UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS SOCIAIS E APLICADAS

DEPARTAMENTO DE DIREITO

FAGNER NASCIMENTO SOARES

PROTEÇÃO DE DADOS NA SOCIEDADE DA INFORMAÇÃO: A FIGURA DO CONSENTIMENTO.

São Cristóvão – SE

2021

UNIVERSIDADE FEDERAL DE SERGIPE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE DIREITO

FAGNER NASCIMENTO SOARES

PROTEÇÃO DE DADOS NA SOCIEDADE DA INFORMAÇÃO: A FIGURA DO CONSENTIMENTO

Trabalho de Conclusão de Curso apresentado para obtenção do grau de bacharel em Direito na Universidade Federal de Sergipe.

Orientadora: Professora Dra. Analice Nogueira Santos Cunha.

São Cristóvão
2021

FAGNER NASCIMENTO SOARES

PROTEÇÃO DE DADOS NA SOCIEDADE DA INFORMAÇÃO: A FIGURA DO CONSENTIMENTO

Trabalho de Conclusão de Curso apresentado para obtenção do grau de bacharel em Direito na Universidade Federal de Sergipe.

Orientadora: Professora Dra. Analice Nogueira Santos Cunha.

São Cristóvão, 17 de dezembro de 2021

BANCA EXAMINADORA

_____

Professora Dra. Analice Nogueira Santos Cunha

_____

Professor Vitor Oliveira

_____

Professor Raphael Leal Roldão Lima

SOARES, FAGNER NASCIMENTO

PROTEÇÃO DE DADOS NA SOCIEDADE DA INFORMAÇÃO: A FIGURA DO CONSENTIMENTO/ São Cristóvão-2021.

Orientadora: Profª. Drª. Analice Nogueira Santos Cunha.

Trabalho de Conclusão de Curso (Graduação) – Universidade Federal de Sergipe, 2021.

1. Relevância dos dados pessoais na sociedade da informação. 2. Mecanismos legais de proteção. 3. Função do consentimento enquanto estratégia normativa. I. SOARES, Fagner Nascimento. II. Universidade Federal de Sergipe. III. Proteção de Dados na Sociedade da Informação: A Figura do Consentimento.

RESUMO

A discussão a respeito dos mecanismos de uso e proteção de dados na internet tem se revestido de importância inédita. O ser humano moderno não apenas utiliza as redes de interação virtual, mas precisa delas, cada vez mais, para ser social e culturalmente integralizado à sociedade da informação. Diante desta necessidade e da valoração econômica, política e social dos dados pessoais, esta pesquisa buscou analisar como o consentimento, instituto jurídico presente no eixo central das normativas de proteção referentes à matéria, está sendo utilizado e interpretado. Neste contexto, questiona-se a eficiência do consentimento enquanto estratégia normativa de proteção, haja vista que através dos extensos e complexos termos de uso e política de privacidade o instituto assume mera função ficcional no processo de tutela jurídica dos dados pessoais. A reflexão que se põe se debruça sobre a capacidade do titular de dados pessoais consentir de forma efetiva, face a patente falta de informações claras a respeito do que vem a ser tratamento de dados. Para tanto, através da análise qualitativa, feita por meio de revisão bibliográfica, fez-se um apanhado do papel do consentimento nas legislações brasileiras que versam sobre o tema, do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados. O resultado encontrado apontou para a insuficiência do consentimento enquanto estratégia normativa de proteção dos dados pessoais, potencializada pela sua interpretação sob os dogmas do direito contratual e pela limitação da tutela jurídica dos dados ao campo do direito à privacidade. Tal insuficiência poderá ser sanada mediante a releitura do instituto jurídico do consentimento e da regulamentação de mecanismos de melhoramento pensados e estruturados dentro da própria tecnologia da informação.

Palavras-chave: consentimento, internet, dados, informação, autodeterminação.

ABSTRACT

The discussion about the mechanisms for the use and protection of data on the internet has gained unprecedented importance. The modern human being not only uses virtual interaction networks, but needs them, increasingly, to be socially and culturally integrated into the information society. In view of this need and the economic, political and social valuation of personal data, this research sought to analyze how consent, a legal institute present in the central axis of protection regulations relating to the matter, is being used and interpreted. In this context, the efficiency of consent as a normative protection strategy is questioned, given that through the extensive and complex terms of use and privacy policy, the institute assumes a mere fictional function in the process of legal protection of personal data. The reflection that is put forward focuses on the ability of the holder of personal data to consent effectively, given the patent lack of clear information about what data processing is. Therefore, through a qualitative analysis, carried out through a literature review, an overview of the role of consent in Brazilian legislation on the subject was made, from the Consumer Protection Code to the General Data Protection Law. The result found pointed to the insufficiency of consent as a normative strategy for the protection of personal data, enhanced by its interpretation under the dogmas of contractual law and by the limitation of the legal protection of data to the field of the right to privacy. This insufficiency can be remedied by re-reading the legal institute of consent and by regulating mechanisms for improvement designed and structured within information technology itself.
Keywords: consent, internet, data, information, self-determination.

LISTA DE SIGLAS E ABREVIATURAS

ARPA - Agência de Projetos de Pesquisa Avançada

CDC – Código de Defesa do Consumidor

CRFB/88 – Constituição Federal de 1988

GDPR - *General Data Protection Regulation*

GPEN - *Global Privacy Enforcement Network*

LGPD – Lei Geral de Proteção de dados

MCI - Marco Civil Da Internet

NSA - *National Security Agency*

PEC – Proposta de Emenda à Constituição

PETs - *Privacy Enhancing Technologies*

UCLA - *University of California, Los Angeles*

SUMÁRIO

INTRODUÇÃO

A regulamentação da internet sempre se mostrou um desafio à ciência jurídica, dada a intensa mutação dos meios tecnológicos que a instrumentalizam, não tendo sido diferente no que se refere à tutela dos dados pessoais. Nesse contexto, a discussão a respeito da proteção de dados pessoais na internet e seus desafios, em que pese antiga, ganhou ênfase com a promulgação da Lei Geral de Proteção de Dados - LGPD[1], no ano de 2018, bem como com a recente entrada em vigor da totalidade de seus artigos, que se deu em agosto de 2021.

A relevância do tema se justifica pela inegável revolução informacional pela qual está passando a sociedade. Em seguida à fase pós-industrial, que se deu com o fim da segunda grande guerra e foi marcada pelo enfoque na prestação do serviço contratado, emerge a era da informação, que passa a ostentar valor econômico e político e assume o centro de reestruturação das bases da sociedade pós-moderna (BIONI, 2020).

Nesta senda, os mercados, as disputas políticas e as relações sociais são conduzidas ou afetadas pela informação, que é diariamente colhida através dos computadores ou dispositivos móveis dos usuários da internet. Tal colheita é realizada através de mecanismos de captação de dados e algoritmos que, além de catalogar e organizar informações, podem extrair delas nossas predileções, gostos e hábitos (BIONI, 2020). A título exemplificativo, tornou-se comum a situação em que um indivíduo pesquisa determinado produto em um site de buscas e depois é surpreendido com um anúncio daquele mesmo objeto numa de suas redes sociais. Esta operação se dá em razão do compartilhamento e cruzamento de dados realizado entre a *Google* e seus parceiros comerciais.

De forma idêntica, fazer um cadastro em uma rede social, serviço de comunicação eletrônica – e-mail ou em um aplicativo de dispositivo móvel exige o fornecimento de dados pessoais que, uma vez colhidos, ficam registrados num banco de dados de acesso e controle difíceis ao cidadão comum. Neste sentido, para que se possa desfrutar dos recursos propiciados pelas redes sociais e outros aplicativos ou programas, o indivíduo precisa fornecer nome completo, idade, endereço, telefone e entre outras informações pessoais que servem à sua identificação.

Nesse contexto, o fornecimento de dados pelo indivíduo, em que pese ser tratado como uma escolha, revela-se cada vez mais como uma necessidade, tendo em vista que a atual vida em sociedade reclama uma constante integração virtual, seja para o convívio familiar, seja para

[1] lei Nº 13.709, de 14 de agosto de 2018**.** Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 de dez. 2021.

o profissional ou pessoal. Os meios de comunicação via mensagem instantânea, como o *WhatsApp*, por exemplo, para muitos tornou-se recurso profissional, bem como o *Instagram*.

Neste sentido, é indispensável se ter em mente que ao titular de dados pessoais não é proporcionado um dimensionamento real e de fácil compreensão sobre a utilização de seus dados e, muito menos, um esclarecimento a respeito dos mecanismos de controle de que dispõe para exercer a fiscalização sobre o uso de suas informações.

A primeira pergunta que se lança, nesta perspectiva, é se é possível falar em livre escolha ao compartilhamento de dados face à forma como se tem tratado e regulamentado o consentimento enquanto instituto jurídico? Somos capazes de consentir, de forma livre e informada, a respeito da utilização dos nossos dados pessoais ?

Nesse contexto, é necessário apontar que esta pesquisa não tem como objetivo se contrapor à utilização dos dados pessoais, o que seria impraticável. O tratamento de dados, que na definição da LGPD consiste em "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição...", em realidade mostra-se positivo por tornar possíveis várias atividades em diversas áreas, a exemplo da mercadológica (DONEDA, 2019). A título exemplificativo, a utilização de dados relacionados à pesquisa de usuários para direcionamento de produtos ou serviços através de anúncios não é algo necessariamente prejudicial. Em realidade, tal ferramenta pode até auxiliar o consumidor na escolha de um produto que lhe proporcione um melhor custo/benefício.

Todavia, apesar de tal apontamento, a realidade contemporânea aponta que a disponibilização de dados pessoais, em que pese travestida de opção, assume a natureza de condição para que o indivíduo consiga ser integrado na sociedade cada vez mais virtualizada. A necessidade de integração virtual acaba por deixar o titular dos dados pessoais, em regra, numa posição de refém, posto que a escolha negativa em compartilhar suas informações lhe privará de usufruir de um bem, serviço ou recurso imediatamente necessário ou desejado por ele (BIONI, 2020). Esta constatação põe em xeque o consentimento enquanto instituto jurídico e centro gravitacional da estratégia normativa de proteção de dados.

O problema desta pesquisa versa, pois, sobre o consentimento e sua função nas normas protetivas de dados pessoais. Por meio de uma análise qualitativa, feita por meio de revisão bibliográfica, questiona-se a adoção do consentimento como estratégia normativa eficiente pelos dispositivos legais brasileiros até então promulgados e, especificamente, a forma como tem sido lido e aplicado enquanto instituto jurídico. Neste contexto, aponta-se como a leitura contratualista clássica do consentimento, reproduzida fielmente nos extensos e tecnicistas

termos de uso e política de privacidade, é ultrapassada à complexidade que emerge do tratamento de dados (BIONI, 2020).

Exposto o problema, propõe-se uma releitura da função do consentimento enquanto ponto cardeal de todo o sistema normativo de proteção de dados brasileiro, que abandonaria a visão clássica contratual calcada na autonomia privada e se aparelharia de recursos, dentro do âmbito da própria tecnologia da informação, para que se promova o empoderamento efetivo do usuário na proteção e controle dos seus dados pessoais. Mostra-se necessária, neste sentido, a regulamentação de uma estratégia normativa que não deixe a tutela dos dados pessoais somente a cargo do usuário, através da pesada decisão de consentir ou não com o compartilhamento de seus dados.

Contudo, até se chegar ao ponto central da discussão proposta é necessário que se reflita sobre a sociedade da informação e suas imbricações. Neste novo modelo social, tratado no capítulo dois da presente pesquisa, "a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos" (CASTELLS, 2021, p. 74). Ainda revela-se pertinente a análise sobre o valor econômico dos dados pessoais na sociedade da informação, fundamental à discussão sobre estrutura ou reorganização social.

O capítulo terceiro, por sua vez, versa sobre a tutela jurídica dos dados pessoais. Traça-se uma discussão a respeito da natureza jurídica da proteção de dados, em que se observa a bifurcação entre dois entendimentos, sendo o primeiro limitador da proteção de dados à tutela da privacidade e o outro expansivo, em que se defende a autonomia da matéria enquanto direito fundamental e da personalidade (BIONI, 2020). Ademais, no referido capítulo ainda se analisa o tratamento jurídico e as definições legais concernentes aos dados pessoais e suas categorias.

No quarto capítulo inaugura-se a discussão a respeito da figura jurídica do consentimento e as suas limitações enquanto estratégia normativa de proteção. Neste sentido, faz-se um apanhado do instituto nas principais legislações aplicáveis à proteção de dados que foram promulgadas no Brasil, começando pelo Código de Defesa do Consumidor - CDC até a Lei Geral de Proteção de Dados.

Analisa-se em que medida o consentimento enquanto manifestação de vontade teve maior ou menor incidência em cada legislação. Neste contexto, a constatação é de que o consentimento ainda é a mola mestra do sistema normativo de proteção dos dados pessoais, em que pese ter existido avanço substancial desde o CDC. De modo idêntico, pouco refletem as legislações a respeito da capacidade de consentir, sendo carentes de mecanismos facilitadores que possibilitem, de fato, a autodeterminação informacional.

2. A proteção de dados na internet

A discussão a respeito da proteção de dados na rede requer a compreensão inicial do que vem a ser internet. Mais do que isto, é preciso refletir sobre o seu uso enquanto ferramenta tecnológica e os seus reflexos na estrutura social. Para tanto, pertinente se fazer um rápido traçado da evolução tecnológica e da mutação social que se deu ao longo deste processo.

Desde as sociedades mais primitivas, o ser humano busca interagir com o meio que o cerca, moldando-se a partir da experiência e alterando seu comportamento com o fim de se chegar a uma maneira mais cômoda e funcional de vida. Neste processo, dois conceitos são relevantes: técnica e tecnologia.

Tais termos, que num primeiro momento podem remeter a algo contemporâneo, moderno, são tão velhos quanto o próprio ser humano. Conceitualmente, eles remontam à palavra grega *techné*, que no apontamento de Estéfano Vizconde Veraszto, Dirceu da Silva, Nonato Assis Miranda e Fernanda Oliveira Simon (2009, p. 21) consiste "[...] muito mais em se alterar o mundo de forma prática do que compreendê-lo."

A respeito da técnica, Veraszto, Silva, Miranda e Simon (2009, p. 21) asseveram:

> Na técnica, a questão principal é do como transformar, como modificar. O significado original do termo *techné* tem sua origem a partir de uma das variáveis de um verbo que significa fabricar, produzir, construir, dar à luz, o verbo *teuchô* ou *tictein*, cujo sentido vem de Homero; e *teuchos* significa ferramenta, instrumento.

Já tecnologia seria algo maior que ferramentas, máquinas e processos, "ela põe em evidência o 'trabalho humano', as tentativas do homem para satisfazer seus desejos mediante a ação humana sobre objetos físicos" (KRANSBERG, 1981; apud GAMA, 1986, p. 12).

Os conceitos referidos coadunam com a compreensão de que a tecnologia compõe o eixo gravitacional da história da própria humanidade. A forma como o ser humano se relaciona com o meio para satisfazer suas necessidades, variantes conforme tempo e lugar, conduz o fio de sua própria evolução. Neste momento, estamos vivendo a era da tecnologia da informação, sendo a interação entre a sociedade e o seu meio cada vez mais digitalizada, desconcentrada e fluida. Mas antes de chegarmos neste ponto da análise, pertinente pensar outras eras da tecnologia, precedentes ao presente momento.

Comecemos pela revolução industrial que, segundo Manuel Castells, teria sido dividida por em pelo menos dois grandes momentos:

> Segundo os historiadores, houve pelo menos duas revoluções industriais: a primeira começou pouco antes dos últimos trinta anos do século XVIII, caracterizada por novas tecnologias como a máquina a vapor, a fiadeira, o processo Cort em metalurgia e, de forma mais geral, a substituição das ferramentas manuais pelas máquinas; a segunda, aproximadamente cem anos depois, destacou-se pela desenvolvimento da eletricidade, do motor de combustão interna, de produtos químicos com base científica, da fundição eficiente de aço e pelo início das tecnologias da comunicação, com a difusão do telégrafo e a invenção do telefone. (CASTELLS, 2021, p. 90).

As primeiras duas revoluções industriais tornaram visível que os meios tecnológicos não se restringem somente a relação do homem com o meio, mas também são determinantes no processo de interação social do homem com seu semelhante. Neste contexto, Castells ensina que as revoluções:

> Foram, de fato, "revoluções" no sentido de que um grande aumento repentino e inesperado de aplicações tecnológicas transformou os processos de produção e distribuição, criou uma enxurrada de novos produtos e mudou de maneira decisiva a localização das riquezas e do poder no mundo, que, de repente, ficaram ao alcance dos países e elites capazes de comandar o novo sistema tecnológico. (CASTELLS, 2021, p. 91).

Posteriormente à fase do apogeu da indústria, da máquina a vapor e as maravilhas da eletricidade, surge uma nova fase que muda os paradigmas até então pensados: a fase pós-industrial, após as duas grandes guerras mundiais. Nesta fase, o enfoque não era mais o produto, mas sim o serviço prestado, eixo da nova economia (BIONI, 2020).

No momento contemporâneo, estamos presenciando uma nova estruturação social e econômica, desta vez focada na informação. Este enfoque surge num contexto de reorganização do próprio sistema capitalista após o enfraquecimento do movimento estatista soviético, em que se destacam a flexibilidade de gerenciamento, a descentralização empresarial e a interdependência internacional, conceitos elaborados por Castells:

> Não é diferente no caso da revolução tecno1ógica atual. Ela originou-se e difundiu-se, não por acaso, em um período histórico da reestruturação g1obal do capitalismo, para o qual foi uma ferramenta básica. Portanto, a nova sociedade emergente desse processo de transformação é capitalista e também informacional, embora apresente variação histórica considerável nos diferentes países, conforme sua história, cultura, instituições e relação específica com o capitalismo global e a tecnologia informacional. (CASTELLS, 2021, p. 70-71).

Esta digressão a respeito da evolução da tecnologia tem como objetivo apontar que qualquer análise a respeito da regulamentação normativa da internet deve, precipuamente, se debruçar sobre a tecnologia da informação como um fenômeno sociológico, metajurídico. É necessária a reflexão a respeito do quão estruturada está a sociedade atual neste novo modelo de desenvolvimento, em que "a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos" (CASTELLS, 2021, p. 74).

Dito de maneira mais prática, a proteção jurídica da informação na internet não surge como uma necessidade isolada, representando uma mudança de paradigmas na forma de comunicação e interação do ser humano com o meio e seus pares, na qual a informação assume a condição de mola mestra social. Este novo sistema econômico e tecnológico, definido por Castells (2021, p. 75) como "capitalismo informacional" reclama uma proteção normativa que enxergue a necessidade de se refletir este novo processo revolucionário.

2.1 Internet: origem e conceito

A internet teve sua gênese numa empreitada com fins eminentemente militares, tendo como grande protagonista a Agência de Projetos de Pesquisa Avançada (ARPA) do Departamento de Defesa dos Estados Unidos da América (CASTELLS, 2021). No contexto da guerra fria, logo após o lançamento dos primeiros satélites russos conhecidos como *Sputniks*[2], na segunda metade da década de 1950, a ARPA elaborou, em meio a inúmeras experiências, um sistema de comunicação imune a ataques nucleares. A ideia foi criar uma rede de comunicação descentralizada e independente de centros de comando. Este teria sido, por assim dizer, o embrião da internet. Mais tarde, em um de setembro de 1969, entrava em funcionamento a primeira rede de computadores: a *Arpanet*. (CASTELLS, 2021).

Deste momento embrionário seguiram-se inúmeros avanços, resultado da atividade conjunta de redes científicas que não se limitavam aos fins militares inicialmente pensados, tomando lugar de destaque grandes centros de conhecimento como a *University of Southern California, Havard University, University of California, Los Angeles (UCLA), Stanford University*. (CASTELLS, 2021).

[2] Sputnik I foi o primeiro satélite artificial a ser lançado pela URSS na orbita com êxodo. Este fato histórico deu início a um grande avanço tecnológico levando após alguns anos o primeiro homem ao espaço. A partir deste, grandes empresas investiram em novos negócios: os chamados passeios no espaço. Disponível em: <https://publicacoeseventos.unijui.edu.br/index.php/enteci/article/view/11654/10197>. Acesso em: 22 de dez. 2021.

A internet como se conhece hoje foi o resultado de mais de cinco décadas de evolução, mas sua ideia base ainda continua sendo a mesma: a descentralização do fluxo de informações. Na definição de Danilo Cesar Maganhoto Doneda, a internet seria:

> (...) basicamente uma rede de computadores cujo funcionamento não depende de centros de controle hierarquizados. Tal configuração cria dificuldades às tentativas de controle do tráfego de dados, visto que a rede consiste basicamente em um protocolo de comunicações, implementado em computadores, possibilitando sua interligação através dos vários meios de comunicação de dados existentes. Essa estrutura de rede é capaz de prescindir de "caminhos únicos" – podendo substituir eventuais vias de comunicação bloqueadas por outras – com a consequência de que não há mais elementos "essenciais" para seu funcionamento. (DONEDA, 2019, p. 67)

Pensando em sua função na sociedade da informação, a internet seria o instrumento tecnológico atual da comunicação. Esta constatação aponta existir uma relação umbilical entre comunicação e tecnologia, de maneira que a primeira é possibilitada em função e conforme os meios dispostos pela segunda, que variam conforme cada época (DONEDA, 2019).

2.2 A sociedade da informação

As grandes revoluções sociais dos últimos três séculos compartilham o fato de ditarem, cada uma conforme sua época, o funcionamento da economia. No momento atual de ruptura histórica, em que a informação e a internet assumem o papel de destaque, surge uma nova economia que remonta ao final do século XX, qualificada por Castells como informacional, global e de funcionamento em rede:

> É *informacional* porque a produtividade e a competitividade de unidades ou agentes nessa economia (Sejam empresas, regiões ou nações) dependem basicamente de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos. É *global* porque as principais atividades produtivas, o consumo e a circulação, assim como seus componentes (capital, trabalho, matéria-prima, administração, informação, tecnologia e mercados) estão organizados em escala global, diretamente ou mediante uma rede de conexões entre agentes econômicos. É *rede* porque, nas novas condições históricas, a produtividade é gerada, e a concorrência é feita em uma rede global de interação entre redes empresariais. (CASTELLS, 2021, p 135).

Nesta nova estrutura social, a informação seria o ponto chave, fonte de valor social político e econômico:

> Por isso, a informação avoca um papel central e adjetivante da sociedade: sociedade da informação. A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial. (BIONI, 2020, p. 05).

No contexto deste novo paradigma, os dados pessoais passam a ser igualmente monetizados. Além do processo de monetização, esta nova modulação social altera a própria esfera relacional do indivíduo, sendo os dados não somente informações, mas prolongamentos da pessoa humana.

Neste sentido, não se pode confundir o termo "dado" com o termo "informação", em que pese alguns autores tratarem as expressões enquanto sinônimas. Na definição de Bioni (2020, p. 31-32):

> [...] O dado é o estado primitivo da informação, pois não é algo per se que acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação.

Os dados, quando desorganizados, representam um conjunto desprovido de valor informativo. Neste sentido, segundo Bioni:

> [...] a dinâmica de um banco de dados envolve entrada (input) e processamento de dados e a saída (output) de uma informação. É imprescindível, portanto, o gerenciamento, manual ou automatizado, de um banco de dados, para que dele seja extraído algum conhecimento"(BIONI, 2020, p. 32).

O termo dado estaria associado a algo menos elaborado do que a informação propriamente dita. Para Doneda (2019, p. 136) o dado estaria "associado a uma espécie de 'pré-informação', anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição."

2.3 A valoração comercial dos dados pessoais na sociedade da informação

As ferramentas e tecnologias da informação permitem que, através da coleta de dados pessoais, se cataloguem preferências individuais, históricos de busca por produtos, padrões de comportamento e entre outras coisas que, quando são cruzadas, possibilitam a previsibilidade daquilo que será desejado pelo consumidor.

Posta a possibilidade de catalogação e organização dos dados pessoais, surge um novo mercado, pautado justamente no paradigma da informação, instituindo-se, na definição de Bioni (2020, p. 12), uma "economia de vigilância":

Com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (marketing) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação.

E, com a possibilidade de organizar tais dados de maneira mais escalável, criou-se um novo mercado cuja base de sustentação é a sua extração e comodificação. Há uma economia de vigilância que tende a posicionar o cidadão como um mero fornecedor das suas informações.

Esta conjuntura mercadológica nasce em paralelo ao comércio eletrônico que segue em franca expansão no Brasil e em todo o mundo. Em 2020, por exemplo, o *E-commerce*[3] representou cerca de 11% (onze por cento) das vendas de varejo no Brasil . Além disso, o faturamento do e-commerce cresceu 41% (quarenta e um por cento) em 2020, contabilizando mais de 194 milhões de pedidos feitos por consumidores brasileiros, com uma arrecadação de cerca de R$ 87,4 bilhões, segundo dados do estudo *Webshoppers* (*Ebit/Nielsen & Bexs Banco*).

Neste novo mercado, os consumidores emitem suas opiniões, trocam informações a respeito da qualidade dos produtos, avaliam a experiência da compra e etc., tudo isto através dos canais disponibilizados pela internet. Nesta atividade, o consumidor deixa de ser meramente a ponta da cadeia de comercialização para passar a atuar no processo de produção, moldando-o sem qualquer custo adicional ao fornecedor. A este respeito, Bioni (2020, p. 13) discorre:

> É com essa voz ativa, que a popular lição promocional do "boca a boca" se potencializou na sociedade da informação, passando o consumidor a atuar como se fosse um assistente de vendas sem custos. Além de ele divulgar o bem de consumo, a informação por ele produzida auxilia em seu processo de produção. O produto ou serviço tende a ser modelado de acordo com os pontos negativos e positivos assinalados por esse elo final da cadeia de consumo, que nunca teve tantos mecanismos para vocalizar a sua opinião.
> [...]

---

[3] O mercado eletrônico, obtido através da aplicação intensiva de Tecnologia de Informação no mercado tradicional, é considerado uma realidade que trará grandes benefícios para as organizações que o considerarem nas suas estratégias e ameaças ainda maiores para as que não o utilizarem. Nesse novo ambiente, o comércio eletrônico, com suas aplicações inovadoras e revolucionárias, é tido como uma das tendências emergentes com maior poder potencial de inovação nas estratégias e nos processos de negócio nos vários setores econômicos. (…). Disponível em: https://www.scielo.br/j/rae/a/mKmhwsVC5zbYqWDGgHrqmvh/?lang=pt. Acesso em: 22 de dez. 2021.

> O consumidor deixa, portanto, de ter uma posição meramente passiva no ciclo do consumo. Ele passa a ter uma participação ativa, que condiciona a própria confecção, distribuição e, em última análise, a segmentação do bem de consumo, transformando-se na figura do prosumer. O consumidor não apenas consome (consumption), mas, também, produz o bem de consumo (production): prosumer.

Neste contexto, a publicidade de massa , através de revistas, jornais, rádio e televisão, que se perfaz sob uma abordagem estandardizada, dá lugar à publicidade direcionada, que focaliza o processo de comunicação para um público específico, mais propenso à aquisição do bem ofertado (BIONI, 2020).

Enquanto espécie de publicidade direcionada, destaca-se a publicidade comportamental *on-line*, que, na definição de Fabrício Germano Alves (2016, p. 214) :

> [...] constitui uma prática que consiste em direcionar anúncios publicitários específicos para determinados consumidores, de acordo com o seu comportamento online anterior, ou seja, é destinada a um grupo, classe ou categoria de consumidores de acordo com uma base de dados a respeito dos mesmos elaborada a partir de interesses previamente demonstrados.

Este direcionamento se torna possível mediante as ferramentas tecnológicas que revelam, a partir do histórico de navegação e hábitos dos usuários, um verdadeiro perfil consumerista. Neste contexto, ao se navegar pela internet são deixados rastros que, quando organizados e catalogados, revelam quais produtos ou serviços agradam a determinados seguimentos de internautas.

O usuário, neste cenário, é cada vez mais monitorado. Os dados fornecidos são armazenados e utilizados para que se possa traçar a figura do consumidor em potencial. Não por outro motivo os anúncios publicitários são cada vez mais específicos e pessoalizados, chegando-se a um nível de precisão e eficiência jamais visto (BIONI, 2020).

Dentre as ferramentas utilizadas neste processo, aparecem com maior relevância os chamados *Cookies* , que monitoram o acesso do usuário a *Websites*, identificam e registram quando ele visita determinada página mais de uma vez. Na definição de Ana Cláudia Redecker (2021, p. 52), os *Cookies "*são arquivos que permitem armazenar temporariamente o que o internauta está visitando na rede, como se fosse seu percurso em determinada página de internet capturando interesses e preferências".

Não é diferente no caso das redes sociais, que "acumulam os mais diversos dados pessoais dos seus usuários, que são extraídos ao longo de toda a sua interação com a aplicação", conforme aponta Bioni (2020, p. 18).

Observa-se que o mercado e os métodos de publicidade se alinham sobre o novo paradigma social e econômico, em que a informação, e por consequência os dados pessoais, passam a ostentar valor comercial. A este respeito, Bioni (2020, p. 18) assevera que nesta nova economia os dados pessoais compõem peça fundamental:

> Diversos outros serviços utilizam da mesma técnica, catalogando o comportamento do usuário para, a partir daí, direcionar uma publicidade condizente ao seu perfil inferido. O usuário da rede é, portanto, a todo momento, monitorado, acumulando-se uma série de dados (comportamentais), que são aplicados para a personalização da abordagem publicitária.
> A ciência mercadológica reverte tal vigilância em um conhecimento para agregar eficiência à publicidade veiculada no ambiente virtual, encerrando-se, pois, um ciclo, como acima demonstrado, da economia da informação e do conhecimento. Os dados pessoais dos usuários são uma peça singular dessa engrenagem.

Outro elemento que ganha destaque neste processo de monetização da informação e dos dados pessoas é a figura do *Big Data*, que pode ser definida como a "tecnologia de maior destaque para a estruturação e mineração de uma base de dados". (BIONI, 2020, p. 31). Com as ferramentas oferecidas por esta tecnologia, a captação de informações efetivamente valiosas através dos dados pessoais catalogados se tornou mais fácil.

2.4 Os *Bits* e o *Big Data*

O estágio atual da forma de organização da informação é resultado da evolução de um processo que começou com a criação dos *bits*[4], que consegue organizar toda a informação em unidades pequenas, através de um sistema binário de dígitos (0 ou 1). Através desta forma de organização foi possível a utilização de uma linguagem compreensível para o processamento e armazenamento de informações pelos computadores.

Através dos *bits* desmaterializou-se a informação até então veiculada através de conglomerados de átomos[5] (escrita em papel):

---

[4] um bit (BInaryDigiT) é a menor unidade de medida de transmissão de dados utilizada na computação possui um único valor zero ou um, operando num sistema binário. Disponível em: http://www.sbgames.org/sbgames2017/papers/CulturaShort/175491.pdf > Acesso em: 22 de dez. 2021.

[5] O átomo é a partícula mais pequena que caracteriza um elemento químico. É constituído por um núcleo central extremamente denso, positivamente carregado, constituído por protões e neutrões (o núcleo de hidrogénio é constituído somente por um protão). Disponível em: https://rce.casadasciencias.org/rceapp/art/2014/047. Acesso em 22 de dez. 2021.

> Dessa forma, os bits desmaterializaram a informação, permitindo a sua introdução em computadores. E, com o passar do tempo, todo tipo de informação passou a ser digitalizado, tal como o áudio e o vídeo.
> Isso implicou uma virada exponencial na quantidade de informações processadas. Com a linguagem binária, permitiu-se um acúmulo de informação inimaginável e em novas plataformas – e.g., compact disk (CD), pen drive, computadores pessoais etc.– em comparação ao suporte primitivo dos átomos – papel.
> Para além desse progresso quantitativo, experimentou-se, também, uma mudança de ordem qualitativa no processamento de informações. A técnica binária permitiu que a informação fosse mais precisamente organizada, facilitando, em última análise, o seu próprio acesso. (BIONI, 2020, p. 07).

Com a nova modulação, não seria necessário ao indivíduo esforço hercúleo para encontrar determinado arquivo, parte de determinada pasta, numa sala completamente repleta de papel. Com a digitalização da informação, possibilitada pelo sistema binário dos bits, basta para a localização do arquivo procurado uma pesquisa com seu nome.

Neste sentido, "a 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." (BIONI, 2020, p. 08).

O *big data* representa o ápice de tal revolução, por ser uma tecnologia que permite a estruturação e análise de um volume incomensurável de dados, para diversas finalidades. Nas palavras de Sarlet e Molinaro (2019, p. 183-184), seria "um tratamento de grandes quantidades de dados que visa reconhecer padrões e obter novas percepções a partir deles."

O *big data* opera utilizando-se da linguagem *Not Only Structured Query Language*[6] (NoSQL), que permite um tratamento de dados em variedade, volume e velocidade jamais vistos nas tecnologias de processamento de dados, por dispensar, como a própria sigla já aponta, a onerosa etapa de prévia estruturação de dados para sua alimentação.

Nas palavras de Bioni:

> [...] os dados passaram a ser analisados não mais em pequenas quantidades ou por amostras, mas em toda a sua extensão. Há um salto quanto ao volume de dados processados, tornando-se possível correlacionar uma série de fatos (dados), estabelecendo-se entre eles relações para desvendar padrões e, por conseguinte, inferir, inclusive, probabilidades de acontecimentos futuros.
> Por esse motivo, o Big Data não é um sistema inteligente. Não se trata de ensinar o computador a pensar como um ser humano, trata-se apenas de uma

[6] NoSQL - segundo (Tiwari, 2011) é um termo que designa todas as bases de dados que não seguem os princípios das bases de dados relacionais e que estão relacionados com grandes volumes de dados. Disponível em: https://recipp.ipp.pt/bitstream/10400.22/6375/1/DM_RicardoCardoso_2012_MEI.pdf. Acesso em 22 de dez. 2021.

> nova metodologia para que tal ferramental processe e organize dados para inferir a (re)ocorrência de acontecimentos. (BIONI, 2020, p. 36).

Através do referido sistema, que evidencia a probabilidade de um evento através de sua recorrência quando presentes uma série de fatos e padrões, é possível, "por exemplo, inferir a probabilidade de que uma consumidora esteja grávida, verificando-se que uma determinada lista de produtos é recorrentemente adquirida por tal tipo de cliente." (BIONI, 2020, p. 36).

O exemplo citado não o foi à toa, trata-se de um dos casos clássicos quando o assunto é demonstrar, na prática, como se opera o *Big Data*. O episódio ficou conhecido como *Target Case*[7]. A *Target* é uma empresa americana de varejo que, com base no histórico de compras de seus clientes, conseguiu traçar um perfil de consumidoras que adquiriam determinados produtos, típicos dos necessários no estágio da gravidez.

A história tomou forma quando um pai extremamente irritado entrou numa loja *Target*, em Mineápolis, procurando o gerente do estabelecimento e estarrecido com o fato de a loja estar enviando à sua filha livretos com promoções de fraldas, berços e roupinhas de bebê, posto que a filha dele ainda estava no colegial[8]. Dias depois, através de ligação telefônica, o referido pai se desculpou com a loja e noticiou ter tomado conhecimento de que, de fato, a jovem estava grávida e não tinha contado à família quando do acontecimento do episódio.[9]

Este caso nos demonstra a capacidade do *Big Data* na correlação de acontecimentos e padrões de comportamento. O estágio atual permite ao *Big Data* prever crises financeiras, surtos de doenças contagiosas e até mesmo o rompimento de relacionamentos de usuários do *Facebook* com base em suas postagens. (BIONI, 2020).

Como se vê, a temática da proteção de dados pessoais na sociedade da informação reveste-se de extrema importância, tendo em vista que através da captação e cruzamento de dados é possível não somente deduzir as predileções dos usuários da internet, mas também prever seu comportamento e auferir lucro com o compartilhamento de tais recursos.

---

[7] O que o case da rede varejista Target, que "descobriu" a gravidez de uma jovem antes mesmo de seus pais, pode nos ensinar sobre privacidade de dados e LGPD. Disponível em: https://rox.cx/privacidade-de-dados-e-lgpd/. Acesso em 11 de out. 2021.

[8] Idem.

[9] Idem.

3 A tutela jurídica de dados na sociedade da informação

Expôs-se que estamos vivenciando um momento de ruptura histórica, em que as tecnologias da informação começam a assumir as engrenagens sociais para redefinir como o ser humano opera suas relações pessoais, profissionais, políticas e sociais.

A informação, tal qual a sua forma mais bruta (o dado), passam a ostentar valor não só econômico, mas social e político, reclamando do direito, tanto em sua esfera legislativa quanto interpretativa, a preocupação em relação a este fenômeno que inaugura, na era da pós-modernidade, um novo paradigma (BIONI, 2020).

Nesse contexto, surge uma discussão doutrinária a respeito da natureza jurídica da proteção de dados que, basicamente, se divide em dois entendimentos: o primeiro, de que a proteção de dados estaria dentro da tutela da privacidade; e o segundo, que defende a autonomia do direito à tutela dos dados enquanto um direito autônomo, classificado, inclusive, como direito fundamental e da personalidade.

Isto posto, para analisar a função do consentimento no sistema regulatório de dados brasileiro, se faz necessário refletir sobre a valoração dos dados pessoais enquanto bem jurídico, especialmente no que se refere a aplicação e interpretação das normas de proteção vigentes.

3.1 A proteção de dados enquanto desdobramento da tutela da privacidade

A Constituição da República Federativa do Brasil - CRFB/88, em seu art. 5. º, incisos X e XII, tutela enquanto direitos fundamentais respectivamente a intimidade e a vida privada; e o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas. Diante de tal previsão constitucional, existe a interpretação de que a proteção de dados pessoais seria um desdobramento do direito à privacidade, mais ainda em razão de a Carta Magna ter instituído um remédio constitucional que serve, basicamente, ao acesso e retificação de dados – o *habeas data*, previsto em seu art. 5.º, inciso LXXII.

Tal interpretação traz um ponto positivo: o reconhecimento de que a proteção de dados pessoais encontra amparo constitucional, enquanto desdobramento de um direito fundamental. No entanto, a adoção do entendimento de que a proteção de dados pessoais seria uma espécie da proteção à privacidade representa uma limitação hermenêutica que destoa da necessidade atual da proteção da informação em si, que seria desprestigiada perante a tutela pura e simples da esfera privada ou do sigilo das comunicações do indivíduo (DONEDA, 2019).

Ao discorrer sobre o tema, Doneda (2019, p. 263) aponta que a limitação da proteção de dados ao campo da privacidade não abarca a complexidade da matéria no contexto da sociedade informatizada:

> A leitura das garantias constitucionais para os dados somente sob o prisma de sua comunicação e de sua eventual interceptação lastreia-se em uma interpretação que não chega a abranger a complexidade do fenômeno da informação ao qual fizemos referência. Há um hiato que segrega a tutela da privacidade, esta constitucionalmente protegida, da tutela das informações pessoais em si – que, para a corrente mencionada, gozariam de uma proteção mais tênue. E esse hiato possibilita a perigosa interpretação que pode eximir o aplicador de levar em conta os casos nos quais uma pessoa é ofendida em sua privacidade – ou tem outros direitos fundamentais desrespeitados – não de forma direta, porém por meio da utilização abusiva de suas informações pessoais em bancos de dados. Não é necessário ressaltar, novamente, o quanto hoje em dia as pessoas são reconhecidas em diversos relacionamentos somente de forma indireta, pela representação de sua personalidade que é fornecida pelos seus dados pessoais, ressaltando, ainda mais, a importância da proteção de tais dados para a proteção da identidade e personalidade de cada um de nós.

Uma proteção que se faz presente tão somente em situações extraordinárias (violação do sigilo, das comunicações) não se mostra suficiente à tutela dos dados pessoais, sobretudo em relação à regulamentação de seu tratamento e à vinculação deste às finalidades para que foi proposto. O que se quer dizer, trocando em miúdos, é que a complexidade da tutela da informação, em si considerada, reclama do legislador e do intérprete a adoção de um critério interpretativo que não limite a extensão da proteção e que não permita situações de grande permissividade, como vem a ser o caso da sua vinculação à tutela da privacidade.

Com este espírito, boa parte da doutrina, legisladores e jurisprudência sustenta o reconhecimento da proteção de dados enquanto direito fundamental autônomo (LIMA, 2020).

Neste contexto, destaca-se a Proposta de Emenda à Constituição (PEC) n. ° 17/2019[10], que visa alterar a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

[10] O Plenário do Senado Federal aprovou, na quarta-feira (20), a Proposta de Emenda à Constituição (PEC) 17/2019, que torna a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental. A PEC também remete privativamente à União a função de legislar sobre o tema. Por acordo entre as lideranças, foram votados os dois turnos na mesma sessão. Aprovada de forma unânime, a PEC recebeu 64 votos no primeiro turno e 76 no segundo (o mínimo exigido é de 49). O texto segue agora para promulgação, em sessão do Congresso Nacional ainda a ser marcada. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/senado-federal-aprova-proposta-de-emenda-a-constituicao-17-pec-17-2019-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-e-garantias-fundamentais. Acesso em: 14 de dez. 2021.

Veja-se o teor da proposta:

> Art. 5° ~[...]
> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;"
> [...]
> Art. 22. Compete privativamente à União legislar sobre:
> [...]
> XXX – proteção e tratamento de dados pessoais.

A PEC n. ° 17/2019 já conta com a aprovação tanta pela Câmara dos Deputados quanto pelo Senado Federal, restando pendente tão somente a sua promulgação em sessão do Congresso Nacional.

Nas palavras Doneda (2020, p. 264), em sendo incorporada a proposta, será proporcionada "certa 'equalização' entre uma série de direitos fundamentais que possuem repercussão direta sobre dados pessoais, como o direito à privacidade, o direito à informação e a transparência."

Para além disso, o alçar do direito à proteção de dados pessoais ao status constitucional autônomo, seguido da estipulação de competência legislativa privativa da União sobre o tema, colocará a questão da tutela de dados na sociedade da informação no lugar que a mesma requer, dada sua importância no momento contemporâneo.

3.2 A proteção de dados enquanto direito da personalidade

A proteção de dados pessoais, como defende parte da doutrina, não deve encontrar limite na tutela da privacidade, fazendo-se necessária uma releitura do enquadramento do referido direito enquanto figura jurídica autônoma. Neste contexto, a sua qualificação como direito da personalidade surge como solução da questão. Façamos um apanhado histórico em relação aos direitos da personalidade e a exposição dos motivos que ensejam a adoção da referida qualificação.

O trajeto dos direitos da personalidade perpassa, antes de mais nada, pela reconstrução ou redefinição do conceito jurídico de "pessoa" ocorrida na segunda metade do século XX. Como cediço, após as duas grandes guerras, palcos de exemplos constantes de desumanidade,

verificou-se que a tutela jurídica da pessoa humana não mais podia ser limitada à compreensão formal e objetiva do indivíduo enquanto sujeito de direitos.

Neste contexto, sobretudo após a Declaração De Direitos Universais da Organização das Nações Unidas, o aspecto subjetivo do ser humano passa a ser valorado com mais ênfase, sendo esta mudança de paradigma guiada pela dignidade da pessoa humana enquanto "metaprincípio", conforme conceituado por Alinne Cardim Alves e Juliana Cristina Borcat (2013, p. 3). A referida mudança coloca o ser humano (material e subjetivamente considerado) no eixo gravitacional da proteção jurídica pensada dali em diante, calcada na positivação dos definidos direitos humanos e na tutela da personalidade. A este respeito, Alves e Borcat (2013, p. 03) discorrem:

> Com a reconstrução dos direitos fundamentais, após a Segunda Guerra Mundial, ocorreu também a reconstrução dos direitos da personalidade, e o metaprincípio da dignidade da pessoa humana passou a ser o guia de todos os demais direitos, alçando a pessoa ao centro do ordenamento jurídico, passando, então, a ser vista não mais como um mero titular de direitos e sim como o ser humano real que sofre, se alegra, tem vontade, sentimentos, aspirações, preferências, dentre outros valores.
>
> A personalidade nesse contexto passa a ser vista como uma característica inata ao ser humano, sendo-lhe indissociável, portanto, a verdadeira proteção jurídica dos direitos da personalidade tem vinculação total com a positivação dos direitos humanos dentro do ordenamento jurídico brasileiro, passando, então, a serem conhecidos como direitos fundamentais em decorrência das desumanidades provocadas nas grandes guerras mundiais.

A pessoa humana deixa de ser tratada enquanto sujeito de direito formalmente considerada para ser enxergada como "o ser humano real, que sofre, se alegra, tem vontade, sentimentos, aspirações, preferências e não somente alguém que tem aptidão para adquirir direitos e deveres." (Alves e Bocart, 2013, p. 05). Ocorre, efetivamente, a positivação de direitos humanos, acompanhada, igualmente, da tutela jurídica dos direitos da personalidade.

A personalidade, por sua vez, corresponde ao conjunto de características que servem para distinguir um ser humano do outro (BIONI, 2020). Seriam, por assim dizer, características pessoais, atribuíveis a cada um em sua individualidade. Neste contexto, Danilo Doneda (2019, p. 148) aponta que a informação pessoal se liga ao seu titular por um elo que não pode ser desfeita pelo tratamento de dados:

> A informação pessoal, em um certo sentido, pode ser desvinculada da pessoa: ela pode circular, submeter-se a um tratamento, ser comunicada, etc. Contudo, até o ponto em que continua sendo uma informação "pessoal", isto é,

> identificando a pessoa a qual se refere, a informação mantém um vínculo indissolúvel com a pessoa, e sua valoração específica deve partir basicamente dela ser uma representação direta da pessoa. Por força do regime privilegiado de vinculação entre a informação pessoal e a pessoa à qual ela se refere – como representação direta de sua personalidade –, tal informação deve ser entendida, portanto, como uma extensão da sua personalidade.

Portanto, os dados pessoais, enquanto extensão do ser humano e reveladores da identidade, reclamam uma proteção que extrapola a privacidade, tendo em vista que ainda que sejam públicas, determinadas informações reclamam proteção para efetivamente reproduzirem a verdade. De maneira mais objetiva, não se trata apenas de proteger aquilo que é íntimo ou privado de cada um, mas a qualidade das informações que são emitidas a respeito do indivíduo.

Neste sentido, importante o esclarecimento de Bioni (2020, p. 57):

> Trata-se de um novo tipo de identidade e, por isso mesmo, tais dossiês digitais devem externar informações corretas para que seja fidedignamente projetada a identidade do titular daquelas informações.
> Isso acaba por justificar dogmaticamente a inserção dos dados pessoais na categoria dos direitos da personalidade, assegurando, por exemplo, que uma pessoa exija a retificação de seus dados pessoais para que a sua projeção seja precisa.

Neste diapasão, verifica-se como a limitação da análise dos dados pessoais à ótica da privacidade é equivocada, posto que a bipartição entre o público e o privado, inerente ao tratamento da matéria, não se mostra suficiente à tutela da informação em todas as nuances necessárias, sobretudo porque não é somente o dado privado ou íntimo que reclama proteção. Um exemplo claro da ineficiência da privacidade enquanto gênero do direito à proteção de dados se refere ao uso dos mesmos para finalidade diversa da que foi inicialmente estipulada. Para tal situação, a tutela da privacidade não oferece qualquer resguardo que fundamente a sua coibição, sobretudo se o dado fornecido se revestir do caráter público.

Mais uma vez, pertinente a lição de Bruno Bioni (2020, p. 58):

> Seria contraproducente e até mesmo incoerente pensar a proteção de dados pessoais somente sob as lentes do direito à privacidade. O eixo da privacidade está ligado ao controle de informações pessoais do que seja algo íntimo ou privado do sujeito.
> A proteção dos dados pessoais não se satisfaz com tal técnica normativa, uma vez que a informação pode estar sob a esfera pública, discutindo-se, apenas, a sua exatidão, por exemplo. Ao lado do princípio da qualidade dos dados, o direito de correção é uma construção que deriva da perspectiva da identidade do sujeito e não do direito à privacidade. É o primeiro direito de personalidade que determina a necessidade de haver uma correspondência fidedigna entre a

> pessoa e seus dados pessoais. A esfera do que é público ou privado revela-se incompleta para dar vazão a esse tipo de dinâmica normativa.

Neste sentido, mais do que cabível a adequação da proteção de dados pessoais como um novo direito da personalidade, esta revela-se necessária ao processo de interpretação e utilização das ferramentas de proteção disponíveis para tanto.

3.3 O tratamento legal dos dados pessoais

O termo "dado pessoal" corresponde a "todas as informações de caráter personalíssimo caracterizadas pela identificabilidade e pela determinabilidade do seu titular" (LIMA, 2020, p. 19). Na definição de Patrícia Peck Pinheiro (2018, p. 25), dado pessoal diz respeito a:

> Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva.

Já a Lei Geral de Proteção de Dados - LGPD, define dado pessoal, em seu artigo 5.º, inciso I, como sendo "informação relacionada a pessoa natural identificada ou identificável".

O conceito de dado pessoal reveste-se de imensurável importância, pois serve como parâmetro de alcance para a proteção jurídica estudada. Em outras palavras, o dado que não ostentar a condição de pessoal não merecerá a proteção encampada pela LGPD.

Neste contexto, o caráter pessoal do dado está presente quando a informação pode revelar uma pessoa identificável, indeterminável, sendo fruto de um vínculo mediato ou indireto, inexato (BIONI, 2020). Pela literalidade do conceito adotado pela LGPD, verifica-se que a espécie normativa anuncia um conceito aberto e que, por conseguinte, reclama um preenchimento de sentido, uma análise contextual.

As hipóteses de tratamento de dados pessoais estão elencadas, de forma específica, no artigo 7.º da LGPD, que enuncia em seu inciso I ser necessário "o fornecimento de consentimento pelo titular".

3.4 Dado pessoal sensível

A definição de dado pessoal sensível constante do art 5.º, inciso II, da LGPD, remete-se a um núcleo mais privado do indivíduo, relacionando-se a informações sobre:

> (...) origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Neste sentido, Pinheiro (2018, p. 25) define que os dados sensíveis são os que "estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais". Os referidos dados merecem proteção especial, tendo em vista que a sua violação implica risco considerável à esfera mais íntima da pessoa e, em última medida, aos suas liberdades fundamentais.

Tais riscos variam conforme fatores sociais e culturais, estando a característica da sensibilidade diretamente relacionada ao risco que sua divulgação pode ocasionar ao seu titular, devidamente considerado o contexto no qual este está inserido. Neste sentido, Doneda (2019, p. 143) aponta que:

> A criação de uma categoria de dados sensíveis foi fruto da observação pragmática sobre a diferença dos efeitos do tratamento desta categoria de dados em relação aos demais. E foi este idêntico impulso pragmático que fez com que se percebesse mais claramente a necessidade de exorbitar os cânones "tradicionais" ligados à privacidade, ao revelar a presença de um outro valor digno de tutela como fundamento da tutela da pessoa neste caso, que é o princípio da igualdade material. A própria seleção de quais seriam estes dados considerados sensíveis provém da constatação de que a circulação de determinadas espécies de informação apresentariam um elevado potencial lesivo aos seus titulares, em uma determinada configuração social.

O autor arremata (2019, p. 144):

> O regime adotado em relação aos dados sensíveis varia de acordo com as concepções a este respeito em cada ordenamento jurídico. Em verdade, é necessário ter em conta que a diferenciação conceitual dos dados sensíveis atende a uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior[...].

Tendo em vista esta proteção especial, o consentimento enquanto condicionante do tratamento dos dados pessoais sensíveis aparece na LGPD de maneira diversa do que estabelece o art. 7.º para a proteção de um dado caracterizado como meramente pessoal. Neste contexto, o

art. 11 da norma citada classifica o consentimento, criando a necessidade de que o mesmo seja dado “de forma específica e destacada, para finalidades específicas”.

Esta diferenciação, para além de já apontar para uma variação de estruturação do consentimento no processo de proteção jurídica dos dados (o que resvala no objeto deste trabalho), revela que a tutela da informação transborda ao direito à privacidade, voltando-se, especificamente quanto aos dados sensíveis, à igualdade e isonomia, apresentando-se como verdadeira combatente das condutas discriminatórias (BIONI, 2020).

3.5 Dado anonimizado e o processo de anonimização

A LGPD, em seu art. 5.º, III, refere-se ao dano anonimizado como sendo o “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”.

O dado anônimo seria o completo oposto de dado pessoal, correspondendo a um dado pelo qual não se poderia chegar à identificação de uma pessoa. Esta impossibilidade de identificação apresenta-se como resultado de uma operação que separa os dados dos seus titulares. A tal processo dá-se o nome de anonimização. (BIONI, 2020). O bojo deste processo é composto por várias técnicas, dentre as quais generalização, supressão, randomização e pseudoanonimização.

A título exemplificativo, pertinente transcrever uma demonstração prática de como se dariam as duas primeiras técnicas (BIONI, 2020, p. 62):

> **a)** **supressão do CPF**: por ser um identificador capaz de diferenciar até mesmo pessoas homônimas, sendo um identificador único; logo, a sua disponibilização, ainda que parcial – e.g., cinco primeiros dígitos –, não seria prudente;
> **b)** **generalização do nome completo**: constaria apenas o prenome, desde que fosse observado que os nomes da base de dados não são comuns. O objetivo é evitar que um nome possa ser atribuído a um indivíduo em específico;
> **c)** **generalização da localização geográfica**: em vez de disponibilizar o número completo do CEP, seriam divulgados apenas os seus primeiros dígitos. Assim, haveria uma localização menos detalhada, a fim de quebrar o vínculo de identificação desta informação com um sujeito;

O processo de anonimização deve ser tão bem elaborado que sequer deve ser possível a quem lhe deu origem identificar, novamente, os titulares de dados inicialmente conhecidos (BIONI, 2020). No entanto, tal possibilidade tem se mostrado cada vez mais improvável

teoricamente, sobretudo com a criação de algoritmos que atuam através do cruzamento de informações oriundas de várias bases de dados para se identificar o titular do dado que, inicialmente, era anonimizado.

Nas duas últimas décadas, destacaram-se os pesquisadores Arvind Narayanan e Vitaly Shmatikov, que atuaram na identificação, através de algoritmos, de usuários protegidos, em tese, pelo processo da anonimização. Neste contexto, relevante caso ganha importância: o caso *Netflix Prize*, que serve para demonstrar que sempre será possível, através da complementação com outras bases de dados, identificar titulares de dados anônimos.

A respeito do caso *Netflix Prize*, Bioni (2020, p. 64) comenta:

> À época, a maior provedora de streaming de filmes do mundo criou um concurso, cujo desafio era melhorar o seu algoritmo de sugestão de filmes. Então, a Netflix disponibilizou a sua base de dados com todas as avaliações dos filmes de seu catálogo do período de 1998 a 2005, suprimindo os nomes dos usuários avaliadores e deixando somente a data e a nota da avaliação.
> A fim de tornar tal processo de reidentificação mais robusto, a Netflix se utilizou da técnica de randomização. Ela alterou algumas datas e ratings das avaliações dos seus consumidores, o que aumentaria o risco de "falsos positivos", a não ser pelo fato de o algoritmo dos pesquisadores ter sido projetado para isso.
> Os pesquisadores "rodaram" tal algoritmo na base de dados disponibilizada, descobrindo que seria necessário entre 3 (três) e 19 (dezenove) bits de informação para reverter o processo de anonimização. Esse pool de informações necessário estava publicamente disponível e acessível na Internet Movies Databases/IMDB94.
> O IMDB é um website onde as pessoas compartilham suas impressões sobre filmes,utilizando-se, na maioria das vezes, dos seus nomes reais. Desta forma, os pesquisadores "cruzaram" essas informações com a base de dados da Netflix, correlacionando as datas das avaliações dos filmes e seus respectivos scorings. Assim, a peça faltante do quebra-cabeça – a identidade dos usuários da Netflix – foi desvendada com base nos nomes contidos nas avaliações do IMDB95.
> O exemplo em questão é simbólico, pois sublinha o "calcanhar de Aquiles" dos dados anônimos. Sempre existirá a possibilidade de uma base de dados anonimizada ser agregada a outra para a sua reidentificação.

O referido caso causa espécie, ao evidenciar ser possível identificar uma pessoa em razão dos rastros que ela deixa em sua navegação pela internet, mesmo quando o ponto de partida para tal identificação seja dados que estariam supostamente protegidos pelo sistema de anonimização.

Atribui-se a esta constatação, inclusive, a prevalência do conceito expansionista de dados na legislações protetivas e na literatura, pelo qual dado pessoal seria "uma informação que, direta ou indiretamente, identifica um sujeito"(BIONI, 2020, p. 64).

Com a adoção do referido conceito, não haveria, conforme as lições de Bruno (2020, p. 85), lugar para dicotomia entre dados pessoais e dados anônimos:

> Por essa lógica, qualquer dado pessoal anonimizado detém o risco inerente de se transmudar em um dado pessoal. A agregação de diversos "pedaços" de informação (dados) pode revelar (identificar) a imagem (sujeito) do quebra-cabeça, a qual era até então desfigurada (anônimo) – o chamado efeito mosaico.
> Por isso, em princípio, eventual dicotomia entre dados pessoais e dados anônimos só guardaria coerência junto ao conceito reducionista de dados pessoais. Isso porque dados anônimos não são dados relacionados a uma pessoa identificada, demandando a reversão do processo de anonimização para se chegar aos respectivos titulares, sendo a sua identificabilidade remota (identificável) e não imediata (identificada).

A LGPD adotou o referido critério expansionista na definição do que vem a ser dado pessoal (art. 5.º, I). No entanto, valendo-se do critério da razoabilidade, optou por também qualificar, de forma diferenciada, o dado anonimizado. A adoção do critério da razoabilidade afasta a aparente redundância normativa, já que, pelo critério expansionista, todo dado que torne o indivíduo identificável – incluindo-se o dado anonimizado – poderia ser considerado dado pessoal (BIONI, 2020).

3.6 Tratamento de dados

Partindo da definição trazida pela LGPD, o termo "tratamento", conceituado no art. 5.º, X, diz respeito a:

> (...) toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

A lei 13.709/2018 delimita, também, um capítulo específico (capítulo II) para estabelecer as diretrizes, limites e hipóteses em que se admitirá o tratamento de dados. O art. 7.º[11], que inaugura o referido capítulo, traz, em seu caput, uma definição restritiva para o

[11] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

tratamento de dados, ao anunciar que "somente poderá ser realizado" nas hipóteses ali constantes. Nesse contexto, o primeiro inciso do referido artigo já vincula o tratamento de dados ao ponto que se faz objeto da presente reflexão, ao condicioná-lo ao "fornecimento de consentimento pelo titular".

Não obstante, para além da figura do consentimento, outros fatores norteiam o tratamento de dados. Neste particular, evidencia-se a influência e inspiração direta ao *General Data Protection Regulation* - GDPR[12] na modulação do modelo normativo brasileiro, que enuncia como valores imprescindíveis ao regular tratamento de dados a observância de

---

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
§ 1º Nos casos de aplicação do disposto nos incisos II e III do caput deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados. (Revogado pela Medida Provisória nº 869, de 2018)
§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)
§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do caput do art. 23 desta Lei poderá ser especificada pela autoridade nacional. (Revogado pela Medida Provisória nº 869, de 2018)
§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência
§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.
§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência

[12] O Regulamento Geral de Proteção de Dados (GDPR) é a lei de privacidade e segurança mais rígida do mundo. Embora tenha sido elaborado e aprovado pela União Europeia (UE), ele impõe obrigações às organizações em qualquer lugar, desde que visem ou coletem dados relacionados a pessoas na UE. O regulamento entrou em vigor em 25 de maio de 2018. O GDPR aplicará multas severas contra aqueles que violarem seus padrões de privacidade e segurança, com penalidades que podem chegar a dezenas de milhões de euros. Disponível em: < https://gdpr-eu.translate.goog/what-is-gdpr/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em: 12 dez. 2021.

princípios como boa-fé, finalidade, lealdade, transparência, exatidão, limite, proporcionalidade, integridade e confidencialidade. (PINHEIRO, 2020).

Boa parte dos princípios citados, além de outros como adequação, necessidade, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação, responsabilização e prestação de contas, estão previstos no art. 6.º da LGPD, que não apresenta natureza taxativa, conforme previsão expressa contida no art. 64 do mesmo diploma. (LIMA, 2020).

A observação dos referidos princípios nos revela que o espírito da LGPD, tal qual a GDPR, eleva a participação do indivíduo, instrumentalizada pelo consentimento, no processo de tratamento de dados. A este respeito, Chiara Spadaccini de Teffé (2020, p. 5) conclui:

> Uma análise minuciosa dos princípios – que têm grande parte de seu centro gravitacional baseado no ser humano –revela a preocupação do legislador com a participação do indivíduo no fluxo de suas informações. Como será exposto, no texto legal, a caracterização do consentimento segue a linha do Regulamento europeu e das normas mais atuais sobre o tema. Há também uma série de disposições que oferecem regramento específico para concretizar, orientar e reforçar o controle dos dados através do consentimento.

Ressalvadas poucas hipóteses constantes do art. 7.º da Lei 13709/2018, todo o tratamento de dados deverá perpassar pelo crivo do consentimento do titular, sendo este o grande lastro da proteção normativa vigente. A questão que emerge é: o indivíduo detém condições de consentir diante da sua vulnerabilidade enquanto usuário da internet?

4. O consentimento e as normativas de proteção de dados brasileiras

A evolução dos meios de comunicação pela internet, sobretudo através dos dispositivos de telefonia móvel, tem alterado substancialmente as dinâmicas das relações sociais, em todos os âmbitos. Nesse contexto, tornou-se raro um indivíduo que não possua, ao menos, uma rede social ou forma de comunicação que se dê por meio virtual.

4.1 A proteção de dados e a figura do consentimento

O questionamento fulcral que se levanta é se existe, de fato, um consentimento firmado sob uma manifestação de vontade hígida, diante da vulnerabilidade do usuário da internet e da sua necessidade de integração virtual no mundo pós-moderno. Este questionamento resume o cerne da problemática que se busca fustigar. Entretanto, antes de se ater a este ponto principal, façamos uma análise a respeito da figura do consentimento em si considerada.

Pois bem, ao se debruçar sobre a temática, Doneda (2019, p. 296), de início, já anuncia que "o consentimento do titular para o tratamento de seus dados pessoais é um dos pontos mais sensíveis de toda a disciplina de proteção de dados pessoais". Ainda segundo o referido autor (2019, p. 296-297), "o direito civil tem a oportunidade de estruturar, a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos desse consentimento à natureza dos interesses em questão."

A ideia trazida pelo referido autor se reveste numa crítica à transposição, pura e simples, do consentimento ordinariamente manifestado em relações patrimoniais às questões envolvendo a tutela dos dados pessoais. Neste sentido, o intérprete teria a tarefa de dar ao consentimento uma interpretação que lhe considere como "o instrumento por excelência da manifestação da escolha individual, ao mesmo tempo em que faça referência direta aos valores fundamentais em questão." (DONEDA, 2019, p. 297).

Neste exercício interpretativo, faz-se necessária a reflexão a respeito dos riscos de se importar para as normas protetivas de dados pessoais uma noção contratualista do consentimento. Doneda (2019, p. 297) aponta:

> Ao encarar essa tarefa dentro da estrutura dogmática do direito civil, é necessário ter em mente a advertência que Messinetti faz sobre os riscos de um "neo-dogmatismo fraco", ou seja, a utilização de categorias dogmáticas tradicionais afastadas de seu âmbito teórico original, com a consequência de

> “atenuar sua relação com as rationes sistemáticas que a tradição dogmática nelas condensava, além da progressiva diminuição do grau de especificidade de problemas e remédios que tal tradição pretendia, com estas categorias, abranger.”

Ao ignorar tal questão, o intérprete acabaria por outorgar ao consentimento uma função mais danosa do que protetiva, legitimadora de um sistema de monetização e exploração dos dados pessoais disponibilizados na internet.

Neste contexto, a noção patrimonialista de consentimento, calcada na autonomia privada, é insensível a situações concretas em que o indivíduo se vê, frente à decisão de consentir ou não com a utilização ou compartilhamento de seus dados, numa situação em que acabará por abrir mão de determinado bem (imediatamente desejado) se escolher não consentir. O desequilíbrio entre o consentidor e o receptor de dados acaba por oferecer ao primeiro, não raro, a dura escolha do “tudo ou nada”, do “pegar ou largar” conforme aponta Doneda (2019, p. 299).

Nessa conjuntura, é reservada ao titular de dados pessoais uma posição de passividade que se disfarça sob o manto da autonomia e liberdade do indivíduo, materializada nos termos de uso e de consentimento à política de privacidade e compartilhamento de dados operada.

Debruçando-se sobre a questão, Maria Cristina Cereser Pezzella e Silvano Ghisi (2015, p. 15) asseveram que “a liberdade informativa dos indivíduos é fortemente relativizada na Sociedade da Informação, pois a circulação de informações passa a constituir pressuposto para participação em oportunidades e acessos dos mais variados”.

Neste mesmo sentido, Bioni (2020, p. 157) assevera:

> Na verdade, a lógica do mercado e da sociedade da informação arquitetam essa (falsa) escolha, já que, para fazer parte do jogo, deve-se aceitar o convite mediante o“ concordo” em compartilhar os “meus” dados pessoais. Daí por que a proteção dos dados pessoais geraria um custo social, qual seja, a não fruição dessas oportunidades que resultaria em uma eremitania na sociedade da informação.

Além disso, a ausência de um dimensionamento claro ao usuário a respeito da utilização de seus dados e das consequências advindas deste uso tornam o consentimento, na interpretação do homem médio, meramente um aceite burocrático que precede à contratação de algum bem ou serviço. A falta de clareza e nitidez a respeito do tratamento de dados, deste modo, pode ser causa concorrente ao esvaziamento dos mecanismos de proteção da informação fundados na autodeterminação (consentimento). (DONEDA, 2019).

Estes fatores relevam que uma interpretação equivocada do consentimento, de forma pretérita à discussão a respeito de sua eficiência enquanto baluarte normativo de proteção, já colaria em xeque a sua funcionalidade. A este respeito, importante a lição de Doneda (2019, p. 300):

> Esse conjunto de características permite caracterizar esse consentimento, se o cotejarmos com a função que dele se pretende, qual seja a de ser um instrumento para a livre construção da esfera privada, "uma ficção". Sua utilização pode ser instrumentalizada pelos interesses que pretendem que seja não mais que uma via para legitimar a inserção dos dados pessoais no mercado. Por outro lado, o consentimento pode ser incentivado pelo próprio Estado sob a (falsa) premissa de conceder aos cidadãos um instrumento forte e absoluto para determinar livremente a utilização de seus próprios dados pessoais – conforme observou Stefano Rodotà, o Estado assim teria um falso álibi para não intervir em uma situação na qual deveria agir positivamente na defesa de direitos fundamentais – e, assim, "lavar as mãos".

O consentimento posto desta forma, pela leitura proposta pelo autor, serviria como um catalizador das relações privadas, consideradas puramente sob a égide da manifestação da vontade, trajada em vestes de instrumento garantidor da liberdade das partes, em detrimento da proteção da informação fornecida. Esta, por sua vez, só poderia ser tutelada *a posteriori*, mediante a demonstração de que a manifestação de vontade apresenta algum vício.

Portanto, de maneira primeva à discussão a respeito do papel do consentimento, pode-se inferir que a delimitação dos parâmetros que devem guiar a interpretação do conceito e natureza jurídica da figura do consentimento é de extrema relevância para a temática.

4.2 Capacidade de consentir

A análise do consentimento perpassa pela complexidade da proteção de dados em si considerada. Esta, por sua vez, é atingida pela fluidez do trânsito de informações e da captação destas na economia de vigilância.

Quando o assunto é captação de dados, muitos indicam a semelhança do atual sistema socioeconômico com a distopia retratada no romance *1984*[13], de George Orwell, em que a figura do Grande Irmão vigiava a tudo e a todos. No entanto, diferentemente da sociedade fictícia da

[13] A obra apresenta, num mundo distópico de uma Londres presa em um regime ditatorial que retém e edita as informações de seus cidadãos, a fim de assegurar seu controle, aprisionar a liberdade e o discurso de ódio se tornam norma, um homem de meia idade – Winston Smith – que resiste e rebela-se contra o sistema buscando elementos do passado, da história e da memória, de si e do mundo que o rodeia, buscando através disto sua própria identidade. Disponível em: https://clickmuseus.com.br/verdade-e-memoria-analise-da-construcao-do-passado-em-1984-de-george-orwell. Acesso em 22 de dez. 2021.

obra, a realidade aponta para a descentralização desta vigilância, tornando o processo de captação de informações quase que onipresente. Fazendo uma análise da referida obra, Bioni (2020, p. 135-136) aponta que a teletela orwelleana é substituída por várias microtelas de smartphones:

> Complementarmente, a teletela é substituída por inúmeras "microtelas". Dos aparelhos celulares smartphones aos trackers (subcapítulo 1.2.2.2 supra), desenha-se uma arquitetura de vigilância que mapeia todos os hábitos dos cidadãos. Com a Internet das coisas há, por exemplo, o estreitamento dos mundos off-line e on-line e, por conseguinte, a difusão dessa vigília. Há, em suma, a datificação das vidas dos cidadãos, que é o pressuposto de uma vigilância ubíqua a movimentar a roda da economia de dados.
> A vigilância está distribuída. Das figuras homogêneas e centrais do Big Brother e da teletela, expande-se o ato de vigiar – em um movimento descentralizador e mais plural – pela presença de múltiplos observadores e pela penetração de inúmeras e novas tecnologias para tal propósito.
> Em suma, a vigilância não é mais ostensiva como no romance 1984. Ela passa a ser mais opaca como decorrência lógica dessa dispersão. As suas características sólidas e bem delimitadas derretem-se nesse processo de distribuição em que o vigia e a sua atividade tornam-se mais voláteis.

Essa vigilância distribuída apresenta-se como um desafio à normatização da proteção de dados. A captação de dados, neste contexto, se daria por inúmeros atores que fomentam o compartilhamento de informações com vistas ao mesmo fim: a sua exploração econômica.

Citando as proposições de Zygmunt Bauman e David Lyon, Bioni (2020, p. 137) assevera que a vigilância "não tem mais as características de firmeza e solidez, tal como se propunha a figura de um único observador e a sua atividade ostensiva de vigiar.". Neste contexto, "ela está diluída no arranjo socioeconômico contemporâneo no qual os dados fluem por inúmeros atores e sensores, os quais, como uma esponja, absorvem-nos para sua exploração econômica." (BIONI, 2020, p. 137).

Isto posto, possivelmente temos um dilema maior do que o enfrentado na distopia de Orwell, dada a descentralização da vigilância. Neste sentido, a complexidade do fluxo informacional aponta para a necessária reflexão a respeito da capacidade do indivíduo controlar seus dados, bem como as suas limitações, que não podem passar despercebidas em função da sustentada autodeterminação informacional (consentimento).

O questionamento que se levanta diz respeito à capacidade do indivíduo comum entender o complexo sistema de captação e tratamento de dados e, mais do que isso, reunir as condições para decidir, em cada situação concreta lhe apresentada, se deve ou não consentir aos "termos e condições de uso".

Neste contexto, ganham ênfase duas teorias. A primeira delas é a Teoria da Decisão da Utilidade Subjetiva, que, segundo Bioni (2020, p. 140), afirma ter o ser humano a "tendência de focar nos benefícios imediatos, o que, de acordo com o arranjo e os modelos de negócios da economia informacional, é representado pelo acesso a um produto ou serviço on-line."

Ao se analisar o processo de outorga do consentimento verifica-se que, efetivamente, não há um dimensionamento claro ao usuário a respeito das consequências daquela manifestação de vontade. Este, portanto, não consegue mensurar sequer quais são as consequências que seu ato pode desencadear. Por outro lado, o bem ou serviço condicionado ao consentimento está logo ali, de pronto visualizável, ao alcance da compreensão do usuário e imediatamente valorizado.

A segunda teoria que aparece com destaque nesta discussão é a Teoria Prospectiva que, segundo Bioni (2020, p. 140), "assinala que o processo de tomada de decisão tende a se levar pelo contexto de que as perdas são maiores do que os ganhos". Segundo o citado autor (2020, p. 140-141), "o usuário que teve acesso a um produto ou serviço sopesará mais essa perda do que o ganho em retomar, em tese, o controle de seus dados pessoais."

Nesta balança, o potencial dano ao indivíduo que, para além de não visualizável, sequer é compreendido a contento, acaba tendo um peso menor. O ato de consentir, trajado como manifestação da liberdade individual, da autodeterminação informacional, acabaria por ser, na realidade, uma injusta e disfuncional atribuição ao usuário, que ocupa uma posição de extrema vulnerabilidade.

Concluindo em linhas parecidas, Bioni (2020, p. 141) assevera:

> A própria lógica do trade-off da economia dos dados pessoais é traiçoeira, portanto, frente a tal arquitetura de escolha de decisões, notadamente por essa idiossincrasia entre gratificações imediatas e prejuízos mediatos/distantes. A crença de que o cidadão é um sujeito racional e capaz de desempenhar um processo genuíno de tomada de decisão para controlar seus dados pessoais é posta em xeque por toda essa complexidade envolta ao fluxo das informações pessoais. Ele está em uma situação de vulnerabilidade específica em meio a uma relação assimétrica que salta aos olhos, havendo uma série de evidências empíricas a esse respeito.

As evidências empíricas mencionadas partem, por exemplo, da pesquisa *Mental Models* (*Universidades de Stanford e Carnegie Mellon*), coordenada pelas pesquisadoras Lorrie Cranor e Aleecia McDonald . A referida pesquisa foi pensada para investigar o comportamento dos indivíduos no contexto da publicidade comportamental no ambiente virtual, buscando mensurar

a “compreensão dos titulares dos dados pessoais quanto ao fluxo de suas informações pessoais”. (BIONI, 2020, p. 141-142).

O estudo trouxe o dado de que “apenas 23% dos usuários usam o modo de navegação privada – aquele que bloqueia a coleta dos dados pessoais –, enquanto 50% dos usuários não usam tal ferramenta e 27% não têm certeza”. Ademais, “somente 17% deletam cookies, 23% não têm certeza, e, por fim, 60% não deletam essa ferramenta de coleta de dados pessoais”. A referida pesquisa ainda aponta que “apenas 30% esclareceram que a ‘limpeza’ de seus cookies estaria relacionada às questões de segurança e privacidade” (BIONI, 2020, p. 142).

Com esse apontamento de dados, já se desnuda a limitação da compreensão do indivíduo a respeito do tratamento de dados. Entretanto, tal limitação é fruto da ignorância relativa aos riscos de consentir e às técnicas de segurança que estão à disposição do usuário na internet. Neste sentido, a citada pesquisa trouxe que “70% dos entrevistados afirmam que, ao efetuar compras on-line, levariam em consideração se o website compartilharia os seus dados pessoais com parceiros, cujas atividades estariam relacionadas à atividade publicitária.” (BIONI, 2020, p. 143.

Em mesmo sentido, 64% dos entrevistados consideraram como “invasiva a vigilância sobre as suas atividades on-line”. (BIONI, 2020, p. 143).

A parte final da pesquisa concentrou-se em dois grupos, questionados da seguinte forma: “i) se pagariam o valor de U$ 1,00 (um dólar) para evitar que os provedores de Internet coletassem suas informações pessoais”, ou “ii) se aceitariam o desconto de U$ 1,00 (um dólar) em troca da permissão para que os provedores de Internet coletassem seus dados pessoais”. No grupo inicial “11% afirmam estar dispostos a pagar o valor de U$ 1,00 (um dólar). Ao passo que, no segundo grupo, 69% concordariam com o desconto ofertado em troca de suas informações pessoais” (BIONI, 2020, p. 143-144).

Esta parte da pesquisa revela a demonstração prática das Teorias da Decisão da Utilidade Subjetiva e Prospectiva. Vê-se que quando se colocou a tutela das informações em plano imediato, 89% (oitenta e nove por cento) dos entrevistados não dimensionaram sua importância e se recusaram a pagar a quantia de um dólar. Em contraposto, quando esta mesma quantia foi oferecida, em troca das informações pessoais, como desconto na aquisição de um bem ou serviço (em primeiro plano), apenas 31% (trinta e um por cento) dos entrevistados se negaram a efetuar a referida troca. Verifica-se não estar claro para os usuários, portanto, a importância dos seus dados e sua valoração imediata no processo de produção.

No entanto, de forma positiva, “houve o consenso de 69% dos entrevistados de que a privacidade é um direito, de modo que eles não deveriam ser obrigados a pagar uma quantia

monetária para evitar que as empresas a violassem", sendo que "61% dos entrevistados afirmaram, categoricamente, que tal tipo de pagamento consistiria em uma extorsão". (BIONI, 2020, p. 144).

O que se verifica da referida pesquisa e da análise traçada até aqui é a insuficiência do consentimento enquanto eixo gravitacional das políticas de proteção da informação, tendo em vista a ausência de conhecimento dos usuários (em regra) sobre o processo de captação e tratamento de dados pessoais. Em que pese indispensável, o consentimento, se desprovido de outros mecanismos protetivos supressores da carência informacional dos usuários, releva-se, tão somente, um grande fardo para estes. Tais mecanismos, por sua vez, devem refletir a respeito da posição de vulnerabilidade ocupada pelo titular dos dados pessoais, sob pena de se revelarem, de igual sorte, esvaziados de sentido.

Resta saber se as normativas de proteção de dados brasileiras trazem em seu bojo a anotação desta reflexão.

4.3 Legislações esparsas

Neste sentido, necessária a análise do caminho percorrido pelo consentimento enquanto instituto jurídico no corpo das legislações que versam sobre a proteção de dados pessoais.

4.3.1 Código de Defesa do Consumidor

De início, para análise do tema à luz da legislação infraconstitucional, o marco de partida não poderia ser outro que não o Código de Defesa do Consumidor (lei n. º 8.078/90 - CDC), que prevê, em seu artigo 43, a proteção e tutela de dados pessoais:

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

O CDC representou, com este dispositivo, a preocupação do legislador em tutelar o consumidor perante a utilização abusiva de suas informações em registros e bancos de dados (DONEDA, 2019).

Vê-se ainda do referido dispositivo legal que há menção expressa ao direito de acesso às informações registradas a respeito do consumidor, bem como às suas fontes. Na mesma linha, o parágrafo terceiro do artigo citado ainda aponta que o consumidor, uma vez encontrado

equívoco a respeito das informações, “poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.”

Ao analisar as normas do CDC aplicáveis à tutela dos dados pessoais, Doneda (2019, p. 265) comenta:

> As disposições do CDC revelam, como foco de preocupação do legislador, o estabelecimento de equilíbrio na relação de consumo por meio da interposição de limites ao uso da informação sobre o consumidor pelo fornecedor (que estaria justificado, de certo ponto de vista, na efetivação da transação com maior segurança). Assim, por exemplo, o registro de dados negativos sobre um consumidor não poderá ser mantido por um período maior de 5 anos; é prevista a necessidade de comunicação escrita sobre o tratamento da informação ao consumidor em certos casos, assim como o direito de acesso, correção e, implicitamente, o cancelamento justificado.

De fato, a conclusão do autor é acertada no que se refere à interposição de limites ao uso da informação sobre o consumidor pelo fornecedor. No entanto, observa-se que este controle de qualidade das informações, que seria o instrumento de limitação, é expressamente outorgado ao consumidor (§3.º, art. 43 do CDC). Trocando em miúdos, o controle se daria de forma repressiva, *a posteriori*, quando assim fosse requerido pelo consumidor.

Nesta esteira, o CDC, como marco inaugural da legislação infraconstitucional protetiva de dados pessoais no Brasil, alavanca a figura do consumidor (titular de dados pessoais) ao centro do eixo normativo enquanto sujeito capaz de se autodeterminar e de, consequentemente, promover sua autotutela. Nesse contexto, não há uma preocupação em relação à natureza das informações, mas somente em relação ao sujeito titular das mesmas.

Neste sentido, Bruno Bioni (2020, p. 122) pontua:

> Tais direitos (acesso, retificação e cancelamento) e princípios (transparência, qualidade [exatidão] e limitação temporal) gravitam em torno da figura do consumidor, para que ele, na condição de titular dos dados pessoais, exerça controle sobre suas informações pessoais. Em suma, o Código de Defesa de Consumidor buscou conferir a autodeterminação informacional, o que perpassa desde regras para garantir a exatidão dos dados até limitações temporais para o seu armazenamento.

Desta maneira, pode-se concluir que o diploma consumerista brasileiro, enquanto norma primária na regulamentação dos dados pessoais, não refletiu a respeito da capacidade (ou não) do consumidor em se autodeterminar.

O marco normativo consumerista tem como presumida a capacidade do indivíduo promover sua própria tutela, estendendo em relação a esta, tão somente, a preocupação no que se refere à clareza das informações, que figura numa superfície muita rasa ao problema da tutela de dados. Neste sentido, ainda que claras e objetivas as informações disponibilizadas ao consumidor (conforme reza o CDC), existem algumas situações em que sequer poderiam ser utilizadas as informações pessoais (dados sensíveis, por exemplo), de modo que o dever de informação, por si só, mostra-se insuficiente à uma tutela efetiva nestas hipóteses.

Portanto, observa-se que a Lei n.º 8078/90, para além de limitação quanto à sua extensão (conflito entre fornecedor e consumidor), fixa como base para seu eixo de proteção normativo a autodeterminação, figurando o consumidor, neste sentido, como um sujeito ativo no processo de proteção.

4.3.2. Lei do Cadastro Positivo – lei n.º 12.414/2011

Segundo Bioni (2020, p. 122), "a Lei 12.414/2011 veio a disciplinar a formação de banco de dados sob um conjunto de dados relativos às operações financeiras e de adimplemento para fins de concessão de crédito". Ainda segundo o referido autor (2020, p. 154), em razão da lei, "a situação econômica do postulante ao crédito não é mais, somente, analisada a partir de dados relativos a dívidas não pagas, mas, também, a partir de outras informações que possam exprimir dados positivos sobre a sua capacidade financeira e o seu histórico de adimplemento".

A lei n.º 12.414/2011, conhecida como lei do cadastro positivo, diferentemente da legislação consumerista, trouxe vedação específica ao tratamento de informações sensíveis e de forma excessiva. Ademais, praticamente reproduziu o art. 43 do CDC, mas foi além para trazer conceitos do que seria informação clara, objetiva, verdadeira e de fácil compreensão. Vejamos o que dispõe o seu art. 3.º:

> Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
>
> § 1º Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado.
> § 2º Para os fins do disposto no § 1º , consideram-se informações:
> I - objetivas: aquelas descritivas dos fatos e que não envolvam juízo de valor;
> II - claras: aquelas que possibilitem o imediato entendimento do cadastrado independentemente de remissão a anexos, fórmulas, siglas, símbolos, termos técnicos ou nomenclatura específica;

> III - verdadeiras: aquelas exatas, completas e sujeitas à comprovação nos termos desta Lei; e
> IV - de fácil compreensão: aquelas em sentido comum que assegurem ao cadastrado o pleno conhecimento do conteúdo, do sentido e do alcance dos dados sobre ele anotados.
> § 3º Ficam proibidas as anotações de:
> I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
> II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

A referida legislação andou bem ao proibir, no parágrafo terceiro, a anotação de informações excessivas e sensíveis, posto que se retirou do titular de dados, neste ponto, o pesado encargo de se autotutelar. Diferentemente da legislação consumerista, a lei do cadastro positivo refletiu a respeito da necessidade de tutela da informação em si considerada, dada a sua natureza.

Verifica-se ainda a vinculação do tratamento de dados ao princípio da finalidade, posto que, por força do referido diploma normativo, as informações colhidas não podem ser utilizadas para outros fins que não os creditícios (BIONI, 2020).

Neste sentido, em que pese modesta, a alteração promovida pela técnica legislativa usada na Lei do Cadastro Positivo pode ser encarada como um primeiro sinal de mudança do eixo normativo da proteção de dados, que tende a deixar de ser, exclusivamente, fundado no consentimento.

4.4. O Marco Civil da Internet

O Marco Civil Da Internet - MCI, lei n.º 12.965/14, surgiu como resultado de um fervoroso debate social a respeito da insuficiência da legislação brasileira para regulamentar o comportamento dos indivíduos na internet. Nesse contexto, a lei chegou para implementar, conforme aponta Santos e Petry (2019, p. 332), "princípios, garantias, direitos e deveres para o uso da internet no Brasil".

Neste contexto, a referida legislação preocupou-se com mais atenção à liberdade de expressão, a proteção da privacidade e dos dados pessoais e a responsabilização dos indivíduos pelo seu comportamento no ambiente virtual. Neste sentido, Pereira (2016, p. 3-4), *apud* Santos e Petry, define que são cinco as bases da Lei protetiva da internet:

> Primeiro, a liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> Segundo, a proteção da privacidade e dos dados pessoais;
> Terceiro, a neutralidade da rede juntamente com a sua estabilidade, segurança e bom funcionamento segundo as boas práticas tecnológicas;
> Quarto; a responsabilidade dos agentes pelos seus comportamentos na rede sem prejuízo da preservação da natureza participativa da rede;
> Quinto, a liberdade dos modelos de negócios promovidos na internet, ou seja, a liberdade de acesso ao mercado digital.

Interessante apontar que durante o processo de criação da referida norma, já antes das primeiras deliberações a seu respeito, existia no país uma preocupação muito latente em relação à responsabilização dos indivíduos por seus atos por meio das redes. No dito popular, tornou-se comum a expressão de que a internet seria uma "terra sem lei".

Este espírito, inclusive, aproximou a discussão a respeito da legislação para o campo do direito penal, que acarretaria uma proposta mais dura e punitiva das normas do projeto do marco legal da internet. No entanto, a ideia que prevaleceu na discussão a respeito da natureza das normas se afastou da tendência punitiva própria do direito criminal.

Nos dizeres de Bruno Bioni (2020, p. 124):

> [...] o MCI procurou, de forma principiológica, assegurar os direitos e garantias do cidadão no ambiente eletrônico, sendo o seu traço marcante a distância de uma técnica normativa prescritiva e restritiva das liberdades individuais, própria do âmbito criminal, que poderia ter efeitos inibitórios para a inovação e a dinamicidade da Internet.

No entanto, a escolha de uma técnica legislativa distante do campo penal não significou, na prática, a ausência de normas de responsabilização mais robustas. Isto porque durante o transcorrer do procedimento de elaboração da norma veio à tona o episódio conhecido como *Snowden Case*[14] que alterou, em certa medida, o trajeto do projeto de lei. Além da alteração material para endurecer as normas de proteção, o próprio processo de aprovação da lei foi acelerado, conforme aponta Bioni (2020, p. 125):

> [...] a sua proeminência (a do MCI) consolidou-se com o episódio do escândalo de espionagem revelado pelo ex-analista Edward Snowden, da Agência Nacional de Segurança dos Estados Unidos. Tais revelações

[14] Edward Snowden foi responsável pela revelação do programa de coleta de dados executado pela Agência de Segurança Nacional norte-americana, fato que provocou o debate acerca das novas formas de violação ao direito fundamental à privacidade, que demonstra a necessidade de adequação do Direito às novidades aportadas pelas constantes inovações tecnológicas. Disponível em: https://www.scielo.br/j/seq/a/BKdjxJFTbXNPwJnnP4hk8kF/abstract/?lang=pt. Acesso em 22 dez. 2021

> repercutiram no MCI, que teve mudanças substanciais em seu texto para "endurecer" a proteção ao direito à privacidade e aos dados pessoais, bem como na própria aceleração de seu trâmite legislativo que, com a adoção do regimento de urgência, culminou em sua aprovação no Congresso brasileiro em 2014.

Interessante fazer um parêntese a respeito do *Snowden Case*, posto que sua relevância ultrapassa a análise do MCI para reverberar na própria discussão sobre violação e proteção de dados pessoais na internet.

Os fatos que foram revelados pelo analista de sistemas Edward Snowden tiveram repercussão tamanha que foram retratados pelo documentário cinematográfico *Citizenfour*[15], dirigido por Laura Poitras e premiado, em 2015, com o Óscar na categoria de melhor documentário.

A história começa em 2013, quando Snowden, do Havaí, trabalhava na *Bozz Allen Hamilton,* empresa ligada à Agência de Segurança nacional dos Estados Unidos do América - *National Security Agency* - NSA. Durante este período no Havaí, o analista de sistemas baixou vários arquivos secretos relacionados ao sistema de inteligência norte-americano, pediu férias para seus supervisores e viajou para Hong Kong, conforme narra José Isaac Pilati e Mikhail Vieira Cancelier de Olivo (2014, p. 284):

> Durante o período no Havaí, fez o download de documentos secretos relacionados a atividades de inteligência dos Estados Unidos e de parceiros internacionais. Realizada a compilação, solicitou ao seu supervisor algumas semanas de férias e seguiu para Hong Kong, onde encontraria o jornalista Greenwald e a Cineasta Laura Poitras, responsáveis pela elaboração das entrevistas e imagens posteriormente divulgadas no The Guardian e no The Washington Post, primeiros jornais a apresentar a denúncia.

Pilati e Olivo (2014, p. 284-285) ainda comentam:

> Na entrevista, Edward Snowden apresentou provas de que a NSA monitora milhões de telefones e dados de usuários online, nos Estados Unidos e em países estrangeiros; a Agência teria acesso aos servidores de empresas como Google, Facebook, Skype e Apple,o monitoramento faria parte de programa de espionagem chamado *Prism14*, que permite aos agentes coletar diversos tipos de materiais como histórico de internet, conteúdo de e-mails e chats e transferências de arquivos.

[15] Citizenfour, da diretora Laura Poitras, exibe uma espécie de reportagem em modo participativo, na qual é essencial a participação do criador do documentário na filmagem do protagonista e na organização das informações. A estratégia visa dar ritmo à narrativa e possibilitar a compreensão da nova era da internet e da falta, ou luta, pelo direito à intimidade, que a sociedade fluídica enfrenta e que, guardadas as devidas proporções, tornou-se parte da decadência de Amy. BAPTISTA, Ana Maria Haddad; BATISTA, José Carlos Freitas; D'AMBROSIO, Ubiratan (Orgs.). Educação e Linguagens – p. 31. São Paulo: BT Acadêmica, 2017

> Snowden acusou a NSA de estar construindo uma infraestrutura tecnológica que permite a interceptação de praticamente qualquer tipo de informação. Com esse aparato, seria possível rastrear a comunicação de qualquer pessoa automaticamente, sem nenhuma forma de controle prévio. Com base nos documentos apresentados, por exemplo, verificou-se que o Brasil teve 2.3 bilhões de telefonemas e mensagens de e-mail espionados. Para a além da comunidade em geral, autoridades políticas, como a Presidente Dilma Rousseff e a Chanceler alemã Angela Merkel também tiveram suas comunicações (via telefone e internet) violadas, gerando a exigência de ainda mais explicações.

O caso Snowden expõe problemas de arestas muito maiores do que os examinados neste trabalho, principalmente por trazer à tona não apenas a violação individual sofrida por cada indivíduo espionado, mas questões que envolvem possível violação de soberania nacional, próprias do âmbito das relações internacionais.

Não obstante, é possível mensurar, através do caso, a importância política dos dados pessoais e da informação, que parece figurar também como eixo fundamental das relações de poder.

O caso Snowden repercutiu diretamente no projeto de lei do MCI. De forma exemplificativa, Bioni (2020, p. 125) aponta que "o art. 7º detinha, apenas, cinco incisos, passando a ter, no cenário 'pós Snowden', oito incisos, sendo que todos eles foram direcionados para a proteção dos dados pessoais".

Bioni (2020, p. 126), examinando esta mudança de cenário ocorrida, aponta que os dispositivos adicionados "fazem menção expressa à necessidade do consentimento do usuário para a coleta, o uso, o armazenamento e o tratamento de seus dados pessoais, tal como para a sua transferência a terceiros".

Atualmente, o referido art. 7.º contém treze incisos[16], estando dos incisos V ao X a menção mais incisiva ao consentimento do usuário enquanto ponto crucial da estrutura normativa de proteção.

---

[16] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
V - manutenção da qualidade contratada da conexão à internet;
VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

Observa-se que o MCI eleva o consentimento a um patamar de importância maior que o exposto na Lei do Cadastro Positivo e no CDC, ao ressalvar, por exemplo, que o direito ao não fornecimento de dados pessoais a terceiros poderá ser declinado mediante o consentimento livre, expresso e informado do usuário (art. 7.º, inciso VII).

Aliado à elevação de patamar veio a qualificação ou adjetivação do consentimento, que impõe requisitos mais robustos à manifestação de vontade para esta ser livre, expressa e informada.

Além disso, o consentimento ainda aparece com grande ênfase no inciso X, em que está previsto o direito de o titular de dados pessoais requerer a exclusão definitiva das informações que vier fornecer a terceiros.

Mais uma vez contata-se que a autodeterminação informacional é colocada, sem questionamentos, no centro gravitacional da estratégia normativa de proteção. Não há, neste contexto, ressalva a respeito da informação em si considerada, sendo irrelevante sua natureza, outorgando-se ao usuário a função de, através do consentimento, promover sua autotutela.

4.5 A Lei n. º 13.709/2018 e a figura jurídica do consentimento

A Lei Geral de Proteção de Dados remete a uma nova disposição normativa em relação ao consentimento. Este passa a ocupar não uma posição de centralidade, mas de paridade em relação a outras hipóteses legais em que se admite o tratamento de dados, todas previstas nos incisos do art. 7. º[17] da referida lei.

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; (Redação dada pela Lei nº 13.709, de 2018) (Vigência)
XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

[17] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

Refletindo sobre esse rearranjo técnico-normativo, Bioni (2020, p. 127) conclui que:

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

Neste sentido, é possível concluir que houve uma mudança considerável em relação aos diplomas normativos anteriores, tendo em vista que as disposições do novo marco legal não estabelecem uma relação indissociável entre proteção de dados e consentimento. Portanto, é possível haver proteção mesmo que dispensado o consentimento. Contudo, a manifestação de vontade ainda aparece como a ponta da lança da estratégia normativa de proteção.

Na mesma linha do MCI, a LGPD também adjetiva o consentimento, que deverá ser "livre, informado, inequívoco e dizer respeito a uma finalidade determinada de forma geral e, em alguns casos, deve ser, ainda, específico" (BIONI, 2021, p. 127). Para além dos adjetivos ao consentimento, boa parte dos princípios estampados no art. 6.º[18] revelam que o indivíduo e

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

[18] 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;

sua manifestação de vontade ainda ocupam o centro da estratégia normativa de proteção de dados.

No entanto, alguns de seus princípios elencados pela norma apontam para a preocupação com a informação em si considerada, a exemplo dos princípios da adequação, finalidade, qualidade dos dados, transparência e segurança.

Nesse contexto, cita-se o princípio da finalidade. Por este, o tratamento de dados precisa estar adstrito a propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Esta limitação está expressamente prevista no inciso I do art. 6.º da Lei 13.709/2018, sendo um evidente exemplo de avanço no que se refere à facilitação do consentimento fornecido, servindo a este como um mecanismo de melhora.

Por força do referido princípio, ao titular de dados não pode ser direcionado um pedido de consentimento genérico ou indeterminado.

Entretanto, em que pese tal mudança, o consentimento ainda é o vetor principal da proteção oferecida pela LGPD, que cita o termo mais de trinta vezes em seu texto legal. Neste contexto, Bioni (2020, p. 128) ainda aponta que:

> (...) há uma série de disposições que dão um regramento específico para concretizar, orientar e, em última análise, reforçar o controle dos dados pessoais por meio do consentimento. Por exemplo: a) consentimento deveria ser extraído por meio de "cláusulas contratuais destacadas"; b) autorizações genéricas (sem uma finalidade determinada) seriam nulas; e, principalmente, c) nas hipóteses em que não há consentimento se deveriam observar os direitos e princípios da LGPD, de modo que haja a possibilidade de o titular dos dados pessoais se opor ao tratamento de seus dados.

Neste sentido, é possível concluir que o consentimento, em que pese não ser a única fonte de proteção normativa dos dados pessoais, ainda é o elemento mais importante da estratégia legislativa trazida pela LGPD. No entanto, o novo marco regulatório se distancia dos

---

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.

demais ao promover princípios que apontam para um aperfeiçoamento da manifestação de vontade do titular de dados pessoais e da autodeterminação informacional.

4.6 A releitura do consentimento e do fomento às tecnologias de melhoramento da privacidade

Feito este apanhado do trajeto do consentimento ao longo das espécies normativas citadas, observa-se que é traço marcante em toda a produção legislativa analisada a referência à autodeterminação, ao empoderamento do titular de dados pessoais enquanto sujeito ativo do processo de proteção.

O consentimento, no entanto, é reduzido a uma concepção por demais contratualista, que se contenta com a manifestação de vontade e não reflete a respeito da complexidade do mercado da informação, da sociedade informatizada. O grande instrumento materializador da referida problemática é o Termo de Uso e Política de Privacidade, que impõe ao usuário instrumentos contratuais enormes e de difícil compreensão, incompatíveis com o ambiente célere da internet.

Discorrendo a respeito dos termos de política de privacidade, Bioni (2020, p. 165-166) aponta para a sua inexpressividade prática, citando, inclusive, um estudo das pesquisadoras da *Carnegie Mellon University*:

> E, nesse sentido, tal ferramenta contratual está longe de ocasionar o empoderamento. Na verdade, os seus textos longos e de difícil compreensão são incapazes de sequer estabelecer uma comunicação adequada para que o titular dos dados pessoais possa racionalizar um processo de tomada de decisão.
>
> É famoso, por exemplo, um estudo das pesquisadoras da Carnegie Mellon University que avaliaram que os usuários despenderiam, ao menos, 201 horas por ano – o equivalente a U$ 3,354169 – para que procedessem à leitura de todos os termos de uso dos websites que são em média acessados por um usuário americano.

Citando ainda o estudo empírico do *Global Privacy Enforcement Network/GPEN*, Bioni (2020, p. 164) aponta para a ineficiência do mecanismo pelo qual se recolhe o consentimento:

> Veja-se, a título de ilustração, o estudo empírico da Global Privacy Enforcement Network/GPEN que, por meio das suas 26 autoridades de garantia de proteção de dados pessoais, constatou que, das políticas de

> privacidade de aplicativos móveis/mobile apps analisadas: i) 85% falham em prestar uma informação adequada sobre a coleta, o uso e o compartilhamento dos dados pessoais; ii) 59% são de difícil compreensão para extração de informações básicas a respeito de privacidade; iii) 1/3 está coletando dados pessoais excessivos e; iv) 43% têm uma interface inadequada, seja porque a tela ou as letras são muito pequenas, seja porque se trata de longos textos que demandam a leitura de inúmeras páginas.

O que se retira é que o consentimento, enquanto encarado como mera manifestação de vontade, assumirá no contexto da proteção de dados pessoais mera função ficcional, tendo em vista as limitações que se apresentam ao titular no processo de tomada de decisão. Conforme visto, a necessidade de integração virtual já se mostra como um grande questionamento à efetividade do consentimento, aliado à ausência de mecanismos que, de fato, empoderem o titular dos dados.

Neste compasso, o consentimento passa a ser condição para acesso a determinados bens ou serviços, não expressando liberdade, mas sim via necessária à vida em sociedade, o que, em última análise, só ratifica o contexto de desproteção que emerge do modelo social informatizado.

A este respeito, discorre Bioni (2020, p. 159):

> É desse descompasso que emerge um debate normativo da proteção de dados pessoais. O consentimento tem sido visto como o pilar dessa estratégia regulatória, mais como um meio para legitimar os modelos de negócios da economia digital, do que como um meio eficiente para desempenhar a proteção dos dados pessoais. Ele tem sido encarado como uma verdadeira ficção legal deformadora e voraz do teorizado regime legal de proteção de dados pessoais e da sua aplicação na prática. Não seria mais do que uma mistificação, na medida em que não é confrontado com o anotado contexto socioeconômico que estrangula a prometida liberdade da autodeterminação informacional.

Desta maneira, há inegável incongruência entre o consentimento (de per si considerado) e a proteção de dados pessoais, na medida em que a visão contratualista da manifestação de vontade ignora a complexidade das relações virtuais. Neste contexto, a mera adjetivação do consentimento, estratégia normativa das normas protetivas do negócio jurídico, pensadas ao longo do século XX, não se mostra suficiente à problemática que se apresenta.

É preciso que se formule uma releitura a respeito do consentimento enquanto instituto jurídico no contexto da proteção de dados pessoais, posto que seu alcance esbarra em limitações diversas. Esta reflexão poderá embasar uma nova estratégia de regulamentação que propicie ao titular de dados pessoais, de fato, a capacidade de autodeterminação informativa prevista no art. 2.º da LGPD. (BIONI, 2020).

Nesse contexto, a utilização dos velhos dogmas contratuais da autonomia da vontade em relação à proteção de dados, sem uma adaptação que reflita a respeito da personalidade do indivíduo e do dano que este pode sofrer ao consentir tornaria inócuo o instituto do consentimento.

Assim, reputa-se como necessário o estabelecimento de ferramentas que auxiliem o titular de dados pessoais no ato de consentir com o uso de suas informações por terceiros. Para tanto, são necessários mecanismos facilitadores que, para além de se apresentarem através de uma linguagem acessível, promovam, efetivamente, o empoderamento do usuário no processo de proteção de dados.

Estes mecanismos, para tanto, devem ser pensados e estruturados dentro da própria tecnologia da informação. Em que pese a tecnologia em rede ser a fonte da vulnerabilidade do titular de dados pessoais, é através dela que se podem se edificar os mais eficientes métodos de proteção e capacitação do titular de dados pessoais.

Em realidade, estas ferramentas já existem e recebem o nome de Tecnologias de Melhoramento da Privacidade (*Privacy Enhancing Technologies*/*PETs*). Segundo Bioni (2020, p. 167), "a tradução literal – PETs como tecnologias que reforçam-melhoram a privacidade – denota abrangência do termo que, como um guarda-chuva, é capaz de abarcar toda e qualquer tecnologia que seja amigável e facilitadora à privacidade."

Estas ferramentas se dirigem ao titular de dados através de uma linguagem mais simples e enxuta, minimizando o uso de dados pessoais e potencializando a segurança e capacitação do usuário, sem privar o usuário do acesso ao site ou aplicativo buscado.

São exemplos de PETs a criptografia das comunicações e os mecanismos de navegação anônima. Através de mecanismos como tais o usuário transita na rede sem deixar rastros, tornando intacto todo seu histórico de navegação. Destaca-se ainda a tecnologia *Do Not Track*/DNT, que, em suma, consiste numa PET projetada para "executar as escolhas dos titulares dos dados pessoais no plano da coleta." (BIONI, 2020, p. 170).

Segundo o referido autor (BIONI, 2020, p. 170):

> Ao contrário de fechar, rejeitar e/ou aceitar inúmeros pop-ups de cookies, ou, ainda, travar uma saga constante para deletar inúmeros trackers, bastaria ao consumidor acionar o botão "DNT" para que, automaticamente, fosse exteriorizada a sua escolha em barrar ou não a coleta de seus dados. Essa funcionalidade seria ativada pelo próprio navegador do usuário que sinalizaria tal opção do usuário a todas as aplicações por ele acessadas. O browser seria, assim, a forma pela qual o consentimento do titular dos dados pessoais seria externalizado e, em última análise, o veículo da autodeterminação informacional.

Tais ferramentas de facilitação, por serem pensadas e estruturadas através dos próprios mecanismos da tecnologia da informação, oferecem um caminho para a renovação da estratégia normativa da proteção de dados pessoais, consistente no aparelhamento da autonomia da vontade (consentimento) e no consequente desenvolvimento da autodeterminação informacional, que não deve ser lida sob a ótica reducionista contratual.

Neste sentido, a regulamentação de tais mecanismos se faz necessária, posto que o consentimento isolado do titular de dados pessoais já se mostrou insuficiente enquanto estratégia normativa de proteção. Com o investimento nos recursos tecnológicos de proteção, o processo de tomada de decisão por parte do usuário da internet se tornará mais simplificado, ao passo em que, por consequência, a proteção de dados será mais efetiva.

CONCLUSÕES

No contexto da sociedade da informação, os mercados, as disputas políticas e as relações sociais são diretamente afetadas pela informação obtida através da captação de dados na internet. Os dados pessoais, neste contexto, ostentam valor social, político e, sobretudo, de mercado.

A legislação existente sobre o tema, por sua vez, tem se mostrado insuficiente à efetiva proteção de dados pessoais, uma vez que não reflete, a contento, sobre a situação de vulnerabilidade do usuário. Concorre para isto a interpretação pela qual a tutela jurídica dos dados estaria limitada ao direito à privacidade. Nesse contexto, numa primeira face, o enquadramento do direito à proteção de dados enquanto um direito da personalidade e fundamental autônomo resolve as limitações hermenêuticas impostas pela equivocada redução da matéria ao âmbito da privacidade.

Não obstante, o instituto jurídico do consentimento conforme aplicado e interpretado hoje assume mera função fictícia, mostrando-se como uma estratégia normativa de proteção ineficiente e incompatível com a complexidade da sociedade da informação, sobretudo por ser analisado sob uma ótica contratual ultrapassada.

Destarte, o que se propõe uma releitura do consentimento enquanto mecanismo central de proteção de dados pessoais que não o limite às noções contratuais clássicas e o aproxime do campo dos direitos da personalidade. De modo idêntico, a autonomia informacional não deve ser limitada à autonomia privada materializada na decisão binária de consentir ou não consentir, que ignora as dificuldades inerentes ao processo de escolha.

Neste contexto, é preciso que se possibilite ao titular de dados pessoais as condições para que o seu consentimento não seja estéril. Tais condições precisam ser projetadas dentro da própria tecnologia da informação e apresentadas ao cidadão através de uma linguagem simples e enxuta, distante do padrão atual dos termos de uso e consentimento e política de privacidade, enfadonhos e ineficientes.

Por isto, propõe-se o fomento, divulgação, investimento e a regulamentação das *Privacy Enhancing Technologies – PETs,* mecanismos que, se devidamente estruturados e outorgados de força normativa, poderão aparelhar o consentimento fornecido pelo titular de dados pessoais para que se chegue mais próximo do efetivo empoderamento deste no processo de proteção de dados e do ideal de autodeterminação informativa.

REFERÊNCIAS

ALVES, Alinne Cardim; BORCAT, Juliana Cristina. **Os Direitos da Personalidade como Direitos Fundamentais e Manifestação da Dignidade**. Disponível em: https://www.univem.edu.br/file/artigo01.pdf. Acesso em 12 dez. 2021.

ALVES, Germano Fabrício. **Análise da Possibilidade de Regulação da Publicidade Comportamental (Behavioral Advertising) pelo Microssistema Consumerista**. Disponível em: https://www.indexlaw.org/index.php/revistadgrc/article/view/696/689. Acesso em: 11 de dez. 2021.

ARAUJO, Luiz Ernani Bonesso de; CAVALHEIRO, Larissa Nunes. **A proteção de dados pessoais na sociedade informacional brasileira:. o direito fundamental a privacidade entre a autorregulação das empresas e a regulação protetiva do internauta.** Revista do direito público, londrina, v.9, n.1, p.209-226, jan./abr.2014.

BIONI, Bruno Ricardo**. Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020;

BITTAR, Eduardo C. B. **A Teoria do Direito, a Era Digital e o Pós-Humano: o novo estatuto do corpo sob um regime tecnológico e a emergência do Sujeito Pós-Humano de Direito.** Rev. Direito Práx., Rio de Janeiro, Vol. 10, N. 02, 2019, p. 933-961.

BLUM, Renato Opice; MALDONADO, Viviane Nóbrega. **LGPD: Lei Geral de Proteção de Dados comentada** [livro eletrônico]. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020;

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 02 de dez. 2021.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. **Código de Defesa do Consumidor.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 07 de abr. 2021.

BRASIL. **Lei nº 10406, de 10 de janeiro de 2002. Código Civil.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 09 de abr. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 09 de abr. 2021.

BRASIL. **Lei nº 13.106, de 16 de março de 2015. Código de Processo Civil**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em 08 de abr. 2021.

BRASIL**. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 09 de abr. 2021.

BRASIL. **Lei nº 12.414, de 09 de junho de 2011. Lei do Cadastro Positivo.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em 09 de abr. 2021.

CASTELLS, Manuel. **A sociedade em rede.** 22 ed. São Paulo: Paz e Terra. 2020.

CORRÊA, Adriana Espíndola; GEDIEL, José Antônio Peres. **Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado.** Revista da Faculdade de Direito - UFPR, Curitiba, n.47, p.141-153, 2008.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados.** 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

E-COMMERCE SOBE 41% em 2020 e atinge R$ 87,4 milhões; alta é a maior em 13 anos. Disponível em: https://revistapegn.globo.com/Banco-de-ideias/E-commerce/noticia/2021/03/pegn-e-commerce-sobe-41-em-2020-e-atinge-r-874-milhoes-alta-e-a-maior-em-13-anos.html. Acesso em 11 de dez. 2021.

GHISI, Silvano; PEZZELLA, Maria Cristina Cereser. **O direito fundamental à intimidade como limite à manipulação de dados pessoais na sociedade da informação.** Disponível em: http://www.publicadireito.com.br/artigos/?cod=eba7fcab4a6903ad. Acesso em: 12 dez. 2021.

LEONARDI, Marcel**. Tutela e privacidade na internet.** 1 ed. São Paulo: Saraiva, 2011.

LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados: Lei N. 13.709/2018, com alteração da lei N. 13.853/2019.** 1 ed. São Paulo: Almedina, 2020.

OLIVO, Mikhail Vieira Cancelier de; PILATI, José Isaac. **Um Novo Olhar sobre o Direito à Privacidade: caso Snowden e pós-modernidade jurídica.** Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2014v35n69p281). Acesso em 12 dez. 2021.

PETRY, Alexandre Torres; SANTOS, Lucas da Silva**. Direito à Privacidade e Proteção aos Dados Pessoais Frente à Lei Nº 12.965/14 (denominado marco civil da internet).** Disponível em: https://www.metodista.br/revistas/revistasipa/index.php/direito/article/view/772/719. Acesso em 12 de dez. 2021.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD).** São Paulo : Saraiva Educação, 2018.

MIRANDA, N. A; SILVA, D.; SIMON, F; VERASZTO, E. V. O. **Tecnologia: buscando uma definição para o conceito.** Prisma.com (Portugual), n. 8, p. 19-46, 2009. Disponível em: http://hdl.handle.net/20.500.11959/brapci/66904. Acesso em: 11 de dez. 2021.

QUESTÕES TECNOLÓGICAS, Éticas E Normativas Da Proteção De Dados Pessoais Na Área Da Saúde Em Um Contexto De Big Data. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/811. Acesso em: 11 de out. 2021.

REDECKER, Ana Cláudia [et al.]. **Proteção de Dados[recurso eletrônico]:** temas controvertidos. Indaiatuba, SP :Editora Foco, 2021.

TEFFÉ, Chiara Spadaccini de. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510/384. Acesso em: 12 de out. 2021.