próprio avanço das práticas mercadológicas e das formas de tratamentos de dados pessoais com as novas tecnologias. Talvez o maior desafio da LGPD seja, em verdade, a sua compreensão pelo cidadão comum, ao menos de seus aspectos básicos, para que este veja nela uma norma de cidadania, assim como é atualmente o Código de Defesa do Consumidor.

4. Considerações finais

Muito embora a LGPD esteja sendo em muitos casos contestada e permanentemente seja colocada uma grande dificuldade na sua implementação, o que pode ser verificado pelas diversas tentativas de adiamento da sua entrada em vigor, não se pode desmerecer sua importância, conforme ressaltado ao longo do estudo. Em um momento em que o crescimento das relações comerciais por meios digitais se expande vertiginosamente nas mais diversas plataformas, a existência da LGPD precisa, sobretudo, ser disseminada entre a população que massivamente utiliza os meios eletrônicos.

A sua compreensão deve ir além das empresas e entidades públicas e privadas, ao menos quanto aos direitos básicos, para que o cidadão comum tenha condições de avaliar como está contratando e em que medida seus dados divulgados aos fornecedores e agentes de tratamento, estão sendo utilizados sem agredir sua privacidade e, principalmente, sem lhe ofertar situação menos vantajosa e discriminatória.

Os avanços da ciência são indispensáveis. Em poucos momentos na história, a humanidade verificou o quanto o conhecimento científico é necessário à sobrevivência em comunidade e isso se aplica também aos institutos jurídicos e a compreensão dos direitos individuais neste século. A LGPD revela-se, assim, como o primeiro passo, mas não o único, para que as transformações da tecnologia ganhem pilares de eticidade e, notadamente, no comércio eletrônico poderá aprimorar a própria compreensão dos direitos básicos do consumidor.

Referencial bibliográfico

ALBERTIN, Alberto Luiz. *O comércio eletrônico evolui e consolida-se no mercado brasileiro*. Rev. Adm. Empres. vol. 40. n. 4. São Paulo: 2000. Disponível em:< https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-75902000000400009>. Acesso em: 27 dez. 2019.

BESSA, Leonardo Roscoe. *Banco de dados e cadastros de consumo*. *In*: BENJAMIN, Herman; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. Manual de direito do consumidor. 4. ed. rev., atual. e ampl., São Paulo: Revista dos Tribunais, 2012, pp. 293-334.

BIONI, Bruno Ricardo; LUCIANO, Maria. *O princípio da precaução na regulação de inteligência artificial*: seriam as leis de proteção de dados o seu portal de entrada?. 2019. Disponível em: <https://brunobioni.com.br/wp-content/uploads/2019/09/Bioni-Luciano_O-PRINCI%CC%81PIO-DA-PRECAUC%CC%A7A%CC%83O-PARA-REGULAC%CC%A7A%CC%83O-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf>. Acesso em 27 fev. 2021.

BOECHAT, Marcos. A responsabilidade do provedor de internet e o "*notice and takedown*". *Revista Jus Navigandi*, ISSN 1518-4862, Teresina, ano 17, n. 3360, 12 set. 2012. Disponível em: https://jus.com.br/artigos/22598. Acesso em: 01 mar. 2021.

BRASIL. *Constituição da República Federativa do Brasil*. 1988. Planalto. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm>. Acesso em: 03 fev. 2021.

BRASIL. *Lei nº 8.078 de 11 de setembro de 1990*. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. 1990. Planalto. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078compilado.htm. Acesso em: 05 fev. 2021.

BRASIL. *Lei nº 9.507 de 12 de novembro de 1997.* Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. 1997. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm>. Acesso em: 02 fev. 2021.

BRASIL. *Lei nº 12.414 de 09 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. 2011. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm>. Acesso em 03 fev. 2021.

BRASIL. *Lei nº 12.527 de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. 2011. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm>. Acesso em: 03 fev. 2021.

BRASIL. *Lei nº 12.737 de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. 2012. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 03 fev. 2021.

BRASIL. *Lei nº 12.965 de 23 de abril de 2014*. Marco civil da internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. 2014. Planalto. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: 10 fev. 2021.

BRASIL. *Lei nº 13.709 de 14 de agosto de 2018.* Lei de proteção de dados pessoais (LGPD). 2018. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm>. Acesso em 30 jan. 2021.

CAPANEMA, Walter Aranha. *A responsabilidade civil na lei geral de proteção de dados.* Cadernos Jurídicos. Ano 21. n. 53. São Paulo, 2020. pp. 163-170. TJSP. Disponível em: <https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712>. Acesso em: 06 fev. 2021.

CASTELLS, M. *A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.* Trad. Maria Luiz X. de A. Borges. Rio de Janeiro: Jorge Zahar, 2003.

CASTELLS, M. *A sociedade em rede. Economia, sociedade e cultura.* 9. ed. - atualizada. Vol. 1. São Paulo: Paz e Terra, 2006.

DIAS, José Carlos Vaz e.; SANT'ANNA, Leonardo da Silva; KELLER, Gabriel Muller Frazão. *Novos horizontes negociais nas plataformas digitais*: a concorrência desleal sob a prática do *geo-blocking* e *geo-pricing*. Revista Quaestio Iuris. vol. 13, n. 04, Rio de Janeiro, 2020. pp. 1914 -1938

EBIT NIELSEN COMPANY. *Relatório webshoppers*. 42. ed. 2020. Disponível em: <https://company.ebit.com.br/webshoppers>. Acesso em: 04 fev. 2020.

FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. Direito à Privacidade na Era Digital. *Revista Internacional Consinter de Direito.* n. IX. 2019, pp. 119-140. Disponível em: < https://www.revistaconsinter.com/wp-content/uploads/2019/02/ano-iv-numero-vii-direito-a-privacidade-e-novas-tecnologias-breves-consideracoes-acerca-da-protecao-de-dados-pessoais-no-brasil-e-na-europa.pdf>. Acesso em 30 jan. 2021.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. *Revista de Direito Brasileira.* Florianópolis. v. 23. n. 9. Mai./Ago. 2019, pp. 284-301. Disponível em:<https://indexlaw.org/index.php/rdb/article/view/5343>. Acesso em: 04 fev. 2021.

FRAZÃO, Ana. *Geopricing e geoblocking*: as novas formas de discriminação de consumidores. Jota. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/geopricing-e-geoblocking-as-novas-formas-de-discriminacao-de-consumidores-15082018>. Acesso em: 09 set. 2018.

FRAZÃO, Ana. *Objetivos e alcance da Lei Geral de Proteção de Dados*. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thompson Reuters Brasil, 2019, pp. 99-129.

GALINARI, Rangel; JUNIOR, Osmar Cervieri; TEIXEIRA JUNIOR, Job Rodrigues; RAWET, Eduardo Lederman. *Comércio eletrônico, tecnologias móveis e mídias sociais no Brasil.* 2015. Revista BNDES Setorial 41, pp. 135-180. Disponível em.: <https://web.bndes.gov.br/bib/jspui/bitstream/1408/4285/1/BS%2041%20Com%C3%A9rcio%20eletr%C3%B4nico%2c%20tecnologias%20m%C3%B3veis%20e%20m%C3%ADdias%20sociais_.pdf> Acesso em.: 15 out. 2018.

GUEDES, Gisela Sampaio da Cruz; MEIRELLES, Rose Melo Vencelau. *Término do tratamento de dados*. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thompson Reuters Brasil, 2019, pp. 219-241.

KUNSCH, Margarida M. Kröhling. *Comunicação organizacional na era digital:* contextos, percursos e possibilidades. Signo y pensamiento, v. 26. n. 51. 2007. Disponível em.: < https://www.studocu.com/pt-br/document/pontificia-universidade-catolica-de-campinas/comunicacao-integrada/outro/2-comunicacao-organizacional-na-era-digital/4720018/view> Acesso em.: 31 out. 2018.

LEMOS, Ronaldo. *O marco civil como símbolo do desejo por inovação no Brasil*. *In:* LEITE, George Salomão; LEMOS, Ronaldo. Marco Civil da Internet. São Paulo: Atlas, 2014, pp. 03-11.

LUCIANO, Edimara Mezzomo; FREITAS, Henrique. *Comércio eletrônico de produtos virtuais*: a internet modificando a operação de comprar e vender produtos. VI SIMPOI - Simpósio de Administração da Produção, Logística e Operações Internacionais, 2003, São Paulo. Disponível em: <http://www.ufrgs.br/gianti/files/artigos/2003/2003_130_SIMPOI.pdf>. Acesso em 30 out. 2018.

MARQUES, Claudia Lima. *Diálogo das Fontes.* In: BENJAMIN, Herman; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. Manual de direito do consumidor. 4. ed. rev., atual. e ampl., São Paulo: Revista dos Tribunais, 2012, pp. 117-133.

MARQUES, Claudia Lima; KLEE, Antonia Espíndola. *Os direitos do consumidor e a regulamentação do uso da internet no Brasil:* convergência no direito às informações claras e completas nos contratos de prestação de serviços de internet. *In:* LEITE, George Salomão; LEMOS, Ronaldo. Marco Civil da Internet. São Paulo: Atlas, 2014, pp. 469-517.

MEDINA, José Miguel Garcia. *Constituição Federal comentada.* 3. ed. São Paulo: Editora Revista dos Tribunais, 2014.

MONTEIRO FILHO, Carlos Edison do Rêgo; CASTRO, Diana Paiva de. *Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados (Lei 13.709/2018).* In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thompson Reuters Brasil, 2019, pp. 323-345.

NOVO, Rafael; NEVES, José Manoel Souza das. *Inovação na inteligência analítica por meio do Big Data: características de diferenciação da abordagem tradicional*. In: Workshop de Pós-Graduação e Pesquisa do Centro Paula Souza. 2013. pp. 32-44. Disponível em:

<http://www.pos.cps.sp.gov.br/files/artigo/file/488/839f2e27fa0fa7f5776622a62a48a776.pdf>. Acesso em: 20 out. 2018.

OLIVA, Milena Donato; VIÉGAS, Francisco de Assis. *Tratamento de dados para a concessão de crédito***.** In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thompson Reuters Brasil, 2019, pp. 561-599.

REIS, Émilien Vilas Boas; NAVES, Bruno Torquato de Oliveira. O meio ambiente digital e o direito à privacidade diante do Big Data. *Veredas do Direito*, Belo Horizonte, v. 17, n. 37, p. 145-167, jan.-abr. 2020. Disponível em: http://revista.domhelder.edu.br/index.php/veredas/article/view/1795. Acesso em: 30 jan. 2020.

RIFKIN, Jeremy. *Sociedade com custo marginal zero:* a internet das coisas, os bens comuns colaborativos e o eclipse do capitalismo. São Paulo: MBooks, 2016.

RUARO, Regina Linden; GLITZ, Gabriela Pandolfo Coelho. Panorama geral da lei geral de proteção de dados pessoais no brasil e a inspiração no regulamento geral de proteção de dados pessoais europeu. *REPATS*, Brasília, V.6, nº 2, p 340-356, Jul-Dez, 2019. Disponível em: <https://portalrevistas.ucb.br/index.php/REPATS/article/view/11545>. Acesso em: 29 jan. 2021.

SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. *Direitos do titular de dados pessoais na Lei 13.709/2018*: uma abordagem sistemática. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019, pp. 243-286.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. *Consentimento e proteção de dados pessoais da LGPD*. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thompson Reuters Brasil, 2019, pp.287-322.

UNIÃO EUROPEIA. *Directiva 95/45/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995.* Disponível em: <https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX:31995L0046>. Acesso em 27 fev. 2021.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.* Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0679> . Acesso em 27 fev. 2021.

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