UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

LAURO DE ARAÚJO COSTA MOURA

SOB "TERMOS E CONDIÇÕES": PRIVACIDADE, CONSENTIMENTO E AUTODETERMINAÇÃO INFORMATIVA NA ERA DIGITAL

FORTALEZA
2021

LAURO DE ARAÚJO COSTA MOURA

SOB “TERMOS E CONDIÇÕES”: PRIVACIDADE, CONSENTIMENTO E AUTODETERMINAÇÃO INFORMATIVA NA ERA DIGITAL

Monografia apresentada ao Curso de Direito da Universidade Federal do Ceará, como requisito parcial para a obtenção do título de Bacharel em Direito. Área de concentração: Direito Constitucional.

Orientador: Prof. Dr. Márcio Ferreira Rodrigues Pereira.

FORTALEZA

2021

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

M887s Moura, Lauro de Araújo Costa.
Sob "termos e condições" : privacidade, consentimento e autodeterminação informativa na era digital / Lauro de Araújo Costa Moura. – 2021.
87 f.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2021.
Orientação: Prof. Dr. Márcio Ferreira Rodrigues Pereira.

1. Proteção de dados pessoais. 2. Privacidade. 3. Autodeterminação informativa. 4. Consentimento. I. Título.

CDD 340

LAURO DE ARAÚJO COSTA MOURA

SOB “TERMOS E CONDIÇÕES”: PRIVACIDADE, CONSENTIMENTO E AUTODETERMINAÇÃO INFORMATIVA NA ERA DIGITAL

Monografia apresentada ao Curso de Direito da Universidade Federal do Ceará, como requisito parcial para a obtenção do título de Bacharel em Direito. Área de concentração: Direito Constitucional.

Aprovada em: ___/___/_____.

BANCA EXAMINADORA

_____

Prof. Dr. Márcio Ferreira Rodrigues Pereira (Orientador)

Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Felipe Braga Albuquerque

Universidade Federal do Ceará (UFC)

_____

Doutorando Francisco Amsterdan Duarte da Silva

Universidade Federal do Ceará (UFC)

À minha mãe e minha irmã,
de quem a ansiedade me
demove.

RESUMO

A intensa presença das tecnologias cibernéticas no cotidiano da população é um traço marcante na sociedade contemporânea. A grande disposição de informações sobre indivíduos na rede motivou discussões sobre o direito à privacidade, sua importância e seus limites, à medida que as redes proporcionaram um ambiente propício à vigilância e à intromissão direta na personalidade do indivíduo. Com o intuito de garantir efetiva proteção individual e coletiva, articula-se o direito à proteção de dados como autônomo direito fundamental e direito da personalidade associado ao direito à privacidade, que em sua abrangência não acoberta suficientemente situações decorrentes dos avanços tecnológicos. A descoberta de técnicas para o aproveitamento de dados pessoais foi capaz de alçá-los a uma posição de alta valorização no mercado. Nesse contexto, sedimentou-se um mercado de dados pessoais, mesmo diante dos riscos à personalidade ocasionados pelo fluxo desordenado desses dados. A coleta e utilização de dados pessoais ocorrem segundo os termos do contrato telemático, com auxílio de documentos tais quais os termos e condições e políticas de privacidade. Entretanto, a legitimidade dessas operações com dados é discutível, em função das circunstâncias que envolvem a aferição de consentimento do indivíduo ante os termos do contrato. Sob análise, depreende-se que o atual sistema de coleta de consentimento nas plataformas digitais, chamado de *Notice and Choice*, é falho em garantir o esclarecimento necessário à tomada de decisão consciente do usuário a respeito das invasões a sua privacidade na forma das operações de tratamento de dados. Assim, faz-se necessária a busca por mecanismos que fortaleçam este consentimento e devolvam o poder de autodeterminação informativa ao indivíduo, como prerrogativa à própria proteção de sua personalidade. Com esse foco, verifica-se a importância da ação coordenada entre Estado, mercado e sociedade. Primeiramente, com a adoção da metodologia *privacy by design* nas tecnologias e empreendimentos, de ponta a ponta, por parte dos agentes econômicos. Da mesma forma, o Estado deve estabelecer uma regulamentação eficaz e em consonância com os valores da sociedade, dada uma visão contextualizada do fluxo informacional e do consentimento, segundo a teoria de Helen Nissenbaum, e fomentar na sociedade uma consciência coletiva a respeito da privacidade. Para a pesquisa, foram utilizados o método dedutivo e a abordagem qualitativa, com um amplo estudo bibliográfico acadêmico e legislativo.

Palavras-chave: Proteção de dados pessoais. Privacidade. Autodeterminação informativa. Consentimento.

ABSTRACT

The intense presence of cybernetic technologies in the daily life of the population is a distinctive feature of contemporary society. The large availability of information about individuals on the net motivated discussions about the right to privacy, its importance and its limits, as the net provides an environment conducive to surveillance and direct intrusion into the individual's personality. In order to guarantee effective individual and collective protection, it is necessary to view the right to data protection as an autonomous fundamental right and personality right, linked to the right to privacy, which in its scope does not sufficiently cover situations resulting from technological advances. The discovery of techniques to exploit personal data succeeded to raise its worth on the market. In this context, a market for personal data became established, even in the face of the risks to personality caused by the immoderate flow of data. The collection and use of personal data follows the terms of the electronic contract, supported by documents like terms and conditions and privacy policies. However, the legitimacy of these transactions with data is debatable because of the circumstances surrounding the assessment of the individual's consent regarding the terms of the contract. It results that the current system for verifying consent on digital platforms, named "Notice and Choice", fails to ensure the necessary clarification for users to make a conscious decision regarding invasions of their privacy in the form of data processing operations. Thus, it is necessary to search for mechanisms that strengthen this consent and return the power of informational self-determination to the individual, as a prerogative to the very protection of his personality. With this focus, it is possible to verify the importance of coordinated action between State, market and society. First, with the adoption of the privacy by design methodology in technologies and enterprises, from end to end, by economic agents. Likewise, the State must establish effective regulation in line with society's values, given a contextualized view of information flow and consent, according to Helen Nissenbaum's theory, and encourage a collective awareness of privacy in society. For the research, the deductive method and the qualitative approach were used, with a wide academic and legislative bibliographic study.

Keywords: Personal data protection. Privacy. Informational self-determination. Consent.

SUMÁRIO

1 INTRODUÇÃO

O desenvolvimento tecnológico, principalmente nas últimas três décadas, trouxe inúmeras revoluções de ordem social, econômica e política. A popularização da tecnologia nas amplas camadas da sociedade consolidou o vínculo entre ser humano e máquina, fazendo com que diversas atividades passassem a depender desta interação. Nesse contexto, estabeleceu-se também uma cultura de vigilância proporcionada pela utilização das tecnologias cibernéticas.

Com essas tecnologias, a quantidade de informação produzida sobre os indivíduos aumentou exponencialmente. Concorreu para isso a portabilidade de aparelhos digitais e a adesão a acessórios, máquinas e utensílios com funções associadas à internet. Dessa forma, foi aberto caminho para o mapeamento das atividades, da rotina, dos pensamentos, das opiniões e da própria personalidade do indivíduo, este agora registrado, traduzido e interpretado por meio de seus dados pessoais. A nova possibilidade de "conhecer" em profundidade o seu público, por sua vez, passou a fomentar a própria economia e o mundo digital, sedimentados agora no mercado de dados pessoais.

O registro, acesso e coleta de dados, no entanto, apesar de intrusivo, é dotado de legalidade. E o embasamento desta legalidade vem da manifestação de consentimento do usuário, concedida digitalmente em concordância com os termos de plataformas das mais diversas, na forma de documentos como Termos e Condições e Políticas de Privacidade, importando em uma espécie de contrato de adesão. Estas plataformas, assim, passam a possuir o direito de lidar com os dados de seus usuários dentro dos moldes "acordados", e, vale dizer, com insuficientes restrições legais e precária fiscalização por parte do Estado para efetivá-las.

Tornaram-se os dados pessoais a matéria-prima para a produção de uma ciência da previsão e indução do comportamento social, aplicável na sociedade cada vez mais dependente e articulada pelas redes digitais. Atualmente, o conhecimento gerado e organizado sobre o indivíduo é apto a moldar o comportamento, prever condutas futuras, ser objeto de análise para deliberações ou instrumento para a prática de crimes. A descoberta de técnicas para o aproveitamento de dados pessoais fez com que estes alcançassem o status de commodity diante do mercado.

Preocupa, porém, o fato de os indivíduos terem tão pouco domínio sobre qualquer desses processos, conquanto sejam capazes seus dados de impactar diretamente sua qualidade de vida, redimensionando a sua autonomia. Diz-se isso, pois a figura dos termos que demandam o consentimento para o uso das plataformas digitais e tecnologias cibernéticas são reconhecidamente ineficazes. Eles não são lidos e, quando o são, são parcamente compreendidos.

Nesse seguimento, emergiram nos últimos tempos discussões acerca da manifestação de consentimento dos usuários na matéria: o que determinaria o consentimento? O que seria dispensável e o que seria indispensável a ele? O que se espera deste consentimento ou do indivíduo que consente? Em suma, discute-se sobre a real legitimidade do consentimento e o seu condão de autorizar procedimentos de tratamento de dados, com grande potencial de lesividade à privacidade e ao desenvolvimento da personalidade dos indivíduos. Buscou-se desenvolver essa questão no presente trabalho.

No primeiro capítulo, buscou-se realizar uma breve retrospectiva histórica, com a análise da criação da internet e o desenvolvimento das tecnologias que partiram dela, bem como as repercussões que ocasionaram nas esferas sociais, e os desafios para o direito causados pelo surgimento dessas tecnologias disruptivas, em constante renovação e desenvolvimento. Em seguida, articulou-se um estudo sobre o instituto da privacidade e as suas diferentes conceituações com o tempo, até chegar à noção de direito à privacidade como o direito de exercer controle sobre as próprias informações e o seu fluxo. Em complemento a este estudo, analisou-se o direito à proteção de dados pessoais, que, além de ser depreendido do direito à privacidade, dele se desloca e ganha a importância de direito autônomo ante as novas realidades proporcionadas pela valorização da informação, mormente no ambiente digital, e os novos riscos decorrentes dela.

Exploradas as premissas do trabalho, aborda-se no capítulo seguinte a regulamentação de dados brasileira: a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que traz conceitos importantes como o de dado pessoal, tratamento de dados e consentimento, individualmente examinados. Atenção especial é dispensada ao instituto do consentimento, peça chave na discussão da proteção da privacidade no meio digital e especialmente caro ao modelo utilizado para a realização dos contratos de adesão digitais (chamados contratos telemáticos): o modelo *Notice and Choice*. Na mesma oportunidade, são evidenciadas as fragilidades deste sistema que é apoiado quase exclusivamente na vontade do usuário, nem sempre íntegra.

No último capítulo, então, são investigados métodos para o aprimoramento deste modelo, bem como alternativas a ele. Notadamente, lança-se mão das teorias de Helen Nissenbaum e as teorias de Robert H. Sloan e Richard Warner, que, articuladas, proporcionam uma transição para uma visão contextual da aferição de legitimidade do fluxo de dados pessoais, avaliada a partir de valores sociais, e oportunizam uma nova forma de pensar a legislação referente a dados que se utiliza da semelhança do mundo digital com as situações vivenciadas no cotidiano do mundo físico para a regulação das redes. A discussão culmina na necessidade

do estabelecimento de uma cultura de proteção aos dados pessoais no Brasil e de um compromisso generalizado com a privacidade, abarcando sociedade, mercado e Estado.

O tema se faz relevante dada a sua atualidade e presença no cotidiano da população, o que é amplificado pelo processo de digitalização das relações e das atividades – inclusive as econômicas e governamentais –, e pelo aumento da acessibilidade aos recursos tecnológicos, com custo cada vez menor e estrutura física reduzida e portátil. Tal quadro, capaz de demonstrar o contato constante do indivíduo com a tecnologia, também aponta para o aumento da quantidade de dados gerados e, por consequência, para a necessidade de salvaguardar os direitos relativos à inclusão digital em massa, postos em risco diante de vínculos jurídicos travados diariamente sob condições não raro arbitrárias.

Para a pesquisa, utilizou-se do método dedutivo, via pesquisa bibliográfica, com abordagem qualitativa, em razão da adoção de método comparativo entre outros ordenamentos jurídicos, além de ter sido realizado amplo estudo de artigos científicos, da legislação pertinente e literatura especializada, buscando agregar também conhecimentos e pesquisas de outras áreas relacionadas ao tema, como a psicologia e informática.

2 A REPERCUSSÃO DAS TECNOLOGIAS CIBERNÉTICAS NA SOCIEDADE CONTEMPORÂNEA E ALGUNS DE SEUS DESAFIOS PARA O DIREITO

De forma a iniciar o presente estudo, será abordado neste primeiro capítulo o desenrolar histórico que levou à concepção do que hoje se conhece como internet, de impacto massivo e global nas relações interpessoais, familiares, de trabalho, de consumo, e que foi capaz de redirecionar todo o sistema econômico. Em paralelo, tratar-se-á da importância do desenvolvimento de um conceito de privacidade na busca por resguardo jurídico diante das inúmeras mudanças de ordem social advindas da popularização das tecnologias associadas à internet, com destaque ao ascendente mercado de dados pessoais que põe em risco não só a privacidade dos indivíduos, mas a sua própria personalidade.

Em meados do século XX, o planeta lidava com os impactos políticos, sociais e econômicos de um cenário pós-guerra. Diante da tensão entre as duas potências mundiais que se destacaram nos conflitos da Segunda Guerra Mundial, a norte-americana e a soviética, sucedeu-se uma busca incessante e sem precedentes por avanço tecnológico, objetivando o estabelecimento de uma hegemonia a nível planetário, mormente no que diz respeito aos investimentos na área armamentista e na promoção da conquista pioneira do espaço.

A Segunda Guerra Mundial constituiu a base para as tecnologias que revolucionaram a microeletrônica, além de todo o esforço científico e de engenharia que ocorreu em torno do conflito. A Guerra Fria, por sua vez, proporcionou um contexto em que havia intenso apoio popular e governamental para o investimento em ciência e tecnologia de ponta, facilitando o seu desenvolvimento (CASTELLS, 2003).

Nesse contexto surgiu nos Estados Unidos a Arpanet, o que viria, após amplas reformas, a se tornar a internet: uma rede global de computadores, de arquitetura aberta e descentralizada, favorável à auto-expansão. Apesar de não ter sido um projeto de orientação militar *per se*, o seu desenvolvimento teve origem dentro do Departamento de Defesa norte-americano e isto impulsionou a sua evolução, principalmente em função do nível de recursos à disposição para que fosse construída uma rede de computadores e projetadas todas as tecnologias necessárias (CASTELLS, 2003).

Toda a parte relevante relacionada a avanços tecnológicos importantes à concepção da internet teve lugar em torno de instituições governamentais, além de universidades e centros de pesquisa de renome. Assim, ela se desenvolveu em um ambiente seguro, sob financiamento governamental, mas de uma forma que não houve repressão à liberdade de pensamento e inovação. A experiência de maturação da internet nos campi

universitários estimulou a liberdade e o caráter aberto das redes, que foi e continua sendo fundamental para o desenvolvimento dos protocolos de infraestrutura da internet, dizendo respeito tanto a sua arquitetura técnica quanto a sua organização social/institucional (CASTELLS, 2003).

A internet, que se tornou disponível na década de 1990 – período relativo a sua utilização pelas populações, ainda que a tecnologia tenha existido por longo tempo antes disso –, teve repercussão enorme no mundo dos negócios, revolucionando a prática das empresas e transformando-se em recurso decisivo ao impulsionamento da produtividade e competitividade nas mais diversas áreas, em uma economia interconectada, interativa, flexível e customizável. Condicionado pelos avanços tecnológicos, o negócio eletrônico marcou o cerne da emergência desta nova economia que alcançou o planeta inteiro, centrada na utilização das redes para organização e processamento de informação.

O computador, antes tido como máquina colossal de complexo funcionamento e alto valor, ganhou portabilidade nos computadores pessoais (do inglês *personal computer* – PC). Estes adentraram as residências, ampliando o alcance da tecnologia informática antes restrita aos centros especializados (RUARO; RODRIGUEZ, 2010). É dizer: um aparelho cujo funcionamento tem como alicerce dados – percebendo-os, acumulando-os, comunicando-os – passou a integrar não só os ambientes de trabalho, mas também o cotidiano dos núcleos familiares, o que se verificou cada vez mais intensamente com o tempo, como se percebe hodiernamente com a transferência da atenção e reverência conferida ao computador voltada para *smartphones* e outros aparelhos cada vez mais (inter) conectados, ao exemplo dos objetos que integram a Internet das Coisas[1] (do inglês *Internet of Things* – IoT).

Estas tecnologias, concebidas e aperfeiçoadas a partir das novas redes e com as mais diversas funcionalidades, podem ser enquadradas como Tecnologias da Informação e Comunicação (TICs). Elas seguem a nova lógica cibernética da interconexão. Segundo Silveira (2017, p. 15), "as sociedades informacionais se estruturam a partir de tecnologias cibernéticas, ou seja, tecnologias de comunicação e de controle". Distinguir-se-iam elas por produzirem um conjunto de informações (dados) a cada utilização, característica esta apta, por exemplo, a alterar a capacidade dos agentes econômicos de avaliar suas práticas e negócios em razão dos pareceres instantâneos viabilizados pelo fluxo de dados.

---

[1] Segundo Magrani e Oliveira (2018), a Internet das Coisas pode ser compreendida como um ecossistema de objetos físicos interconectados com a internet que propõem soluções para o cotidiano, criando assim um ecossistema computacional ubíquo voltado à facilitação da vivência das pessoas.

Como ressalta Bioni (2019), na “sociedade da informação” a informação avoca um papel central e adjetivante da sociedade, sendo seu novo elemento estruturante e reorganizador, comparável ao que fizeram antes a terra, as máquinas a vapor, a eletricidade e os serviços, respectivamente nas sociedades agrícola, industrial e pós-industrial. Na contemporaneidade, a informação é o elemento nuclear para o desenvolvimento da economia e seu fluxo mudou o formato desta, bem como remodelou o próprio capitalismo.

Num contexto de transformações proporcionadas pela evolução da informática, as últimas três décadas foram marcadas por uma presença crescente desse tipo de tecnologia no cotidiano. Tal fator teve o condão de ocasionar mudanças nos padrões de comportamento social, nos mecanismos de mercado e mesmo na relação de um povo com o seu governo. Estas mudanças, no entanto, nem sempre configuraram avanço. Ao contrário, a sucessiva necessidade de conexão constante trouxe desafios substanciais para o campo do direito, principalmente no que diz respeito à proteção da personalidade do indivíduo.

Apesar de a internet, em um primeiro momento de sua popularização, ter se escorado nos princípios da liberdade individual, da abertura e da cooperação, que não previam inicialmente qualquer forma de verticalidade e hierarquia (CASTELLS, 2003), novas tecnologias e regulações influenciadas pelos interesses entrelaçados do comércio e dos governos passaram a desafiar essa diretriz. Logo, com tecnologias de captura de dados e vigilância em associação com a assimetria no controle das informações entre os provedores e os usuários, a privacidade destes foi posta em xeque, problemática esta que continua a se refletir, se atualizar e se complexificar na contemporaneidade.

Essa realidade, que remonta às origens da nova economia, da própria internet e das Tecnologias de Informação e Comunicação (TICs), se perpetuou. Atualmente, de forma banal, os indivíduos abrem mão do seu direito à privacidade para ter condições de fruir das vantagens das redes e da hiperconectividade. Havendo a renúncia a esse direito à proteção dos dados – comparável a uma cessão, ou concessão – os dados pessoais tornam-se legítima propriedade de qualquer que seja o negócio que na rede se pratique, de seus controladores, e dos clientes destes.

Sob pretextos de segurança externa e interna, demandas da administração pública e interesses de mercado, amparados em um cenário globalizado, corrobora-se a diminuição de garantias e valores ditos essenciais a um Estado Democrático de Direito, no mesmo ritmo em que o direito fundamental à privacidade é transmutado em mero obstáculo à consecução de objetivos supraindividuais, frequentemente dizendo respeito à segurança pública e aperfeiçoamento do mercado (RUARO; RODRIGUEZ, 2010).

Nesse contexto, em um cenário de redes digitais e de uso crescente de tecnologias cibernéticas, fora pintado um retrato da privacidade como um direito anacrônico, datado. Diz-se que a existência da privacidade dificultaria não somente a ação do mercado para a coleta de dados, mas também a ação contra criminosos que se aproveitam desse direito, o qual alegadamente é protetor do crime, do desvirtuamento ou não cumprimento de regras, proporcionando assim a impunidade (SILVEIRA, 2017).

Ainda, há de se destacar que a maioria dos produtos e serviços online são "gratuitos", não havendo uma contraprestação pecuniária direta por parte dos usuários para sua fruição. Assim, apesar do acesso "livre" aos ambientes proporcionados pelas tecnologias cibernéticas, quais sejam, as redes sociais, serviços de correio eletrônico, motores de pesquisa, *softwares*, portais de notícias e aplicativos para *smartphones*, por exemplo, o novo modelo de negócio proporcionado pelo avanço tecnológico possibilitou uma via diversa de lucratividade.

Enquanto em um modelo de negócio tradicional consumidores trocam uma quantia pecuniária por um bem de consumo, sob o novo modelo os consumidores cedem seus dados pessoais em troca do acesso às plataformas e recebem publicidade direcionada. Onde havia uma relação bilateral entre o consumidor e o fornecedor fora incluída uma parte terceira, composta pelo anunciante de conteúdo publicitário, que viabiliza o retorno financeiro (BIONI, 2019).

Em muitos casos, por essa razão, a principal fonte de rendimentos das companhias de comércio eletrônico são a publicidade e o marketing. Tal aspecto possui dupla perspectiva. Se de um lado as empresas recebem o lucro das publicidades exibidas em suas páginas; por outro, utilizam os dados de seus usuários para aumentar a eficiência dos seus serviços ou os vendem para clientes para fins de marketing. Nesse sentido, cada acesso e cada clique do usuário passam a apresentar uma dimensão economicamente aproveitável, desde que eficazmente associados e analisados. Diante dessa "troca", o consumidor, ao fazer buscas, ler uma notícia de algum portal, enviar um e-mail ou postar nas redes sociais acaba movimentando o ciclo econômico.

Não demorou muito, então, para que se decretasse a morte da privacidade, sob o pretexto da sua falta de relevância. Segundo Sérgio Amadeu da Silveira (2017), consultores do mercado de dados pessoais produziram diversos discursos sobre as vantagens do fim da privacidade para a sociedade, defendendo que, para além de uma fatalidade, a sua morte seria bem-vinda. "Nesta concepção, talvez a morte da privacidade fosse a purificação social de algo que não gerava negócios, nem empreendimentos tão lucrativos quanto a possibilidade de uso dos dados do cotidiano pessoal" (SILVEIRA, 2017, p. 36). O resguardo da vida privada do

indivíduo, por esse prisma, é visto como entrave à geração de capital, sendo defendidos não somente os benefícios para o mercado, mas também as vantagens para os próprios indivíduos, que renunciariam alguns encargos originados pela condição de cidadão visando ao aperfeiçoamento de sua experiência como comprador.

Em função do facilitado acesso às ferramentas disponíveis na internet, estas de grande conveniência ao cotidiano dos usuários, destaca Bioni (2019) que a realidade do mercado de dados deve ser encarada com cautela. Isto pois o titular dos dados não tem real consciência do efetivo custo da transação, diante das inúmeras possibilidades de uso que podem ser feitas dos seus dados num contexto de armazenamento massivo e cruzamento intenso de informações. São desconhecidas as repercussões dessa operação econômica, seus prejuízos e benefícios, mesmo porque a coleta dos dados é contínua, sendo contínuo também o "pagamento" pelo produto ou serviço (na forma dos próprios dados), e imprevisível a sua utilização, inviabilizando a inferência sobre os custos efetivos da transação.

Com a consolidação das tecnologias da informação no cotidiano e a invasão paulatina de um espaço que antes era próprio (privativo) do indivíduo, e que estava sempre e somente sob sua supervisão – mas passou a ser compartilhado, publicizado e explorado mesmo que não público em si –, imperioso tornou-se que o Direito acompanhasse tais transformações sociais. A sociedade contemporânea experimentou uma nova percepção dos limites dos direitos da personalidade e a ciência do direito deparou-se com desafios que demandaram o investimento contínuo em novas ferramentas jurídicas para tratá-los.

Nesse sentido, como contramovimento, a manifesta intensificação de mecanismos de coleta de dados – cada vez mais avançados, eficientes e rápidos – e o tratamento de informações suscitou um aquecimento no resgate à privacidade, trazendo oportunamente à tona a consciência da necessidade de uma abordagem diferente ao cuidar do assunto. Assim, fez-se necessário inclusive um aprofundamento no estudo da própria infraestrutura da informação como componente fundamental, protagonista e objeto de debates, além de notável recurso da modernidade (RUARO; RODRIGUEZ, 2010).

Como colocam Ruaro e Rodriguez (2010), a despeito do propício crescimento da preocupação político-institucional no que concerne à tutela de dados, o nível de controle das pessoas sobre suas informações tem potencial de acarretar conflitos de segurança e de interesse comercial. A outorga de direitos e, notadamente, autonomia, ao indivíduo, segundo essa análise, não é desejável aos sujeitos que auferem lucro do tráfego exorbitante de dados. Assevere-se que o desenvolvimento da informática e o advento da possibilidade de armazenamento e concentração de dados de populações inteiras – de forma, sobretudo em sua

gênese, sub-reptícia – mobilizou todo um mercado e forneceu substrato para a condução política de diversos Estados.

É interessante perceber que, em face do agigantamento contínuo do papel da tecnologia na sociedade e suas repercussões na atualidade, a necessidade de uma intervenção de ordem jurídica objetivando amparar o indivíduo e administrar a influência e dominação de terceiros, grandes corporações e até do próprio Estado sobre a esfera privativa individual encontra entraves derivados da própria natureza do que se pretende regular. Isto em função das sempre em evolução, e por isso sempre recentes e inovadoras, tecnologias cibernéticas, que trazem elementos inéditos que fogem ao domínio do Direito tradicional e da compreensão das pessoas de um modo geral.

É preciso entender ainda que as tecnologias cibernéticas, representadas pelas TICs, e sua rápida evolução trazem certo grau de imprevisibilidade – notadamente quando se destacam inventos dotados de autoprogramação, inteligência artificial, *machine learning, deep learning* etc. – dificultando qualquer tomada de decisão que se dê em função apenas de um resultado ou consequência, ou mesmo previsão de um ou de outro. Diante do caráter experimental do desenvolvimento tecnológico neste campo, algumas consequências sociais provenientes de determinada tecnologia só emergem quando esta é implementada (MAGRANI, 2019).

Um desafio para o Direito, nesse sentido, consiste em "encontrar maneiras de desenvolver e regular essas tecnologias, de modo que elas alcancem seus objetivos, mantenham sua utilidade e, simultaneamente, protejam a privacidade e outros direitos fundamentais" (LEONARDI, 2011, p. 38). Isto pois a presença na sociedade dessas tecnologias disruptivas ligadas à internet deve ser tratada como irreversível e, embora a sua regulamentação seja urgente, não é oportuno que sirvam as ciências jurídicas e o legislador como entraves a revoluções proporcionadas pela informática. Afirme-se ainda que as tecnologias ligadas à internet como "novo" elemento no cenário social não exigem apenas novas soluções jurídicas para novos problemas, mas também transfiguram o prisma sob o qual tais questões devem ser analisadas.

Dito isto, vê-se necessário explorar o instituto da privacidade, bem como o direito a sua proteção, e a proveniência deste, atravessando sua evolução histórica e mudanças de percepção e conceituação. Ver-se-á a seguir também como se deu a adaptação do instituto da privacidade à realidade contemporânea e a problemática que diz respeito à captura do imenso fluxo de dados pessoais na atualidade, tendo esta aberto espaço ao reconhecimento do direito à proteção de dados pessoais sob a lógica da autodeterminação informativa.

2.1 A articulação de um direito à privacidade e à proteção de dados

A privacidade, como direito que salvaguarda a vida privada, apesar de ter se consolidado jurídica, social e subjetivamente na Modernidade, é efeito de embates sociais, políticos e econômicos, sendo, por isso, sujeita a variações históricas e condicionada à instabilidade (BRUNO, 2010). Nessa acepção deve-se levar em conta a sua inevitável ressignificação em vista da crescente interferência na esfera privada por parte do poder público (no exercício do poder de polícia e na atividade judiciária) e da maior possibilidade de intromissão de terceiros do âmbito da intimidade das pessoas, para o que impulsionam as inovações tecnológicas (LAFER, 1991).

Assim sendo, na atualidade, discutir a privacidade tornou-se urgente, visto que o instituto tem sido confrontado a cada momento com inovações tecnológicas as quais insistentemente buscam avançar divisas, movendo-se de forma progressiva a fim de possibilitar a expansão da vigilância – em concretização aos desejos do mercado e de governos, mas em detrimento da existência do indivíduo como sujeito de direitos fundamentais. Afinal de contas, como colocado por José Afonso da Silva (2014), o segredo da vida privada é condição de expansão da personalidade, sendo necessária ampla liberdade de realizar a vida privada sem intromissões de terceiros, restando fora do alcance do olhar público (ou número indeterminado de pessoas) eventos próprios da vida pessoal e familiar.

Para além disso, a proteção da vida privada coincide com diversos elementos do direito das liberdades públicas (às vezes funcionando em associação a eles, mas também em oposição, a depender do caso), tais quais a segurança (pensando num âmbito de vigilância, proteção contra investigações ilícitas), liberdade de imprensa e direito à informação, o direito à proteção da própria imagem e à liberdade de expressão (RIVERO; MOUTOUH, 2006), podendo ser somados a estes o direito à livre associação, o de liberdade de crença religiosa, os direitos de vizinhança e até mesmo o desenvolvimento regular da democracia (LAFER, 1991).

> A privacidade, como direito, tem por conteúdo a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão. […] No direito à privacidade, o objeto é, sinteticamente, a integridade moral do sujeito. (FERRAZ JÚNIOR, 1993, p. 440)

Tendo a proteção à privacidade um objeto intangível – a integridade moral do sujeito, como coloca Tércio Sampaio Ferraz Júnior – e sendo a repercussão de sua eventual lesão, em geral, materialmente imensurável, muitas foram as transformações sociais e legislativas ocorridas para que se firmasse hoje um conceito amplo de privacidade, possibilitando, a princípio, uma mais eficiente tutela dessa esfera do indivíduo.

Far-se-á um breve resgate histórico sobre a distinção entre a esfera pública e a esfera privada. Para os gregos a esfera privada compreendia o reino da necessidade, era o terreno do que era o próprio homem, que dizia respeito a sua sobrevivência imediata, o seu alimentar, repousar, procriar etc., atividades que ocorriam em casa. De forma diversa, a esfera pública era, esta sim, própria do cidadão (condição elitista à época), que, com seus iguais exerciam a prerrogativa de participar das ações políticas – o público era em si o âmbito do político – em um movimento de dignificação do indivíduo (FERRAZ JÚNIOR, 1993, 2018).

Diferente era no Direito Romano, conforme o qual a oposição entre o público e o privado se relacionava com a separação entre o que era de utilidade comum e o que dizia respeito à utilidade dos particulares, sendo declarada então a supremacia do público sobre o privado. Além disso, o público é também o que é visível, em oposição ao privado, ao secreto, ao que não se mostra em público, o que não precisa nem deve ter transparência, circunscrito ao âmbito privativo do indivíduo (FERRAZ JÚNIOR, 1993).

Todavia, como afirma Ferraz Júnior (1993), essas distinções mais ou menos rígidas perderam nitidez na era moderna. Isso ocorreu em virtude do aparecimento da noção do social, comum tanto à esfera pública quanto privada. Segundo o autor, o social público se referiria à área da política e o social privado à área do econômico, do mercado. Daí irromperam duas importantes dicotomias fundamentais aos direitos humanos modernos: a do Estado e sociedade, e da sociedade e indivíduo.

> É nesse contexto que surge a privacidade. O social privado, o mercado, passa a exigir a garantia de um interesse público (livre concorrência, propriedade privada dos bens de produção) que não se confunda com o governo (política), embora dele precise. Mas contra a presença abrangente e avassaladora do mercado que nivela os homens à mercadoria, contrapõe-se a privacidade do indivíduo. (FERRAZ JÚNIOR, 1993, p. 441)

Samuel Warren e Louis Brandeis, pioneiros no estudo relativo ao que hoje se tem como o direito à privacidade, no fim do século XIX, já dissertavam sobre os avanços e adaptações legais sob a jurisdição do modelo *common law* estadunidense diante das mudanças políticas, sociais e econômicas do país. No notável artigo "*The Right to Privacy*" dos autores, publicado na *Harvard Law Review* em 1890, a dupla traça brevemente a evolução na proteção

dos bens jurídicos pelo sistema jurídico do seu país, ressaltando a importância, para tanto, do protagonismo do poder judiciário para a sedimentação de alguns direitos.

Em análise à relevância e abrangência de alguns bens jurídicos protegidos pela legislação, notam os autores o marco inicial e abstrato do resguardo da pessoa humana, o qual residiria no princípio da proteção plena do indivíduo e da propriedade. No entanto, destacam eles a necessidade de contínua atualização na definição da extensão e natureza dessa proteção ante transformações políticas, sociais e econômicas, as quais ensejam o nascimento de novos direitos e compelem o progresso da legislação e da atividade judicante para que acompanhem os avanços da sociedade (WARREN; BRANDEIS, 1890).

Conforme seu estudo, partindo da proteção à incolumidade física da pessoa, da liberdade em sentido estrito e da propriedade – direitos primários e de pronto reconhecidos –, alcançou-se posteriormente e inevitavelmente o reconhecimento da dimensão espiritual do ser humano, em conjunto com seus sentimentos e intelecto. Gradualmente, o amparo jurídico (jurisprudencial e legal) aprofundou o simples e restrito conceito de proteção à vida em direção ao direito de aproveitar a vida, o qual englobava, como afirmam os autores: a concepção do que se referem como "direito de ser deixado só" ("*right to be let alone*"); a extensão do direito à liberdade ao exercício dos diversos direitos civis; e a incorporação da proteção das demais formas de propriedade, incluídos os bens intangíveis (WARREN; BRANDEIS, 1890).

Ressalte-se que a obra foi concebida em um contexto em que o direito à privacidade não possuía delimitação clara, sendo poucos os mecanismos para sua defesa em juízo, incluindo a lei que tratava da difamação (que viabilizava uma ação de reparação de danos) e a relativa à propriedade literária e artística, cuja utilização era limitada. Nem mesmo havia qualquer norma na esfera penal que salvaguardasse o indivíduo e a sociedade nesse aspecto (WARREN; BRANDEIS, 1890). Por essa razão, buscavam na obra evidenciar a urgência do estabelecimento de novos mecanismos para a defesa da privacidade de forma deslocada do direito à propriedade e da honra objetivamente considerada.

À época, a principal preocupação dos autores se voltava às menos que adequadas investidas da impetuosa indústria jornalística em detrimento da intimidade de indivíduos, bem como à popularização da mídia fotográfica e à possibilidade de sua circulação massificada e, não raro, não autorizada[2].

---

[2] As câmeras fotográficas portáteis foram inventadas pela empresa Eastman Kodak em 1884, apenas seis anos antes, ampliando sua acessibilidade.

> Se casuais e desimportantes declarações em uma carta, se trabalhos manuais, mesmo que inartísticos e sem valor, se posses de quaisquer gênero são protegidas não somente contra reprodução, mas também contra descrição e enumeração, quão mais devem ser guardados da publicidade implacável os atos e discursos de um homem em suas relações sociais e domésticas.[3] (WARREN; BRANDEIS, 1890, p. 213-214, tradução nossa)

Paralelamente, afirma Leonardi (2011) que a conceituação de privacidade apenas como o resguardo contra interferências alheias é vago e amplo – e por isso falho –, mesmo quando afirmada a sua constituição por três elementos distintos: segredo, anonimato e solidão. Estes, em última análise, se relacionam ao isolamento e ao sigilo, não abarcando o conceito atividades como a coleta, armazenamento e processamento de dados pessoais que não revelem segredos, não identifiquem imediatamente a pessoa ou perturbem a solidão. Para o autor, o entendimento da privacidade apenas como o direito a ser deixado só é marcado por um individualismo exacerbado, amparando uma situação de "relação-zero", um isolamento social, mesmo em contextos em que a interação é viável e até racionalmente inafastável, o que oportuniza o abuso de direito em função da fácil configuração da intrusão.

> Por derradeiro, é necessário observar que, mesmo em público, há privacidade: a mãe que amamenta seu bebê em público provavelmente não deseja que estranhos publiquem fotos de seus seios *online*, o rapaz gordo que frequenta um parque ou uma praia sem camisa não autoriza o resto do mundo a ridicularizar sua forma física na Rede. Além disso, a maioria dos hábitos de um individuo – os livros que lê, os produtos que compra e as pessoas a quem se associa – frequentemente não são segredos, mas ainda assim são considerados assuntos privados. O acesso mais facilitado de fatos públicos, possibilitado pela Internet, dificulta a assimilação e aceitação de um conceito tão polarizado como o da privacidade. (LEONARDI, 2011, p. 66)

Dessa noção muito bem justificada por Marcel Leonardi depreende-se a insuficiência da dicotomia entre público e privado para fundamentar o direito à privacidade atualmente. A vivência do indivíduo na contemporaneidade é altamente vulnerável no que diz respeito às intromissões na sua esfera individual, com o que contribuem as tecnologias amplamente acessíveis e multifuncionais. E aqui não se fala exclusivamente de publicização de segredos da vida íntima cuja revelação causaria constrangimento, ou da publicação de artigos em revistas de fofoca sobre a vida sexual de um casal de celebridades, mas também da rotina de uma pessoa comum – do "homem médio" –, seus relacionamentos, interesses, *hobbies*, fontes de renda, seus desejos, suas compulsões e gatilhos.

---

[3] *"If casual and unimportant statements in a letter, if handiwork, however inartistic and valueless, if possessions of all sorts are protected not only against reproduction, but against description and enumeration, how much more should the acts and sayings of a man in his social and domestic relations be guarded from ruthless publicity.*"

Importa evidenciar que a discussão abordada por Warren e Brandeis foi intensificada pela evolução tecnológica da época. Como colocam: “Agora que dispositivos modernos proporcionam inúmeras oportunidades de perpetração de tais ofensas sem qualquer participação da parte ofendida, a proteção garantida pela lei necessita ser ampliada”[4] (WARREN; BRANDEIS, 1890, p. 211, tradução nossa).

Nessa toada, como que em ciclo, a emergência contemporânea de um novo debate sobre privacidade se assemelha à que tomava lugar no fim do século XIX. Diferencia-se, logicamente, no que diz respeito às matérias controversas a serem tratadas, as quais hoje são relacionadas às transformações ocorridas nas últimas décadas dadas as mudanças nas áreas de informática, comunicação e vigilância.

Fruto do desenvolvimento dessas discussões, tomou forma a ideia de controle sobre informações e dados pessoais. Autores como Alan Westin (1967) inclusive concebiam a privacidade como a reivindicação de indivíduos, grupos ou instituições de determinar por si próprios quando, como e em que extensão suas informações são comunicadas a terceiros. Esta importante corrente de Westin, assevere-se, traz um sujeito mais ativo, que não simplesmente se recolhe aos recônditos da sua vida privada, temeroso com a possibilidade de divulgação de seus segredos mais íntimos, mas sim exerce, como protagonista, controle sobre essas informações e dados pessoais.

Nesse sentido, a privacidade não se resumiria apenas ao direito de ser deixado em paz de Warren e Brandeis, mas incluiria também a prerrogativa de delimitar o que cabe ser revelado ao outro da própria esfera de individualidade. Tal controle sobre as informações apresentada pelo conceito defendido por Westin desvelava então uma nova dimensão do direito à privacidade em amplo sentido: o que o Tribunal Constitucional Federal alemão em 1983 veio a nomear como o direito à autodeterminação informativa – reconhecendo ainda na ocasião o seu status de direito fundamental – (RUARO; RODRIGUEZ, 2010), cujo conteúdo é de grande valor para a discussão deste trabalho.

Em consonância com os estudos de Westin, entende-se o direito à autodeterminação informativa como “o direito de um indivíduo se proteger contra a coleta, o armazenamento, o uso e a revelação de seus dados pessoais, efetuados de modo ilimitado, direito esse que somente poderia ser restringido em caso de um interesse público superior,

---

[4] *“Now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon broader foundation.”*

com base constitucional" (LEONARDI, 2011, p. 70), noção esta que direcionará o atual estudo.

Leonardi (2011), pondera, no entanto, acerca deste último conceito de privacidade de Westin. Observa o autor o não estabelecimento de uma limitação razoável a este exercício do indivíduo de controle das informações e dados a seu respeito, tendo em vista a própria definição ampla de dado pessoal. Diante da funcionalidade material do Direito de defender o indivíduo – seja por meio da regulamentação direta e específica no caso das leis, seja por meio de preceitos abstratos que preveem prerrogativas ideais – a prática jurídica já demonstrou a necessidade de sopesamento de valores, bem como da prevenção contra abusos de direito.

Dessa forma, difícil se faz estabelecer um conceito aberto e perfeitamente aplicável de privacidade quando os seus moldes são refinados de fato na prática, assim como se transformam com o tempo e com a sociedade, como demonstrado. Ao passo que muitas informações pessoais correm pelas redes e atualmente seja virtualmente impossível acompanhar o ritmo proporcionado pela tecnologia, a proteção ao indivíduo e sua personalidade pode se dar sobre outras bases, outros fundamentos e até sob outro foco, como é o caso da proteção contra aferição de lucro em função do mercado de dados pessoais, resgatando um viés mais patrimonial da informação.

Daí decorre a importância da ideia de privacidade não apenas como o direito de ser deixado em paz, mas também como o controle sobre informações e dados pessoais, o direito de determinar que atributos de si podem ser utilizados por outros. Isto independe da natureza da informação ou dos dados, mesmo porque, tratando-se da esfera própria do indivíduo e da sua personalidade, deve caber ao indivíduo, dentro da razoabilidade posta em discussão por Leonardi, deliberar sobre a extensão do seu conforto, confiança e segurança em relação às ditas operações que tenham como objeto informações que versem sobre ele. "A privacidade é o poder de revelar-se seletivamente ao mundo"[5] (HUGHES, 1993, p. 1, tradução nossa).

Distanciando-se das abordagens eminentemente teóricas, é importante verificar ainda o tratamento dispensado ao instituto da privacidade por parte da Constituição Federal de 1988. Nela, dois dispositivos se destacam e são de relevância para este trabalho. São estes: o art. 5°, inciso X, da Constituição Federal de 1988: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano

[5] "*Privacy is the power to selectively reveal oneself to the world.*"

material ou moral decorrente de sua violação"; e o inciso 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" (BRASIL, 1988).

A Constituição Federal de 1988 trouxe inclusive a proteção ao sigilo de dados como hipótese nova, elaborada no art. 5º, XII, e correlata ao direito fundamental à privacidade (art. 5º, X), porém estabelecida de modo genérico e limitado. Registre-se que o contexto na década de 80 no País era, por lógico, diverso do atual. Não obstante, faz-se possível, por meio de técnicas hermenêuticas, a atualização de princípios (que de outra forma poderiam ser taxados como anacrônicos) para adequá-los às novas realidades da vida. Assim, na falta de previsão específica restou aos juristas a busca por reinterpretações dos direitos e garantias constitucionais a fim de assegurar uma proteção do indivíduo contra riscos advindos do processamento da informação.

Nesse seguimento, ressalta Doneda (2011) que, apesar de não haver em expresso o reconhecimento da proteção de dados pessoais como direito fundamental e autônomo na Constituição, este caráter sobreviria da "consideração dos riscos que o tratamento automatizado [de dados] traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada" (DONEDA, 2011, p. 103).

Dentro do âmbito da tutela da vida privada e da intimidade se faz imperiosa a delimitação de um espaço de autonomia no que concerne a aspectos existenciais do ser humano, isento da ingerência indevida da sociedade ou Estado. Isto se dá em função da afinidade da proteção da vida privada com o próprio desenvolvimento da personalidade, razão pela qual a privacidade atua de forma tão fundamental, alicerçando direitos outros conexos a ela. São estes, por exemplo, a proteção ao domicílio, ao sigilo de correspondência e das conversas telefônicas e telemáticas, à proteção contra a videovigilância, ao sigilo profissional e ao direito à proteção da vida familiar.

Vê-se que, embora as garantias de sigilo e inviolabilidade da intimidade e da vida privada configurem importantes mecanismos constitucionais de proteção individual, ante os efeitos do processamento e utilização de informações de indivíduos tal abordagem revela-se insuficiente. Estas garantias restringem-se a situações determinadas como a divulgação de informações íntimas ou interceptação de comunicação e não compreendem diversos riscos proporcionados ao indivíduo na sociedade da informação.

Ademais, como visto, proteger dados não se limita a tornar sigilosas informações, nem diz respeito somente a informações sigilosas. Em seu núcleo está a regulação de efeitos das informações na sociedade, notadamente no tocante ao seu fluxo, e a instituição de procedimentos de controle, focos estes cuja complexidade e especificidade tornam limitada a sua compreensão sob a ótica puramente constitucional, mesmo que seja a Constituição de interpretação dinâmica (MENDES, 2014).

> 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 [...]. E este hiato possibilita a perigosa interpretação que pode eximir o aplicador de considerar 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. (DONEDA, 2011, p. 106)

Diante disso, é de eficácia questionável que se busque em paradigmas do passado bases para solucionar controvérsias inéditas geradas na sociedade contemporânea. Em sentido semelhante, questionam Ruaro e Rodriguez (2010, p. 194): "a mera derivação do direito à proteção de dados pessoais do direito à privacidade, e não como direito fundamental autonomamente reconhecido, não arriscaria simplificar os fundamentos de tutela deste novo direito, o que implicaria na diminuição do seu alcance de proteção?"

Tal preocupação parece alinhada com a de Rivero e Moutouh (2006). Estes, abordando a necessidade de se decompor e pormenorizar as liberdades públicas, no plural, em oposição a reservar-se à ampla aplicabilidade do princípio de uma só liberdade global escrevem:

> Certas aplicações da liberdade são secundárias em comparação a outras, muito mais essenciais e que merecem por isso ser individualizadas visando uma proteção especial. […] A experiência prova que há setores nos quais a liberdade é, mais do que noutros, contestada e ameaçada, especialmente pelo poder: aí também impõe-se a necessidade de uma proteção reforçada. Assim justifica-se a individualização, no seio da liberdade global, de certas liberdades, que o direito reconhece e regulamenta de modo especial. (RIVERO; MOUTOUH, 2006, p. 20-21)

Com essas bases, ocupou-se a doutrina, e posteriormente a própria legislação, de desmembrar o estudo da privacidade aplicada ao novo contexto da sociedade da informação, esta atravessada pela massiva influência das redes – na figura de seu maior expoente, a internet – e pela utilização das Tecnologias de Informação e Comunicação, cuja potência advém da capacidade de interconexão sob a lógica cibernética.

Tal tratamento apartado, voltado eminentemente à proteção de dados pessoais como projeções da personalidade, visou à maior eficiência no encaminhamento jurídico das novas questões suscitadas pelos avanços destas disruptivas tecnologias que repercutiram no modo de funcionamento de toda a sociedade. Esta segmentação, possibilitada somente pelo fortuito desenvolvimento da ampla ideia de privacidade, servirá de ponto de partida aos temas que serão aprofundados a seguir: a proteção de dados, a autodeterminação informativa e a importância do consentimento na relação entre ambas.

2.2 A proteção de dados pessoais, a autodeterminação informativa e a influência do mercado de dados pessoais

A privacidade, instituto de reconhecida importância e objeto de diversas discussões e adaptações ao longo da história, positivado e assentado na prática judicial e também, em linhas gerais, na consciência social na maior parte dos países do globo, ganhou uma nova dimensão. O aumento da importância da informação para a era atual e a insistência da doutrina em dissecar o instituto da privacidade provocaram a emergência de um novo tópico multifacetado e em contínua expansão: o tópico da proteção de dados pessoais. Ressalta Doneda:

> Por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais. Para uma completa apreciação do problema, estes interesses devem ser considerados pelo operador do direito pelo que representam, e não somente pelo seu traço visível – a violação da privacidade. (DONEDA, 2011, p. 95)

Assim, a proteção de dados e o direito à autodeterminação informativa (incorporado à noção de privacidade) se mostram as duas faces da mesma moeda. São desdobramentos da garantia do desenvolvimento da personalidade cuja defesa o Direito por muito tempo menosprezou e, mesmo quando em pauta, fora incapaz de elaborar uma regulamentação adequada. É de relevo, então, que se explorem estes desdobramentos de um direito tido antes como razoavelmente consolidado.

Apresenta Bruno Ricardo Bioni (2019) que os direitos da personalidade fazem parte de uma cláusula geral de proteção, tutela e promoção da pessoa humana e têm como característica principal a sua elasticidade. Assim sendo, como coloca o autor, os direitos da personalidade seriam uma “noção inacabada” cuja exploração ainda há sempre de gerar frutos e, ao exemplo da legislação brasileira, não se limitam às situações previstas no Código Civil.

Por essa visão, seria possível reconhecer novas nuances dos direitos da personalidade e, dentro deste espectro, reconhecer a proteção dos dados pessoais como novo direito da personalidade.

Ressalte-se que o autor afirma consistir a função dos direitos da personalidade na promoção e garantia do valor-fonte do ordenamento jurídico: a pessoa humana, conforme a cláusula geral de proteção e todo o seu respaldo dentro do próprio sistema jurídico. Assevera que os dados pessoais podem ser reconhecidos como formadores de um "novo tipo de identidade" que se manifesta em um universo digitalizado, movimentado a partir de signos identificadores do cidadão que conduzem as relações sociais, a economia e até a relação de uma população com seu governo (pensemos, por exemplo, nas páginas oficiais que exercem função de colher a opinião pública sobre projetos de lei mediante cadastro digital vinculado ao CPF). Para tanto, porém, o referente dado deve ser adjetivado como pessoal, caracterizando-se como projeção, extensão ou dimensão do seu titular (BIONI, 2019).

Segundo Bioni (2019), essa realidade de projeção da identidade para um meio que transcende a materialidade acaba por justificar dogmaticamente a inserção da proteção aos dados pessoais na categoria dos direitos da personalidade, transbordando inclusive sua concepção jurídica superficial interligada à noção de privacidade quando, a saber, passa a ser discutida não mais somente a possibilidade de acesso e divulgação de determinados dados, mas também a sua exatidão e o consecutivo direito à retificação das próprias informações, consolidando a transformação do direito à proteção de dados para além do seu núcleo de liberdade negativa relacionada aos clássicos conceitos de privacidade.

Enquanto a substância da privacidade está associada ao controle de informações da esfera íntima e privada do sujeito, a proteção de dados não se contenta com tal abordagem, mesmo porque a informação pode estar sob a esfera pública e ainda ser digna de resguardo. A importância dessa alteração de visão se dá em função da ampliação do alcance normativo que passa a ser permitido, objetivando abranger toda e qualquer atividade de processamento de dados que impacta a vida de um indivíduo, mormente na sociedade atual em cujas relações são continuamente digitalizadas.

Além disso, acerca da exploração dos dados pessoais, pode-se afirmar que seus riscos ultrapassam os da mera violação da privacidade. A própria individualidade e autonomia do indivíduo, entre outros desdobramentos da sua personalidade, são colocadas em risco pela economia movida a dados, além de ameaçado o desenvolvimento regular da democracia (FRAZÃO, 2019). Essa problematização tem lastro nas práticas das quais os operadores de tratamento de dados se valem após a coleta de dados pessoais.

Conforme explanado anteriormente, o mercado de dados ampara especialmente setores da publicidade e propaganda direcionadas. Por meio do processamento de grandes bancos de dados, viabiliza-se a formação de padrões e perfis de comportamento e de consumo. Estes embasam previsões sobre probabilidades de tomada de decisão, possibilitando uma atuação direta de terceiros nesse âmbito para a condução ou reversão de condutas e modulação do comportamento do indivíduo, de impacto claro no desenvolvimento de sua personalidade (SILVEIRA, 2017).

Assim, o principal objetivo dos agentes que coletam dados não é tanto produzir saber sobre um indivíduo em questão, mas sim utilizar conjuntos de informações pessoais para agir sobre ele e também sobre outros indivíduos. Nesse aspecto, esse saber traduz-se em controle. Por essa razão, a vigilância muitas vezes se dá sobre informações e não sobre pessoas, visto que os dados em si mesmos não são reveladores nem interpretáveis de pronto, além de serem numerosos e fragmentados. Os indivíduos sobreviriam em um segundo momento, após técnicas de composição de perfis computacionais (Em inglês: *profiling*, ou perfilização) (BRUNO, 2006).

Vale ressaltar que esse poder de elaboração de perfis a partir do monitoramento de ações no ciberespaço e de aplicação destes para indução do comportamento convive relativamente bem com o anonimato dos sujeitos sobre os quais versam os dados. Ainda, por não necessariamente expressarem manifesta intrusão à privacidade, esquece-se que as repercussões dessas atividades se dão mais profundamente nas esferas da consciência, vontade e desejo do indivíduo (BRUNO, 2007). Como resultado, assevera Bruno, temos a criação de um conhecimento ao mesmo tempo impessoal e ultrapersonalizado, infra-individual e individualizado e, apesar de a coleta de informações não dizer respeito necessariamente à profundidade do indivíduo, paradoxalmente a sua aplicação se dá diretamente sobre o íntimo da sua personalidade (BRUNO et al., 2006).

Em suma, os bancos de dados possuem hoje a capacidade de desenvolver o perfil de uma pessoa com base em seus acessos às plataformas de internet, seu histórico de compras online, cadastros realizados no meio digital, interações em redes sociais, sua geolocalização capturada pelas TICs, e em tantas outras ferramentas auxiliares à vigilância, monitoramento e identificação por meio das quais são coletados diversos dados pessoais. Tal perfil funciona para atrair mercado consumidor ou moldar a opinião sobre pessoa ou assunto, bem como servem de alicerce a uma estrutura de tomada de decisão algorítmica que lida com questões de variada relevância e indiscutível impacto existencial.

Tem-se, assim, uma repercussão da formação de bancos de dados e do tratamento e comercialização de dados pessoais que tem relação com a influência na dimensão psíquica do indivíduo, atingindo o subconsciente deste a partir do direcionamento de informações – notadamente anúncios publicitários, mas podendo incluir também propagandas políticas, por exemplo – determinadas em associação aos padrões de comportamentos concebidos pelos seus rastros digitais.

Segundo Fernanda Bruno (2006), o modo de ação dos bancos de dados envolve ao mesmo tempo previsão, simulação e performatividade. Ou seja, o cruzamento de dados, estes representados pelo conhecimento infra-individual (caráter derivado da sua fragmentação) gerado pelo usuário, possibilita a projeção de perfis que antecipam preferências, tendências e padrões comportamentais tanto atuais quanto potenciais. Esses perfis orientam a intervenção no campo de ações e escolhas do usuário após o seu enquadramento nas categorias ou segmentos de interesse ao agente. A questão da performatividade relaciona-se à função "oracular" dos processos anteriores de previsão e simulação. Os efeitos que decorrem da antecipação por meio do perfil, mera construção probabilística, não se deve à previsão de um futuro certo e determinado. Ao contrário, a própria antecipação e ingerência sobre as probabilidades intervêm nas escolhas e comportamentos, tornando efetivo o que se antecipou.

Compara ainda a autora esse encadeamento da modulação de comportamento com uma cartografia circular e reversa, onde o mapa se sobreporia ao território por conhecê-lo, ao passo que nele influi, com o território curiosamente se acomodando às mudanças traçadas no mapa e não o oposto. O potencial performativo se concretiza quando o indivíduo torna efetivo, real, o que antes era possibilidade, ou mais que isso: potencialidade e probabilidade (BRUNO, 2006).

Outra questão a ser mencionada é a da tomada de decisão automatizada. Os mesmos dados que, processados, podem ser revertidos para finalidades de modulação de comportamento de indivíduos ou grupos, podem ser reorganizados, reapreciados e aplicados para resolver sobre, a saber, a seleção de indivíduos "mais aptos" ao exercício de um cargo em uma empresa, a determinação do custo de um plano de saúde, ou a decisão final acerca de uma concessão de crédito. Nesse sentido, os dados pessoais também redimensionam a autonomia e o livre desenvolvimento da personalidade do indivíduo (MONTEIRO; BIONI, 2015). Aqui também seria possível a aplicação da analogia cartográfica de Bruno (2006), com o território – a realidade – sendo substituído pelo que fora traçado pelo processamento massivo de dados na forma do perfil – o mapa –, a despeito da existência do próprio indivíduo, sua vivência e sua privacidade.

Se os dados pessoais expressam a personalidade do indivíduo no meio digital, o tratamento de dados com a extração de informações sobre aquele – via processamentos nos quais o titular dos dados não toma parte – podem gerar e fixar uma imagem que não é representativa da realidade e sobre a qual a pessoa retratada perde o controle. Essa imagem, um perfil digital, é capaz de substituir o indivíduo no mundo digital, o que pode trazer conveniências (como a abertura de uma conta em banco por meio de autentificação realizada virtualmente) e contratempos (o roubo de identidade e prática de fraudes utilizando-se de dados de terceiros; a negativa de uma vaga de emprego por decisão automatizada de desenrolar pouco transparente).

Nesse seguimento, dada a interdependência entre ser humano e tecnologia na contemporaneidade, o mundo que correntemente se diferencia por ser digital, incorpóreo, tem reduzido sua distância em relação ao mundo físico. É dizer que o mundo digital tem se tornado cada vez mais "real" e isto é endossado pela multiplicação das consequências ao indivíduo de acontecimentos que tomam parte unicamente nessa dimensão virtual.

Diante desse contexto, é claro, o reconhecimento do direito à proteção de dados como direito da personalidade implica na necessidade de seu reconhecimento como direito autônomo. Como dito, é importante que se amplie a visão dos dados pessoais para além do eixo da privacidade, visto que a prerrogativa do indivíduo de controle dos seus dados pessoais, manifestado por meio do direito à autodeterminação informativa, não tem como propósito único a permissão e negação ao acesso e utilização dos dados. Trata o direito, então, de uma possibilidade ampla de ingerência do titular dos dados sobre suas peças de informação difusas nas redes, seja para acessá-las, retificá-las, transferi-las ou apagá-las. Considerados os dados pessoais projeções do sujeito, é justo que se conceda e facilite a este o seu acesso e a prestação de informações de forma clara quanto ao armazenamento e utilização de ditos dados em todos os seus termos.

Ao consistir em direito autônomo, a proteção de dados passa a não mais ser condicionada à análise do instituto da privacidade, de onde fora depreendido e destacado. Sendo ainda correlatos, é justa a expectativa de que lesões à personalidade do indivíduo em função de vazamentos ou utilização incorreta de dados, por exemplo, venham a impactar a sua privacidade. No entanto, o tratamento da proteção a dados como tema apartado do direito à privacidade pretende trazer maior precisão e mais eficácia na abordagem das suas questões muito particulares. Isso em função da especificidade e tecnicidade demandada para cuidar do assunto oriundo do desenvolvimento da era informacional.

Tendo sido salientada até aqui a relevância da prerrogativa de autodeterminação informativa do indivíduo – este poder amplo de ingerência sobre informações pessoais – infere-se a necessidade de sujeição dos agentes que operam estes dados (notadamente atores do mercado, ou os governos) à fiscalização dos titulares dos dados e à proteção dos interesses e da personalidade destes. Vê-se que o consentimento do interessado é o ponto de referência de todo o sistema de tutela da privacidade (PAESANI, 2013), e, em particular, no atinente à proteção de dados pessoais. Nesse enquadramento, o consentimento passa a figurar como o instrumento por excelência da manifestação da escolha individual, seja como aspecto da autodeterminação, seja como instrumento de legitimação, dimensão que será aprofundada no próximo capítulo (RUARO; RODRIGUEZ, 2010). De qualquer forma, configurou-se como elemento determinante à análise das problemáticas relativas à legalidade e legitimidade do fluxo e utilização de dados pessoais.

O modelo centrado na manifestação de consentimento do indivíduo, apesar de apresentar razoabilidade em primeira análise, enfrenta questões de ordem prática advindas principalmente da dimensão subjetiva do consentimento em face da natureza de objetivação do direito e da heterorregulação na figura da atividade legislativa. Nesse sentido, surgem problemas como a apreciação da medida do consentimento, sua legitimidade, a harmonização entre as expectativas do indivíduo e a prática dos agentes de tratamento de dados, a capacidade do ser humano de – dentro de sua racionalidade própria – assimilar informações sobre o alcance e repercussão das operações a serem realizadas com seus dados, entre outros.

Tais problemas, que contêm aspectos profundos de subjetividade, dificultam uma regulamentação eficaz e em consonância com os princípios os quais a ordem jurídica pretende resguardar. Essa realidade se apresenta também em função da insuficiência da interferência do Estado para dar vazão ao conflito entre os direitos da personalidade e os interesses do capitalismo da informação.

Com isso em mente, afirme-se que direitos à privacidade e à proteção de dados tutelados de forma eficaz não dependem só de uma atuação legislativa e judiciária. Ainda que estabelecido o mais perfeito e delimitado dos conceitos (o que, como visto, é vital), antes, é razoável que se conceba como indispensável o desenvolvimento de processos políticos e educacionais nesse sentido. Dentre outras coisas, tais processos deveriam ter o objetivo de alertar e provocar a consciência crítica da população sobre o mundo de dados que permeia a sociedade, sobre o valor dos dados pessoais no atual cenário hiperconectado e sobre a atuação direta e indireta das esferas digitais na modulação de comportamentos, abarcando os

comportamentos relacionais, os políticos e, de forma especial, os de consumo (MAGRANI, 2019).

Este direcionamento faz-se fundamental diante dos encantos proporcionados pelas redes, que disponibilizam entretenimento, facilidade de acesso ao mercado para o consumidor, oportunidades de novos empreendimentos, e, permeando tudo isso, uma interação social a nível global, ao passo que desempenham um papel ativo na influência de decisões e têm impacto direto e temerário na forma como se percebe o mundo e como se atua nele. A apreensão de tal duplicidade é urgente; mas a percepção dessa realidade na sociedade ainda resta latente.

Nada obstante, a sedimentação da proteção de dados como direito da personalidade firma um novo ponto de partida para o encaminhamento jurídico de problemas relacionados à hiperconectividade e devassamento de informações para sustentar a economia de vigilância. Há de se reconhecer, porém, que ainda se está no início da trilha de transformação tecnológica e adaptação dos mecanismos intrusivos; estas não estagnaram. Nesse contexto, traçar um norte que facilite a interpretação e aplicação do direito na área da proteção de dados importa para que se consolidem conceitos e sejam fixados parâmetros de atuação, no que se refere à atividade dos sujeitos do mercado, dos indivíduos, mas também da doutrina e atividade judiciária para melhor tratar das devidas limitações e responsabilizações.

Após desenvolver, neste trabalho, o estudo do instituto da privacidade e, notadamente, do direito à proteção de dados pessoais ante as vivências na era da informação e a mercantilização de dados, o próximo capítulo pretende aprofundar a análise da coleta de dados mediante a utilização das tecnologias relacionadas à internet pelos usuários, com enfoque no instrumento concebido para viabilizar e legitimar a coleta e tratamento de dados: os contratos telemáticos. Para tanto, abordar-se-á a citada Lei Geral de Proteção de Dados Pessoais – que traçou diversas diretrizes necessárias sobre o tratamento de dados pessoais. Será de destaque no estudo, igualmente, a abordagem crítica da noção de consentimento trazida pela norma e de que forma se dá a aplicação desse instituto ante a realidade fática no cotidiano, digitalizado e profundamente marcado por sutis e solícitas intrusões na privacidade do indivíduo.

3 A LEGISLAÇÃO DE DADOS PESSOAIS NO BRASIL E A LEGITIMAÇÃO DO TRATAMENTO DE DADOS PESSOAIS

Já tendo sido abordados o avanço das tecnologias e sua onipresença na contemporaneidade – com suas repercussões na sociedade da informação, principalmente no que diz respeito ao direito à privacidade e à proteção de dados – o presente capítulo evidenciará em seu início a legislação brasileira de dados pessoais e os conceitos básicos de dados pessoais, tratamento de dados e consentimento, segundo seus dispositivos e a doutrina brasileira. Posteriormente tratar-se-á da emergência dos acordos telemáticos – aqueles celebrados por via digital –, analisando o seu papel na atualidade e investigando a eficácia e legitimidade da manifestação de consentimento do usuário segundo o formato rápido e desembaraçado do referente modelo de contratação: o sistema *Notice and Choice*.

Como visto, apesar de ter sido a Constituição Federal de 1988 fundamental ao reconhecimento do direito à proteção de dados pessoais, a sua leitura trazia ainda óbices à concretização deste direito por se mostrar insuficiente e parecer não abarcar a complexidade e a relevância dos dados e seu correspondente mercado na sociedade contemporânea. Fazia-se necessária, então, uma regulação específica que tornasse possível delimitar e facilitar a proteção do indivíduo, principalmente ante a construção doutrinária dos dados pessoais como projeções da personalidade e, em função disso, considerando o seu resguardo como propriamente um direito da personalidade.

Nesse contexto, em 14 de agosto de 2018 foi sancionada no Brasil a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, conhecida por LGPD (BRASIL, 2018). A norma empenhou-se em promover avanços no tocante à defesa e proteção de dados pessoais no ordenamento jurídico pátrio. No entanto, importa lembrar que não foi a primeira vez que o assunto foi tratado em matéria legislativa, podendo a proteção a dados pessoais ser identificada em outras leis especiais e setoriais como a de nº 8.078/1990 (Código de Defesa do Consumidor), Lei nº 12.412/2011 (Lei do Cadastro Positivo), Lei nº 12.527/2011 (Lei de Acesso à Informação), Lei nº 12.965/2014 (Marco Civil da Internet), dentre outras. Com isso, a regulamentação era, até então, nas palavras de Bioni (2019), uma “colcha de retalhos” que não cobria setores importantes da economia e, mesmo os que cobria, não o fazia com uniformidade em seu regramento.

Note-se que a LGPD, no Brasil, muito teve de influência dos debates que cercavam o assunto em âmbito internacional, notadamente no que dizia respeito ao Regulamento Europeu de Proteção de Dados Pessoais, o famoso GDPR (General Data

Protection Regulation), normatização adotada na União Europeia em 2016, que atuou como atualização da Diretiva da Comunidade Europeia nº 46, datada de 1995 – a qual então já abordava o tratamento e circulação de dados pessoais (MULHOLLAND, 2019).

Como forma de avanço legislativo, o que a LGPD veio a propor em matéria de dados pessoais e tratamento de dados foi uma sistematização de natureza geral, principiológica e programática em nível federal passível de ser aplicada tanto na esfera privada quanto na pública (MULHOLLAND, 2019). A legislação ainda internalizou a orientação constitucional quanto aos princípios da ordem econômica, estabelecendo uma dialética normativa que balanceasse a proteção ao consumidor, a dignidade da pessoa humana, a livre iniciativa, livre concorrência, além do desenvolvimento econômico-tecnológico e a inovação (BIONI, 2019).

No artigo inaugural da Lei Geral de Proteção de Dados Pessoais são enunciados os bens jurídicos os quais a norma pretende proteger em suas disposições. São estes: os direitos fundamentais da liberdade, privacidade, e o livre desenvolvimento da personalidade da pessoa natural (LGPD, art. 1º) (BRASIL, 2018). Afirma, por lógico, que o tratamento de dados pessoais, objeto principal da legislação, caso reste desregulamentado, apresenta potencial relevante de lesividade aos direitos do indivíduo. Tal risco motivou a movimentação da máquina estatal a fim de tratar da questão, seguindo inclusive a tendência global de estabelecimento de políticas de proteção de dados pessoais. Ressalte-se preliminarmente que a lei dispõe sobre o tratamento de dados pessoais "inclusive" nos meios digitais, como é colocado também no artigo inaugural (BRASIL, 2018). O presente estudo, como aponta desde o início, terá como enfoque o âmbito do digital.

Como exposto, a Lei Geral de Proteção de Dados Pessoais cumpriu a função de sistematizar a matéria de dados pessoais e suas modalidades de tratamento. Para tanto, e fortuitamente, elaborou alguns conceitos a fim de guiar a interpretação da legislação e auxiliar na aplicação dos princípios explícitos e implícitos em seu texto. Os conceitos principais são: dados pessoais, tratamento de dados e consentimento. Nesse seguimento, serão tais conceitos apresentados, dando destaque aos dispositivos da Lei Geral de Proteção de Dados Pessoais.

De início, é relevante que seja feita a interessante distinção entre "dado" e "informação". Apresentar-se-á em seguida o primeiro conceito basilar para o desenvolvimento deste trabalho: o conceito de "dados pessoais", pela legislação brasileira e pela doutrina. Segundo Doneda (2011), a palavra "dado" tem conotação mais primitiva e fragmentada, associada a uma "pré-informação", podendo consistir, por exemplo, em ato ou sinal, em estado anterior à interpretação e compreensão. A informação, por outro lado,

apresenta um sentido instrumental por já ter passado por uma fase inicial de depuração de seu conteúdo. Sob essa perspectiva, pode-se elaborar que a interação de um indivíduo (como uma "curtida" ou comentário) em uma publicação de uma determinada rede social consistiria em um dado. A significação ou tradução deste ato, que pode inferir um interesse por um gênero musical, posição política ou tendência de consumo, entretanto, consistiria em informação.

Em se tratando de dados pessoais, Mendes (2014) assevera que eles correspondem a fatos, comunicações e ações acerca de circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável. A autora afirma ainda que informações pessoais são aquelas que têm vínculo objetivo com o indivíduo por revelarem aspectos que dizem respeito a ele, a atributos de sua personalidade. Apesar da distinção entre os termos, o conteúdo de ambos se sobrepõe em várias circunstâncias, razão pela qual se justifica a sua utilização de forma mais livre neste trabalho, em consonância inclusive com as produções da doutrina especializada (DONEDA, 2011).

No que diz respeito à perspectiva legal, temos que no art. 5º, I, da LGPD define-se dado pessoal como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Destaque-se também aqui a equivalência com que o legislador trata os conceitos de dado pessoal e informação. A compreensão da extensão do conceito de dado pessoal, na figura da "informação", é indispensável para que haja a efetiva e eficaz aplicação da norma.

Quando se fala de "informação" para os fins da LGPD facilmente poder-se-ia recair na concepção restrita de que trata somente de informações escritas, tais quais: nome completo, idade, data de nascimento, números dos documentos de identificação, domicílio, endereço eletrônico. Embora estas obviamente tenham o caráter de dado pessoal, visto que são relativas à pessoa natural identificada ou identificável, outras mídias como vídeos, áudios e fotos (capazes de expressar informações nas formas gráfica, fotográfica e acústica) (MENDES, 2014) – mormente com o avanço tecnológico e o refinamento dos aparatos de vigilância, monitoramento e identificação de indivíduos – podem ser abarcadas sem grandes complicações hermenêuticas pela definição legal de dado pessoal, até mesmo por servirem cada vez mais eficientemente ao propósito de identificação de sujeitos. Além destes, dados como currículos escolares, dados profissionais, fiscais e bancários, dívidas e créditos, imagens recolhidas por câmeras de segurança, dados de saúde e biométricos também podem ser considerados dados pessoais (GEDIEL; CORRÊA, 2008).

Apresenta a lei ainda, em seu art. 5º, II, um conceito apartado relativo a "dados sensíveis". São estes, nos dizeres da lei, os que tratam 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" (BRASIL, 2018). A distinção é feita em função da necessidade de particular proteção devida a estas informações, num movimento que reconhece a possibilidade de segregação e preconceito advindas de sua eventual utilização arbitrária, abusiva e discriminatória pelos agentes de tratamento de dados.

Ressalta Mulholland (2019) que a definição legal de dados sensíveis não é taxativa ou exaustiva, mas sim exemplificativa. Assim, o conceito poderia abarcar outros conteúdos e situações não previstos no referido inciso, desde que algum contexto de seu uso represente ofensa à igualdade substancial no tratamento (amplamente considerado) dos dados.

Segundo a autora, não é só a natureza de um dado, estruturalmente considerado, que define o caráter especial de dado sensível. Deve ser levado em conta também que certos dados que, a princípio, não apresentem potencial lesivo em seu tratamento podem vir a ser considerados sensíveis a depender do uso que deles é feito. Tal fator está intimamente ligado aos avanços nas tecnologias, mormente no que diz respeito a algoritmos[6] complexos e inteligências artificiais, que, possibilitando a realização de cruzamento de informações, podem chegar a revelações as quais, estas sim, abalariam direitos fundamentais do titular e possuiriam potencial discriminatório (MULHOLLAND, 2019).

Como informações, genericamente, temos aquelas fornecidas voluntariamente – como nome, idade, data de nascimento, endereço eletrônico etc. – e aquelas extraídas no curso da utilização das plataformas digitais pelos usuários. Dentro deste último grupo poderíamos citar informações sobre: localização geográfica, endereço de IP (*Internet Protocol* – que permite a identificação de um usuário de computador), interesses, padrões de comportamento e padrões de consumo. Tais dados são de fácil levantamento, tendo em vista a intensa e crescente presença da sociedade nas redes sociais, popularizando-se inclusive entre os indivíduos de pouca idade.

Assevere-se que, em função da fácil aferição e organização destes dados – pelo automatizado cruzamento de informações dentro do próprio sistema, tendo como material páginas visitadas, buscas por conteúdos específicos, palavras-chave utilizadas em *chats* ou e-

---

[6] Segundo Magrani (2019, p. 19), algoritmos consistem em "conjuntos de regras que os computadores seguem para resolver problemas e tomar decisões sobre um determinado curso de ação. Em termos mais técnicos, um algoritmo é uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa, ou seja, uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa."

mails etc. –, muitas das análises podem apontar de forma imediata ou mediata a dados pessoais considerados pela lei como sensíveis, e por isso passíveis de maior proteção.

Afirma-se, então, a existência dessas duas ordens de dados pessoais geradas nos ambientes digitais. A camada superficial seria composta pelos dados pessoais que os indivíduos geram e disponibilizam voluntariamente. Estes dados, agregados em bancos de dados, processados e submetidos a técnicas de mineração de dados[7], são capazes de gerar uma segunda camada de dados – contendo perfis de consumo, interesses, comportamento, preferências políticas etc. – que podem ou não conter meios de identificação dos seus titulares (BRUNO, 2010). Assim, o avanço das tecnologias vulnerabiliza ainda mais o titular dos dados cujas informações fragmentadas estão dispostas nas redes, pois o conhecimento gerado pode a qualquer tempo ser reorganizado e reprocessado, dando luz a novas informações sobre as quais o indivíduo não mais possui controle direto (ou cuja existência desconhece).

Nesse sentido, imagens publicadas em uma rede social ou capturadas em rede de vigilância privada podem conter dados pessoais acerca da etnia, religião, orientação sexual, opinião política do indivíduo, da mesma forma que uma eventual triangulação utilizando-se de informações quanto a locais de acesso à internet em um aparelho móvel poderia apontar para estas mesmas informações (havendo ainda possibilidade da associação das duas abordagens, dando precisão aos resultados).

Mulholland (2019) cita o exemplo em que o bairro de residência de uma pessoa pode indicar a sua origem étnica. Tal análise poderia ocorrer, por exemplo, em bairros estadunidenses que apresentam grande parcela de moradores de etnia negra, ou também se analisarmos localidades que concentram comunidades judias ou de ascendência asiática. Interessante notar que o próprio nome da pessoa pode possuir uma carga indicativa de dados sensíveis quando composto por prenome e/ou sobrenome fortemente associados a específicas etnias, correntes religiosas ou ideologias.

Reafirme-se que qualquer dado pode tornar-se sensível caso explorado de forma a revelar informações cuja coleta a princípio não fora autorizada pelo seu titular e cujo uso seja dotado de potencial discriminatório ou de lesividade, dada a sua natureza inerentemente personalíssima. Soma-se a isso a possibilidade de terceiros também alimentarem as redes com dados sobre qualquer indivíduo sem que seja demandada deste uma autorização prévia (pensemos no maior exemplo: as redes sociais).

---

[7] Mineração de dados se refere à atividade computacional automatizada que extrai informações e padrões relevantes e/ou implícitos de um ou mais conjuntos de dados. (SLOAN; WARNER, 2014b)

No que pertine ao tratamento de dados publicizados voluntariamente pelos indivíduos a lei faz ressalva relevante, estabelecendo que mesmo nesses casos os agentes de tratamento devem se ater à finalidade, boa-fé e interesse público que justificaram a sua disponibilização (art. 7º, § 3º) (BRASIL, 2018). É dizer que: o fato de dados eventualmente não apresentarem qualquer óbice ao seu acesso não autoriza a sua utilização de forma displicente pelos operadores. Antes, cabe a eles ponderar sobre aspectos menos superficiais que cercam a disponibilização do conteúdo, o que configura, ao menos formalmente, avanço em matéria de proteção de dados pessoais.

Mas, afinal, em que consiste o tratamento de dados pessoais o qual busca a lei precipuamente regulamentar? A própria Lei Geral de Proteção de Dados Pessoais também fornece esse segundo conceito em seu texto, sob os seguintes termos:

> Art. 5º. Para os fins desta Lei, considera-se: X – tratamento: 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. (BRASIL, 2018)

Verifica-se que o conceito legal de tratamento de dados é abrangente, visto que até operações como recepção e reprodução de dados pessoais o integram. A intenção é de responsabilizar os agentes de tratamento por todas as atividades realizadas tendo como objeto dados pessoais e resguardar ao máximo os direitos fundamentais do indivíduo sob os fundamentos do respeito à privacidade, autodeterminação informativa, liberdade de expressão, inviolabilidade da intimidade, honra e imagem, entre outros (LGPD, art. 2°), servindo como um freio a fim de conter a exploração e utilização de dados sem a ciência ou consentimento informado dos usuários (FRAZÃO, 2019).

A fim de regulamentar e restringir a prática das condutas identificadas como tratamento de dados, a lei em seu artigo 7º estabeleceu em rol exaustivo as hipóteses em que elas podem ser legitimamente realizadas. Como epítome da proteção à autodeterminação informativa – explorada no capítulo anterior – o consentimento do titular é trazido logo no primeiro inciso, ressaltando sua importância como peça central no cenário do tratamento de dados, nos termos: “art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular” (BRASIL, 2018). Entre as outras hipóteses estão: a utilização de dados pela administração pública para execução de políticas públicas; por órgãos de pesquisa para realização de estudos; para o

exercício regular de direito em processo judicial, administrativo ou arbitral; para a proteção da vida ou incolumidade física do titular ou terceiro etc.

Apesar de o fornecimento do consentimento pelo titular dos dados ser somente uma dentre as dez situações previstas no dispositivo da LGPD que legitimam o tratamento de dados – sem haver, a princípio, distinção ou hierarquia entre elas –, a reiterada posição de destaque do consentimento não há de ser ignorada e reflete a vontade do legislador de sujeitar o controle dos dados ao conhecimento e aceitação do indivíduo. Afirma Mulholland (2019) que, a despeito da centralidade do consentimento na abordagem regulatória da proteção de dados, abre-se espaço para hipóteses que independem do consentimento e que foram colocadas na lei em posição de igualdade em relação à efetiva manifestação de autonomia do indivíduo, indeterminando a prevalência do consentimento e seu real papel na legitimação das operações com dados pessoais.

Ainda, destaca Bioni (2019) que na primeira versão do anteprojeto de lei colocada sob consulta pública em 2010 o consentimento era a única base legal para o tratamento de dados pessoais. A tendência se repetiu na sua segunda versão em 2015, quando as outras bases legais da LGPD foram incluídas no texto do anteprojeto em dispositivo autônomo, mas constituíam expressamente hipóteses de dispensa do consentimento. O texto que foi posteriormente sancionado, no entanto, dispôs todas as hipóteses horizontalmente num mesmo dispositivo.

Tal abordagem que primaria pelo consentimento já se apresentava na Lei nº 12.965/2014, o chamado Marco Civil da Internet (BRASIL, 2014). Nesta legislação, em seu artigo 7º, é assegurado ao usuário o não fornecimento a terceiros de seus dados pessoais salvo mediante consentimento livre, expresso e informado (ou nas outras hipóteses previstas em lei), e desde que a referente cláusula contratual esteja destacada das demais com informações claras e completas sobre a coleta, uso, armazenamento e proteção dos dados pessoais.

Isto leva ao último conceito, de importância fundamental para o presente estudo, o conceito de consentimento. Este é estabelecido no inciso XII do artigo 5° da LGPD como sendo a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018). Logo daí podemos extrair algumas características que, especialmente para os efeitos desta lei, foram tidas como determinantes ao referente conceito.

Sob o paradigma da legislação, o consentimento é tratado como uma manifestação de vontade do próprio titular dos dados (com capacidade jurídica) que seja: livre, isto é, sem o sentimento de coação ou obrigação relativa à prática do ato; embasada em conhecimentos

exatos e suficientes para uma tomada de decisão esclarecida; determinada a anuir com o tratamento de dados pessoais, para finalidade prevista e sob termos bem estabelecidos previamente. É dizer que, ausente na respectiva manifestação qualquer dos elementos dispostos, não há consentimento para os efeitos legais.

Vale ressaltar que, em matéria de aferição do consentimento relativo ao tratamento de dados pessoais sensíveis (aqueles aos quais a lei dispensa cuidado especial em função da possibilidade de discriminação em seu uso), a LGPD estabelece a necessidade de que a manifestação seja fornecida de forma específica e destacada, além de para finalidades determinadas (BRASIL, 2018, art. 11, I). Comparativamente, pode-se dizer que o tratamento de dados pessoais considerados sensíveis demanda um consentimento qualificado em função da posição de vulnerabilidade de uma das partes contratantes – o titular dos dados – e da sua mínima autonomia de deliberação acerca das condições do tratamento de dados, a despeito de abarcarem interesses seus de natureza personalíssima (MULHOLLAND, 2019).

Apresenta-se assim, sob a égide da legislação e do direito à autodeterminação informativa, o consentimento como referência para determinar o quão legítimas são as operações realizadas com dados pessoais. Consequentemente, quando estas ocorrem sem a coleta do consentimento ou tendo sido ele fornecido de forma imperfeita, há uma contaminação de todo o processo de tratamento que o torna ilegítimo e, portanto, ilegal, ensejando responsabilização dos agentes de tratamento, inclusive com sanções administrativas como a própria lei prevê (sem prejuízo à aplicação de demais penas estipuladas em leis específicas, como o Código de Defesa do Consumidor, conforme art. 52, § 2° da LGPD), desde que o contexto do tratamento de dados obviamente não se enquadre em qualquer dos demais casos elencados no art. 7º, que dispensam o consentimento.

Dessa forma trata a LGPD: “Art. 9°. § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca” (BRASIL, 2018).

Sob ótica diversa, para entender o consentimento como peça chave na discussão da proteção da privacidade no meio digital, viabilizando uma análise mais aprofundada em sua dimensão concreta em tópicos que se seguirão, importa também destacarmos o papel do consentimento nas relações contratuais abstratamente consideradas.

Lançando mão da melhor doutrina, apresenta Orlando Gomes (2009) o consentimento como elemento intrínseco do contrato, indispensável à sua validade. Possuiria o termo conceito duplo: o consentimento como acordo de vontades, a integração de vontades

distintas; ou como a declaração de vontade de cada parte independentemente considerada. Tal declaração, segundo o autor, far-se-ia mediante palavras, gestos ou sinais (conforme o meio empregado: de forma verbal, escrita ou simbólica), ressaltadas ainda as circunstâncias em que se deva atribuir valor jurídico ao silêncio.

Segundo Gomes (2009), faz-se o consentimento particularmente necessário nas figuras contratuais em comparação a outros negócios jurídicos bilaterais em função da contraposição de interesses das partes contratantes. Por isso, a declaração como exteriorização da vontade, para importar em consentimento, deve ser emitida com o propósito real de realização do contrato, ciente e consciente das consequências da avença.

> Para o consentimento ser perfeito, não basta que a vontade de celebrar o contrato seja livre e séria. Inexiste propósito de contratar *in abstrato*. A declaração de vontade há de ser emitida em correspondência ao conteúdo do contrato que o declarante tem em vista, atento ao fim que o move a contratar. Muitas vezes ocorre divergência entre a **vontade real** e a **declarada**. Quando se origina de certa causa, diz-se que o **consentimento** é viciado. (GOMES, 2009, p. 57, grifos do autor)

Acerca da forma de veiculação da declaração de vontade, a LGPD estabelece em seu artigo 8º que o consentimento condicionante do tratamento de dados deverá ser fornecido por escrito ou por meio diverso capaz de demonstrar a vontade do titular (BRASIL, 2018). Há de se ponderar quais meios diversos da forma escrita, conforme dicção da lei, seriam aptos a demonstrar a manifestação de vontade deste titular. A questão é deixada em aberto, possivelmente em virtude da dinamicidade das relações do mundo digital.

Em paralelo, estabelece a GDPR – norma anterior à LGPD que versa sobre temática semelhante na União Europeia – que consentimento do titular dos dados consistiria na "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento" (art. 4°, 11, GDPR) (UNIÃO EUROPEIA, 2016).

É interessante a colocação do legislador europeu ao imprimir a expressão "ato positivo" no texto legislativo, pois, ao mesmo tempo que parece aumentar expressamente a abrangência do que poderia configurar-se como manifestação de consentimento do sujeito, o faz de forma sutilmente calculada abarcando condutas comissivas (MULHOLLAND, 2019), em oposição à norma brasileira. Esta, além de não se referir aos legítimos veículos da declaração no próprio conceito de consentimento, quando o faz contenta-se com a vagueza da determinação de que aquele deverá ser fornecido "por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (art. 8º, caput). A expressão "outro meio"

parece trazer incertezas sobre sua circunscrição, como no que diz respeito ao reconhecimento da omissão e do silêncio como manifestações de vontade, por exemplo.

Deve ser ressaltado que, tanto no consentimento manifestado por meio escrito quanto em outros meios adaptados às relações digitais, as problemáticas de aferição da legitimidade do consentimento parecem se resumir basicamente à garantia de vontade livre e informada, sem coação, erro e outras máculas que digam respeito ao indivíduo, este devendo ser também dotado de capacidade (ainda que relativa) de praticar o referente ato. Porém, em se tratando de consentimento fornecido nos meios digitais a verificação de qualquer destes requisitos torna-se intrincada, revelando a distinção prática entre as duas formas.

Diante desse contexto, o mercado necessitou se adaptar à dinamicidade das redes e do fluxo informacional, à fugacidade da atenção difusa dos usuários e à ascensão do mercado de dados pessoais. Isto acarretou, por fim, a fundação de novas formas de travar vínculos jurídicos como solução de mercado. Ascende assim a figura do contrato telemático, conexo às figuras dos termos e condições e políticas de privacidade, analisadas a seguir.

3.1 Os contratos telemáticos no contexto do mercado de dados pessoais

A necessidade de diversificação dos meios formais de contratação e de manifestação de vontade em geral diante das relações cada vez mais digitalizadas se consolidou com a popularização irrefreável dos meios tecnológicos – computadores, smartphones, eletrodomésticos e utensílios “inteligentes” – e dos ambientes proporcionados pela internet (redes sociais, portais de notícias online, ferramentas de pesquisa, lojas virtuais, jogos online). Esse cenário impôs a prática das contratações também por meio diverso do que era habitual, agora por intermédio das redes.

Foram concebidos assim os chamados acordos telemáticos – acordos travados por meio digital. Eles funcionam como tipos contratuais muito próprios de seu meio, contagiado pela velocidade das interações, e, em função da sua forma mais livre, impessoalidade e por não admitirem modificações, aproximam-se da figura do contrato de adesão (LIMA, 2014).

Na doutrina de Orlando Gomes (2009) o contrato de adesão trata-se de método de estipulação contratual que surgiu das necessidades da vida econômica, distinguindo-se pela sua uniformidade, abstratividade, predeterminação e rigidez. Isso tudo objetivando a repetição em contratos singulares de cláusulas preestabelecidas por uma das partes, eliminando, em geral, a fase das negociações preliminares. O modelo reduz custos e aumenta a celeridade,

ambos convenientes, em primeiro plano, tanto para o usuário quanto para o provedor, possibilitando ainda uma maior abrangência em seu alcance.

> É certo que o contrato de adesão é praticável quando os interesses em jogo permitem, e até impõem, a pluralidade de situações uniformes, de modo que, sob esse aspecto, é, com efeito, oferta feita a uma coletividade. A necessidade de uniformizar as cláusulas do negócio jurídico elimina a possibilidade de qualquer discussão da proposta, criando para o oblato o dilema de aceitá-lo em bloco ou rejeitá-lo. Nada disso o distingue porquanto tais características são comuns a outras figuras jurídicas. […] O traço característico do contrato de adesão reside verdadeiramente na possibilidade de predeterminação do conteúdo da relação negocial pelo sujeito de direito que faz a oferta ao público. (GOMES, 2009, p. 138-139)

Fazer o paralelo entre os acordos telemáticos e as figuras contratuais tradicionais vem a ser de grande relevo por colocar em evidência a juridicidade dos compromissos travados digitalmente, mesmo que aparentem excessivamente simplificados e, à primeira vista, sem maiores repercussões na esfera jurídica dos envolvidos, notadamente para a parte hipossuficiente na relação – o usuário – que costuma encarar tais acordos com passividade.

Sabendo-se que não há viabilidade na exigência de uma manifestação de consentimento expressa e direta, a exemplo da assinatura física, nas relações contratuais do meio digital, essa manifestação de vontade em aquiescência a operações de tratamento de dados realizadas por toda a rede, na generalidade dos casos, é dada por meio de acordos no modelo *click-wrap* ou *browse-wrap*, por intermédio também dos Termos e Condições e Política de Privacidade do respectivo serviço ou portal online.

Segundo Adam Gatt (2002), acordos digitais – aqui abordados como telemáticos – são uma adaptação dos acordos chamados "*shrink-wrap*"[8], utilizados desde o início dos anos 1980 na ocasião da venda massificada de *softwares* em mídia física para computadores. O acordo ou licença no modelo *shrink-wrap* consistiria na prática da venda e/ou envio do produto juntamente como um acordo padrão (também disponível para consulta antes da venda), o qual não mais demandava assinatura de qualquer das partes. O consumidor estaria sujeito a seus termos a partir da abertura do produto físico, com a remoção do invólucro plástico (AN OVERVIEW..., c2020). A sua adoção fora necessária após enfrentada a frustração da utilização do tradicional método de contratação individual com cada usuário em um mercado com demanda crescente, modelo que se revelou insustentável (GATT, 2002).

---

[8] O termo *shrink-wrap*, em sua literalidade, diz respeito ao processo de envelopar um produto físico (uma caixa, por exemplo) com plástico a fim de lacrá-lo; embalar a vácuo. "*Shrink*" pode ser traduzido como reduzir, diminuir de tamanho; e "*wrap*" como envolver, embrulhar.

Como evolução do modelo *shrink-wrap*, os acordos realizados tendo como plataforma a internet vieram a ser conhecidos como acordos "*click-wrap*", hoje utilizados universalmente. De forma quase autoexplicativa, a sua denominação deriva do fato de que a conclusão dos acordos se daria no momento em que o usuário assente com os termos e condições da plataforma ou serviço selecionando, com um clique, algum botão que indique a sua concordância, na mesma oportunidade em que confirma a leitura dos termos e condições e demais políticas (como as de privacidade) a que fazem referência (GATT, 2002). Na contemporaneidade, tal é a condição para o acesso da maioria dos conteúdos e serviços nos meios digitais. A despeito, é claro, de consistirem em acordos realizados completamente via internet (acordos telemáticos), devem ter validade tal qual o contrato tradicional e seguem as normas que o regulam.

Uma expressão associada aos acordos *click-wrap* que igualmente merece ser ressaltada diz respeito ao modelo de acordo *browse-wrap*, que designa a prática comercial em que os termos e condições de uso do *site* ou serviço online são dispostos em página diversa da inicial ou daquela na qual o consentimento é solicitado e só podem ser acessados via *hyperlink* localizado usualmente no canto inferior da página (LIMA, 2014). Assim, não haveria a requisição direta de um aceite, visto que o próprio prosseguimento na navegação do *site* ou utilização do aplicativo o presumiria (STROINK-SKILLRUD, 2020). A prática, assim como acontece com os acordos *click-wrap,* também promove a celeridade da contratação, com a redução da quantidade de informações na página da internet, e a presunção do aceite do usuário. Isto se dá em função da fortuita ocultação dos termos do acordo a ser travado, sendo o usuário obrigado a ativamente buscá-los ("*browse*") caso deseje lê-los.

Documentos como os Termos e Condições e Políticas de Privacidade regem a relação do indivíduo com o referente provedor, definindo o que cabe em matéria de direitos e obrigações a cada parte, além de dispor sobre: regras de utilização de serviços como *sites*, plataformas e aplicativos; a proteção à propriedade intelectual dos conteúdos veiculados pelas partes; responsabilidade e limites de responsabilização etc. (OLIVEIRA et al., 2019).

Outras expressões e formatos podem ser utilizados para sua designação, tais quais: "acordo do usuário" ("*user agreement*"), "condições de uso" ("*conditions of use*"), "termos de uso" ("*terms of use*"), "avisos legais" ("*legal notices*"), "termos" ("*terms*") e "termos e condições de uso" ("*terms and conditions of use*") (LIMA, 2014).

Tratando-se de acordos no meio digital, é notável que as disposições que demandam o consentimento do usuário versam sobretudo sobre a coleta e utilização de dados pessoais, operações que geram o lucro capaz de garantir a rentabilidade do oferecimento

gratuito do produto ou serviço. Para tanto, por força legal, as disposições dos termos e condições devem explicitar informações tais quais: os tipos de dados que são recolhidos, quem poderá ter acesso a eles, sob que condições, por quanto tempo e para que finalidade, sendo tais termos vinculantes a ambas as partes, desde que legais e não abusivos *in concreto*.

Esta coleta pode ser realizada para viabilizar o bom funcionamento de um serviço (como os de localização, por exemplo), assim como fortalecer a sua segurança (como na garantia da identidade do usuário tal qual declarada em uma operação financeira). O que ocorre também é a composição de bancos de dados de diversos indivíduos e a utilização e comercialização destas informações para fins de marketing direcionado via processo de perfilização (*profiling*), como abordado no capítulo anterior.

É que portais, *websites*, aplicativos de celular, entre outras plataformas, dentre as quais são incluídas as Tecnologias da Informação e Comunicação, utilizam-se da coleta de dados pessoais como forma de capitalizar uma atividade oferecida como gratuita ao usuário ou garantir uma rentabilidade que transcende a relação de compra e venda inicial com o consumidor, no caso dos objetos "inteligentes" – de natureza interconectada e oriundos da lógica cibernética ao exemplo da Internet das Coisas. Assim, é demandada por lei a coleta do consentimento do usuário como condição para qualquer operação de tratamento de dados pessoais, de onde provém a renda de tais serviços, considerando-se, por isso, a remuneração como indireta. O consentimento é confirmado digitalmente com a aceitação dos termos e condições do respectivo serviço pelo usuário.

O paradigma que permite as práticas de uso e coleta de dados nas redes baseada nesse meio de verificação do consentimento do usuário é chamado de "*Notice and Choice*" (ou "*Notice and Consent*"). A palavra "*notice*"[9] faz referência à apresentação dos termos que contêm as informações sobre as políticas do agente de tratamento, em tese capaz de informar a decisão ou escolha ("*choice*") do usuário na forma do seu aceite (SLOAN; WARNER, 2014a). O modelo faz incumbir ao indivíduo todas as decisões relativas a seus dados pessoais, reservando aos agentes de tratamentos o dever de disponibilizarem as informações necessárias para esclarecer as suas escolhas.

Ainda que efetivos em garantir celeridade na celebração do acordo entre usuário e fornecedor do produto ou serviço diante do cenário da urgência por agilidade e dinamismo nas redes, o modelo *Notice and Choice,* os termos e condições e as políticas de privacidade enfrentam problemas que colocam em risco a legitimidade do consentimento fornecido: os

---

[9] Em tradução livre: notificação, aviso, comunicação.

primeiros seriam relativos a como são concebidos os termos, ao conteúdo que apresentam; os segundos seriam relativos à recorrente forma de sua disposição nas páginas da internet e a como são percebidos pelo usuário (este último caráter dizendo respeito ao indivíduo, mas com íntima e clara relação com os referentes mecanismos).

Dedicando-se inicialmente ao conteúdo dos termos (expressão aqui escolhida para tratar também das políticas de privacidade, a eles correlatas), crítica recorrente diz respeito à tecnicidade das suas disposições, que se tornam ininteligíveis para a população em geral, distanciando-a da pretensa finalidade dos termos que seria informar e melhor fundamentar a tomada de decisão do indivíduo. Não raro isso ocorre para que sejam ocultadas do indivíduo particularidades sobre a coleta dos seus dados. Paralelamente, a extensão dos termos se faz longa o suficiente de forma a desestimular a leitura ou dispersar a atenção do leitor (MAGRANI; OLIVEIRA, 2018; FREITAS, 2017).

Acrescente-se que, no contexto da globalização e do caráter unificado e interligado da internet, não necessariamente o usuário terá o domínio do idioma no qual foram redigidas as disposições dos termos do portal acessado. Tal fator torna a leitura ainda mais intricada, catalisada novamente pelo uso de termos técnicos ou específicos que podem fugir mesmo ao vocabulário daqueles com algum conhecimento prévio do idioma. Não obstante, a necessidade de acesso àquele conteúdo pode sobrepor a barreira imposta pela linguagem, sendo inepta, em qualquer dos casos, a falta de compreensão para o impedimento da manifestação de consentimento do usuário.

O próprio hábito generalizado da população de ignorar a leitura dos termos necessita ser ressaltado (FREITAS, 2017), principalmente em função do papel que tais documentos assumem no acordo telemático – de natureza eminentemente contratual e jurídica por excelência. Considerando a não leitura dos termos e a inconsequente manifestação de consentimento que costuma se seguir, poder-se-ia cogitar que o mercado de dados restaria alicerçado sobre uma (ou mais) geração de acordos telemáticos de legitimidade questionável.

Um estudo conduzido em 2015 por Obar e Oeldorf-Hirsch (2018) publicado sob o título *The Biggest Lie on the Internet* (A Maior Mentira na Internet, em tradução livre) pretendeu analisar a relação de usuários da internet com políticas (termos de serviço e políticas de privacidade) de redes sociais. Para isso, solicitaram que 543 participantes se inscrevessem em uma suposta nova rede social chamada NameDrop, inspirada na rede LinkedIn, e cujas páginas acessadas foram criadas somente para os fins da pesquisa.

Segundo a pesquisa, no ato de inscrição 74% dos participantes nem mesmo acessaram as políticas de privacidade. Aqueles que a acessaram investiram em média 74

segundos em sua leitura (que, em sua inteireza, deveria tomar entre 29 e 32 minutos, segundo cálculos dos autores), dispensando também 51 segundos aos termos e condições (que deveria tomar de 15 a 17 minutos de leitura). Ainda, somente nove – correspondendo a 1,7% dos participantes – evidenciaram a existência da cláusula que determinava expressamente e de forma destacada uma das formas de pagamento do serviço como consistindo na cessão do filho primogênito do usuário (caso não tivesse filhos, a cláusula teria validade até o ano de 2050). Não obstante, dois destes participantes que identificaram tal cláusula aceitaram os termos (OBAR; OELDORF-HIRSCH, 2018).

Aponta o estudo que, para os usuários, as referentes políticas agiriam somente como uma inconveniência, um óbice ao real propósito do acesso à internet. Não seria desejo dos usuários que houvesse intervenções com os fins de educação ou discussão sobre a utilização dos meios digitais (OBAR; OELDORF-HIRSCH, 2018), principalmente quando eles não têm o conhecimento do quanto valem seus dados e nem querem lidar com as complicações de administrá-los (DATA..., 2017; MAGRANI; OLIVEIRA, 2018).

Diante disso, argumenta-se ainda que tal desídia poderia estar teoricamente obstaculizando que o mercado agisse de forma a produzir seus termos mais eficientemente, análise esta, porém, que não explica o fenômeno do desinteresse do usuário pelas cláusulas do próprio contrato. Esta crítica é de Russell Korobkin (2003), que assevera ainda: "eficiência requer não somente que consumidores estejam cientes do conteúdo de contratos de adesão, mas também que eles o incorporem em sua inteireza nas decisões de consumo"[10] (KOROBKIN, 2003, p. 1217-1218, tradução nossa).

Somando-se a isso, temos que o aderente teria o "dever-de-ler" ("*duty to read*") os termos do contrato em sua integralidade, "sob pena de sofrer o ônus da vinculação a uma cláusula contratual desconhecida" (LIMA, 2014, p. 10). Consoante doutrina anglo-saxã, desde que seja dada a oportunidade para a leitura e entendimento do acordo ("*hypothetical knowledge*"), a manifestação pode importar, sim, em consentimento, pois teriam sido assumidos os riscos das consequências do contrato (SLOAN; WARNER, 2014a).

Para além das discussões a respeito da efetiva leitura dos termos e condições e políticas de privacidade pelos usuários, questões são levantadas a respeito da própria percepção a nível cognitivo do indivíduo, relativas a sua capacidade de compreensão e internalização das informações disponíveis nas disposições contratuais, quando lidas. Para

---

[10] "*efficiency requires not only that buyers be aware of the content of form contracts, but also that they fully incorporate that information into their purchase decisions.*"

abordar esse assunto, é necessário questionarmos até que ponto o avolumamento da informação apresentada ao indivíduo efetivamente amplia a sua capacidade de tomar uma decisão consciente, garantindo um grau de "eficiência" da internalização da informação, como trata Korobkin (2003).

Estudos sobre a racionalidade limitada ("*bounded racionality*") do ser humano e sobrecarga de informação ("*overloaded information*") têm apontado que nem sempre há correspondência entre o aumento da quantidade de informação disponível e o aumento da capacidade decisória (livre e consciente). Verifique-se, por exemplo, que o impacto das informações em indivíduos não é linear, não sendo suficiente o aumento quantitativo da informação para que pessoas de baixo nível de escolaridade – em contraposição às camadas sociais de maior privilégio e melhor educação – capacitem-se materialmente a formar uma decisão sem vícios intrínsecos (mesmo que, ao manifestar a vontade, seja dissimulada na forma do "eu aceito" a pouca compreensão dos termos). Ao contrário, nesse caso, a influência do aumento quantitativo das informações na garantia do esclarecimento do indivíduo seria pouca o nenhuma (MACEDO JUNIOR, 1999).

Outro aspecto a ser ressaltado é o da tendência do ser humano em focar nos benefícios imediatos, valorizando-os em detrimento dos possíveis prejuízos. Trata-se esta da chamada teoria da decisão da utilidade subjetiva (BIONI, 2019). Alocando essa observação no cenário da sociedade informacional, é dizer que o titular dos dados pessoais, ante o acesso a um popular produto do mundo digital – seja este uma rede social, jogo online ou um aplicativo de celular que concede convenientes descontos –, tende a criar distância em relação a riscos a que poderia estar se submetendo ou à própria perda do controle sobre informações pessoais, cujas repercussões no momento da decisão se apresentam como futuras, improváveis e até desimportantes quando contrastadas com as vantagens imediatas do produto ou serviço pleiteado.

Insere-se na equação da avaliação de vantagens e riscos, também, a inclinação dos indivíduos a estimar ou perceber probabilidades com base na subjetiva e individual facilidade de rememorar objetos que se enquadram numa mesma classe. Em outras palavras, o grau de exposição de uma pessoa a certo acontecimento influencia a sua capacidade de ponderar sobre a frequência e probabilidade da ocorrência de situações semelhantes (TVERSKY, KAHNEMAN, 1974).

Essa análise é aplicável ao objeto deste trabalho visto que, em razão do massivo fluxo de dados – que adquiriu uma enorme fluidez e dinamicidade com o evoluir da tecnologia –, a frequência a que a sociedade é notificada a respeito de situações envolvendo

segurança de dados é mínima em face do número de ocorrências, dada a dificuldade de fiscalização, a efetiva complexidade em resguardar os dados no ambiente digital e a regulamentação incipiente dos Estados sobre a matéria.

Estima-se que no primeiro semestre do ano de 2020 o Brasil tenha sofrido mais de 2,6 bilhões de tentativas de ataques cibernéticos (BRASIL SOFREU…, 2020). Além disso, de 47 países monitorados, o Brasil estaria em 46ª posição em matéria de velocidade de detecção de vazamento de dados – à frente somente da Turquia –, sendo de 46 dias a média de tempo entre um evento de vazamento de dados até a sua detecção pela empresa invadida, enquanto nos Estados Unidos a detecção ocorreria entre 24 e 48 horas (DEMELLO, 2021). Ademais, mesmo quando são expostas na mídia, as situações parecem abstratas e distantes, sem repercussões negativas palpáveis.

Tendo isso tudo em mente, não parece verdadeira a afirmação de que o titular de dados, ao tomar parte em uma relação contratual por intermédio do modelo *Notice and Choice*, em consonância com as práticas dos acordos *click-wrap* e *browse-wrap*, estaria capacitado a balancear vantagens e desvantagens para ao fim tomar uma decisão ótima, em consonância com seus interesses, expectativas e sua segurança, acerca da coleta e utilização dos seus dados pessoais.

Nesse sentido, soluções aparentemente lógicas como a de informar mais para informar melhor podem se revelar ineficazes em função das limitadas funções cognitivas do ser humano, incluindo sua falha memória, que afetam julgamentos e sua capacidade de decisão. Apesar de, por vezes, percorrer uma trilha racional de pensamento, seus desvios e inclinações podem induzir o indivíduo a erro. Desse modo, teorizações que determinam causa e efeito sem incluir a humanidade do indivíduo demonstram-se falhas, visto que a linha de pensamento que levaria a uma escolha racional (no plano do ideal) difere da que resulta na escolha real (SUNSTEIN et al., 1998). Esse contexto de falibilidade da cognição humana inclusive favorece os setores que buscam o poder de ingerência na personalidade do indivíduo, sendo facilitada a coleta de autorizações formais apesar de estas não refletirem a realidade material do consentimento, não importando as escolhas do indivíduo em, de fato, escolhas livres, esclarecidas e conscientes.

Em um cenário em que o usuário é somente um dos sujeitos atuantes na rede – entre tantos que se encontram inseridos no controverso mercado de dados – toda a navegação é pensada em função dele, do indivíduo que é consumidor e ao mesmo tempo mercadoria. Buscando conferir fluidez, dinamicidade e intuitividade para esse acesso, no entanto, há uma suavização da realidade, uma ocultação de atores e interesses no processo de navegação

individual. Tal fantasia existe em prol do usuário, “otimizando a sua experiência” (como é comum que se diga) ao passo que transmite a ele ilusões de controle, de poder de decisão e, por fim, de autodeterminação.

Ruaro e Rodriguez chamam a atenção para as duas dimensões do consentimento, a de autodeterminação e a de legitimação:

> Se por um lado [no consentimento] está presente o caráter de autodeterminação, funcionando como condição de acesso à esfera privada [do indivíduo], também há o aspecto da legitimação propriamente dita quando da inserção de dados em algum tipo de mercado, seja ele qual for. Desvela-se, por estes argumentos, o problema do consentimento e seus matizes – autodeterminação e legitimação – no âmbito da proteção de dados pessoais, buscando sempre um equilíbrio entre ambos. (RUARO; RODRIGUEZ, 2010, p. 196)

O que os autores ressaltam é que, ao mesmo tempo que a manifestação de consentimento age como ferramenta em prol da prerrogativa de decisão do indivíduo sobre as suas próprias informações – caráter de autodeterminação –, também serve de legitimação para o tratamento de dados e seu correspondente mercado. Segundo eles, no contexto dos dados pessoais, o consentimento (tradicionalmente associado a mecanismos negociais) deve ser abordado de modo a evitar que se torne um instrumento de exoneração em favor do mercado, capaz de neutralizar direitos fundamentais (RUARO; RODRIGUEZ, 2010).

Tomam parte nisso, obviamente, os agentes que compõem o mercado de dados, aproveitando-se da hipervulnerabilidade do usuário e da desigualdade informacional entre as partes contrapostas de forma a extrair o máximo possível dos dados pessoais, os verdadeiros ativos econômicos da contemporaneidade. Colhem, então, os frutos lucrativos da resignação e mesmo incapacidade cognitiva dos usuários em tomar decisões eficientes e “racionais”. Estes, que não são esclarecidos suficientemente da dimensão da importância de seus dados pessoais como projeções do sujeito, mostram-se impotentes e acabam ostentando a sua pseudoautonomia em controlar as próprias informações (BIONI, 2019).

Tendo a tecnologia evoluído com a promessa de, em suma, conectar, em todas as dimensões possíveis, atribuiu-se um senso lúdico ligado às possibilidades de entretenimento, engajamento em redes sociais, novas facilidades ao consumidor e empreendedor (independente de ramo e relevância no mercado) etc. Tal brilho irreverente ofusca ainda hoje a seriedade da intensificação do digital no cotidiano, bem como a percepção da eficácia dos compromissos travados virtualmente.

Isto parece se dar em função também de a liberdade no meio digital criar no usuário um senso de irresponsabilidade sobre os próprios atos, impulsionada pela sua pretensa

anonimização. Ademais, a aparente benevolência de portais provedores de produtos e serviços de fato úteis – os quais são ofertados não raro com gratuidade – aprofunda a confiança do usuário e constroem uma identidade positiva conveniente às empresas, que, perpassando-as, imprime uma sensação de segurança e confiança no ambiente digital de forma geral.

Ao dar o seu aceite aos termos e condições, então, o indivíduo presumidamente manifesta concordância com todo o consignado, sem reservas, e aprova todas as atividades que dizem respeito a dados pessoais realizadas pela plataforma, seus controladores e os sujeitos ligados a estes (desde que constem nos referidos termos e estes não sejam revestidos de ilegalidade, como estabelecido). O fornecimento dos dados acaba por tornar-se requisito para utilização do serviço, o qual, em geral, é tendencial e tendenciosamente gratuito.

Nesse ritmo, rotineiramente "concorda-se" com termos de diversas plataformas, seja por serem desprezadas ou mal compreendidas as consequências daquele aceite, em virtude da necessidade do serviço ofertado, por razões de trabalho, estudos, entretenimento ou mesmo num movimento de integração social. Para isso concorrem a dinamicidade do acesso e a fortuita – mas condicional – gratuidade dos serviços. A ilusão criada é que o usuário desfruta das tecnologias cibernéticas e não arca com qualquer ônus por isso, ou que qualquer consequência negativa seria mínima e improvável em contraste com as vantagens oferecidas.

> A noção de gratuidade deve ser tida com ressalvas. Os maiores provedores de serviços gratuitos, com parte daqueles oferecidos pela Google, tem como contrapartida o aceite pelo usuário quanto à coleta de dados pessoais, hábitos de consumo e outras informações que, uma vez agregadas e organizadas, têm valor comercial expressivo. Assim, embora um serviço de *e-mails* comum possa ser gratuito no sentido de não envolver pagamento em dinheiro por parte do usuário, isso não significa que ele ocorra sem qualquer tipo de retorno dos usuários em favor das empresas ofertantes. (ASTONE; FERES, 2017, p. 355)

É interessante perceber que a própria cogência na coleta do consentimento dos usuários nos meios digitais antecipa a sua importância, tanto para a preservação do que diz respeito aos direitos e interesses mais íntimos do indivíduo quanto para o resguardo da parte que solicita a manifestação de vontade, que busca o amparo jurídico para a regular e legal execução das suas atividades. Sustenta-se, assim, que a decisão consciente partiria de uma interiorização dos benefícios reais e dos custos reais de um negócio, aliada a um fidedigno alinhamento de expectativas entre usuário-consumidor e agentes do mercado, o que, como transparece, demanda proatividade não só da parte que define os termos e os apresenta, mas também dos que são expostos a eles e indiferentemente se sujeitam.

Na prática, ocorre que a funcionalidade e fluidez da navegação são privilegiadas em detrimento da garantia da obtenção da vontade legítima do usuário. Assim, o valor da

manifestação do indivíduo é mitigado e nasce a incerteza acerca do caráter de consentimento que lhe é atribuído. Isto está diretamente associado à redução dos dados pessoais ao aspecto meramente patrimonial, em contraposição à sua dimensão existencial que a legislação pretende acentuar, em consonância com a doutrina e as normatizações em dimensão global (FRAZÃO, 2019).

A despeito da atenção dispensada pela comunidade jurídica e científica em âmbito global acerca da imperiosidade da implantação de políticas públicas de proteção a dados pessoais dos cidadãos, as práticas relativas aos contratos telemáticos condicionados por uma padronizada manifestação de vontade sob o modelo *Notice and Choice* restam consolidadas há décadas em adaptação ao seu meio característico, tornando-se corriqueira a convivência com suas falhas, limitações e eventuais riscos à privacidade e personalidade dos usuários.

Considerando o quanto a matéria dos dados pessoais, sua importância e os riscos de sua administração precária – bem como a ligação íntima entre estes e direitos fundamentais como os da liberdade e privacidade – estão em pauta atualmente, não há de se sucumbir à comodidade, ignorando as emergentes discussões acerca do uso das plataformas digitais e a intercessão com o mundo do direito, principalmente quando parece não haver soluções perfeitas para os conflitos existentes.

É certo que os seres humanos se tornaram involuntariamente – ou inevitavelmente – reféns da tecnologia e dos algoritmos que os encapsulam e os rotulam, ao passo que são buscadas a promessa da hiperconectividade e suas facilidades. Esta mudança no funcionamento da sociedade, apesar de drástica, é também sutil e quase imperceptível. Falta consciência crítica sobre toda a situação de dependência entre o real e o digital. Há conveniência na troca cada vez mais frequente entre ser humano e máquina, na sua esfera social, nas relações econômicas e de trabalho. Entretanto, assevere-se que o pano de fundo que ampara essa alta funcionalidade e personalização tecnológica muitas vezes atende a disputas políticas ou modelos de negócio privados que visam a maximizar os lucros, não tendo como foco necessariamente a concretização de direitos fundamentais como o acesso à informação, expressão, cultura e, por fim, a própria privacidade (MAGRANI, 2019).

São questões como essas que dão peso e urgência à necessidade de resguardo aos dados pessoais. Infelizmente, a efetivação deste direito é irregular e muitos dos desafios enfrentados pela sociedade da informação acerca da proteção de dados têm conexão com a vulnerabilidade específica estabelecida na relação do indivíduo com os agentes de tratamento de dados, com a qual contribui imensamente a desigualdade na instrução dos indivíduos sobre a problemática, que reflete diretamente na qualidade e legitimidade subjetiva da sua

manifestação de vontade. No próximo capítulo, com uma análise dos papéis do Estado, do mercado e da sociedade na busca pela efetivação do direito fundamental à privacidade, explorar-se-ão alguns recursos práticos e teóricos que têm o fim de auxiliar a população na melhor ingerência de seus dados e na potencialização de sua aptidão para consentir.

4 A BUSCA PELA LEGITIMAÇÃO DO CONSENTIMENTO NO MERCADO DE DADOS PESSOAIS

Foram expostos anteriormente alguns dos processos de tratamento pelos quais passam os dados pessoais e como a sua utilização pode afetar negativamente dimensões íntimas do indivíduo que ultrapassam a lesão à privacidade, atingindo o seu direito à autodeterminação informativa, autonomia, individualidade e desenvolvimento da personalidade. A problemática da precarização no trato dos dados pessoais, mormente no que diz respeito à legitimidade do consentimento colhido, enfraquece direitos fundamentais e atrapalha a consecução dos objetivos de legislações como a Lei Geral de Proteção de Dados Pessoais.

Questões que devem ser evidenciadas são a desigualdade entre o usuário e os agentes do mercado (uma relação marcada pela hipossuficiência do indivíduo, portanto) e a deficiência de informação do usuário em relação aos termos a que se submete (endossado pelo modelo de contrato de adesão), principalmente acerca de quem detém seus dados, como são tratados, em que extensão e para quais fins reais, tangíveis e determinados.

No centro da discussão, então, tem-se o próprio modelo adotado para celebração dos acordos telemáticos, na forma do sistema *Notice and Choice*, que, a despeito da nomenclatura, não tem proporcionado uma tática de notificação e informação eficaz, nem, por consequência, contribuído para uma escolha consciente do usuário. Neste último capítulo abordar-se-ão medidas que visam a amparar os indivíduos no tocante a seus direitos fundamentais à privacidade, à proteção de dados e à autodeterminação informativa, partindo primeiramente de mecanismos pertinentes à concepção das tecnologias e todo o sistema do mercado de dados, na forma da autorregulação, para depois ser analisado o papel do Estado e sua heterorregulação nesse impasse que busca equalizar interesses do mercado e a privacidade.

O sistema de notificação, que se irradiou globalmente, com a adoção do consentimento “informado” como instrumento de legitimação das atividades empresariais e do mercado de dados, propõe o fundamento de que a coleta, o manejo e o processamento de dados (todos os três abarcados pelo termo tratamento de dados segundo a LGPD) são questões de escolha individual. No entanto, como posicionam-se Barocas e Nissenbaum (2014), ainda que fosse possível a concepção de meios para a melhor instrução dos usuários sobre as práticas contidas em termos e políticas das plataformas digitais a respeito da privacidade individual do usuário, o consentimento à luz da tecnologia atual já teria perdido a sua função

prática. Isto se daria em função do que os autores chamam de “tirania da minoria” (“*tyranny of the minority”*), a circunstância em que a recusa da manifestação de consentimento de alguns perde a eficiência diante da adesão em massa da população, que em si já provê material suficiente para que sejam inferidas informações por assimilação sobre estes dissidentes, minando a privacidade de forma ampla.

Diante desse quadro, importa repensar o sistema *Notice and Choice*. Considerando a assimetria informacional, a vulnerabilidade específica do usuário-consumidor na relação com os agentes de tratamento de dados, a complexidade dos procedimentos de tratamento e as teorias que sinalizam a racionalidade limitada do indivíduo, passa a ser discutível a aptidão deste em desempenhar um processo genuíno de tomada de decisão para controlar seus dados pessoais. Sendo assim, a conjuntura tanto legal quanto econômica que eleva o consentimento à posição de elemento central e suficiente para justificar a própria existência e viabilidade do mercado de dados, apoiada em uma autodeterminação e autonomia imperfeitas, falha em efetivar princípios e direitos básicos e caros à ordem jurídica, entre eles o da própria privacidade e, pode-se dizer, dignidade, razão pela qual uma reavaliação é imperativa.

Antes de analisar algumas propostas que têm sido apresentadas por especialistas e pesquisadores visando a aprimorar a segurança de dados e o status do direito à privacidade das populações, cabe aqui primeiramente um breve desvio para que se discuta um mecanismo diverso cuja utilização, em conjunto com o sistema *Notice and Choice*, intenta ainda hoje dar legitimidade à comercialização de dados pessoais. Este mecanismo consiste na técnica de anonimização de dados pessoais.

Sobre ela, asseveram Gediel e Corrêa (2008) que, a primeira vista, a anonimização parece conciliar os interesses do mercado, do Estado e do indivíduo. O mercado, como visto no capítulo anterior, de fato não necessita da identificação da pessoa para operar seus negócios de marketing direcionado, entre outros; o Estado teria interesse em dados estatísticos para estabelecer políticas públicas; o indivíduo, por sua vez, teria, em tese, a sua intimidade poupada no processo. Afirmam os autores, porém, que “essa perspectiva ‘neutraliza’ a dimensão política do controle sobre o acesso e o uso das informações. Ela empurra para fora dos limites do Direito a discussão sobre os poderes sociais associados a esse controle” (GEDIEL; CORRÊA, 2008, p. 151). Isto, pois, ainda que a anonimização pretenda revestir as projeções da personalidade do usuário em um nível maior de segurança (tornando-o não identificável), não garante a utilização de forma não discriminatória dos dados e não remedia a problemática acerca da perfilização e dos mecanismos adjacentes de controle.

Em que pese a adoção do processo de anonimização, a finalidade a que servem os dados na sociedade da informação independe da precisa identificação do indivíduo-usuário. Os dados pessoais na contemporaneidade são o elemento-chave para a formação de perfis de comportamento, de consumo e até de opções culturais e políticas. Sendo assim, com a crescente digitalização das relações, massivos bancos de dados reúnem a matéria-prima para a produção de uma verdadeira ciência da indução do comportamento social, condicionando o mercado capitalista à microeconomia da interceptação de dados pessoais (SILVEIRA, 2017).

A própria LGPD dispõe no sentido de que poderão os dados que passaram pela anonimização ser considerados dados pessoais para os fins da lei, caso utilizados para a formação do perfil comportamental de determinada pessoa natural, se identificada (art. 12, § 2°) (BRASIL, 2018). Sobre o tema, destaca Bioni (2019) que o foco não está no dado, mas no seu uso – a formação de perfis comportamentais – e que as expressões "determinada pessoa" e "identificada" devem ser compreendidas com relação à sua repercussão na esfera do indivíduo. Segundo ele, deveria o referido dispositivo ser aplicado mesmo que essa identificação diga respeito a um grupo, sem haver propriamente a individualização, visto que já é suficiente para que uma série de decisões sejam tomadas a respeito do indivíduo.

Por esse prisma, não há de se encarar o processo de anonimização de dados como o apogeu da sua proteção. Basta a atribuição de um identificador eletrônico único ao usuário e a contraposição rígida entre dados pessoais e dados anonimizados verifica-se como ficção, principalmente no que diz respeito à técnica de *profiling*, cujo objetivo é de alguma forma influenciar a vida de uma pessoa ao expô-la a conteúdo direcionado ou definir a apresentação de uma oferta ou oportunidade, tudo conforme peças de informações previamente colhidas e associadas. Tais "identificadores anônimos" que caracterizam a técnica de anonimização de dados apresentam-se somente como meio diverso de identificação, independente das categorias tradicionais de identificação, porém não diferindo delas em propósito (BAROCAS, NISSENBAUM, 2014).

Assim, as implicações na esfera do livre desenvolvimento da personalidade se configuram praticamente como objetivo final do tratamento de dados de legitimidade precária, num contexto macro da sociedade da informação, com atores sociais dotados de poder tanto econômico como informacional para antecipar decisões e então conduzi-las. Repise-se que o foco não está no dado, mas no uso que dele será feito, e nas repercussões na esfera do indivíduo, razão maior da proteção dos dados pessoais e dos direitos da personalidade. Ainda, há uma amplificação disto em função da incompreensão do panorama geral por parte daqueles impactados.

Tecidas as críticas acerca dos moldes do sistema *Notice and Choice*, bem como sobre a viabilidade da anonimização dos dados como alternativa primária para a garantia dos direitos dos usuários, importa registrar o pensamento de Barocas e Nissenbaum:

> Nós não estamos afirmando que inexista lugar para o consentimento e anonimização na proteção à privacidade. O consentimento e a anonimização não devem suportar, nem nunca deviam ter suportado, todo o fardo de proteger a privacidade. Reconhecer os seus limites nos permite melhor aferir onde e sob que condições eles possam cumprir as tarefas às quais sejam pertinentes. […] Essas mitigações procedimentais há tempos aliviam o encargo dos tomadores de decisão de julgarem a substantiva legitimidade de práticas informacionais específicas e as finalidades a que servem estas práticas. É tempo de reconhecer os limites das abordagens puramente procedimentais de proteção à privacidade.[11] (BAROCAS; NISSENBAUM, 2014, p. 33, tradução nossa)

Levando em conta as reiteradas renovações técnicas que levam à progressiva complexidade dos sistemas informacionais, garantir um ambiente de segurança para o usuário na forma da proteção de dados não é tarefa simples. Foram abordados anteriormente a dimensão econômica dos dados e o interesse do mercado em sua comercialização; os riscos ao desenvolvimento da personalidade do indivíduo, à sua privacidade e autonomia; e a posição do Estado como ente regulador na tentativa de conformar a atual situação dos dados pessoais com os preceitos constitucionais da proteção à dignidade humana sem impactar negativamente a implementação dos princípios da ordem econômica. Assim, é justo que se pense em soluções para a questão dos dados e da legitimidade do consentimento que tenham fundamento na atuação destes três sujeitos: o Estado, o mercado e o usuário.

Em primeiro lugar, introduzir-se-á o papel do mercado em zelar pelos direitos do usuário, na forma da condução da tecnologia. Em seguida, tratar-se-á da responsabilidade estatal sobre a matéria e do lugar da população nesse cenário.

4.1 Autorregulação: a tecnologia como recurso para a proteção da privacidade

Tendo sido estabelecido que as mais diversas manifestações da evolução tecnológica passaram desde muito cedo a apresentar potencial lesividade a direitos fundamentais, há de se buscar alternativas também na própria tecnologia para atenuar o caos

---

[11] "*We are not saying there is no role for consent and anonymity in privacy protection. Consent and anonymity should not bear, and should never have borne, the entire burden of protecting privacy. Recognizing their limits allows us to assess better where and under what conditions they may perform the work for which they are well suited. […] These procedural mitigations have long relieved decision-makers of the burden of rendering judgment on the substantive legitimacy of specific information practices and the ends that such practices serve. It is time to recognize the limits of purely procedural approaches to protecting privacy.*"

causado pelo fluxo informacional. Isto pois o que se tem verificado é justamente o oposto. Enquanto a tecnologia tem o potencial de adequar o aproveitamento do fluxo informacional em favor do elo mais fraco do mercado informacional – o usuário –, ela, sob a influência e controle do próprio mercado, dá condições à perpetuação da assimetria entre as partes, neutralizando a possibilidade de esclarecimento e autonomia dos indivíduos (BIONI, 2019). Dessa forma, a aptidão do mercado em operar visando à promoção da privacidade dos usuários está associada à gestão da tecnologia e o seu direcionamento.

Nesse sentido, mais do que oportunizar o vício de consentimento, o mundo das redes deve ter seus arquitetos redirecionando esforços a fim de garantir o esclarecimento do titular dos dados, o que verdadeiramente se faz possível dentro da liberdade de criação no universo digital. Assim, no lugar de ocupar-se com opções estéticas para tornar *websites* mais amigáveis, capazes de passar uma sensação de segurança e confiabilidade – com a disposição de botões coloridos e o planejamento das plataformas como um todo com o intuito de conduzir o usuário (e pretenso consumidor) ao aceite de seus termos –, é importante que sejam pensadas estratégias também no âmbito da apresentação das plataformas (o que também muito se relaciona com o seu *design*) aptas a revestir o consentimento fornecido pelo usuário não só de legalidade, mas também de legitimidade (RAVICHANDER et al., 2020).

> […] a ideia de que é ampla a prática de ignorar políticas de privacidade e termos de serviço infere uma considerável falha regulatória. Se é verdade que as pessoas usualmente ignoram as políticas ao aderir a formas de mídias digitais, sugere-se que a política de notificação [referindo-se ao *Notice and Choice*] não funciona, e talvez que o empenho contínuo voltado para a notificação esteja sendo desperdiçado[12]. (OBAR; OELDORF-HIRSCH, 2018, p. 5-6, tradução nossa)

Adentramos aqui o campo do "*privacy by design*", consistente na metodologia que define que a concepção de um produto ou serviço deve ser orientada pelo escopo da proteção de dados, havendo a incorporação de tecnologias que facilitem o controle e a proteção das informações pessoais (BIONI, 2019). A sistematização da tecnologia sob o princípio do *privacy by design* representa, em suma, a aplicação autorreflexiva da tecnologia, protegendo-a contra os riscos que ela mesma apresenta. Constatado o seu poder de lesão à privacidade, assim, é possível orientá-la a fim de que o padrão se torne a proteção do indivíduo, *in casu* na forma da proteção dos dados, utilizando-se de mecanismos que fomentem a independência do usuário em tomar as próprias decisões acerca de suas informações dispersas em rede.

---

[12] "[…] *the idea that the practice of ignoring privacy and TOS policies is widespread, points to considerable regulatory failure. If it is true that people typically ignore policies when engaging forms of digital media, it suggests that notice policy doesn't work, and perhaps that committed and continued resources devoted to notice efforts are being wasted*."

Essa orientação, é claro, necessita do empenho dos setores responsáveis pela programação de tais plataformas, agentes também inseridos no contexto do mercado de dados. Sobre a questão, Lokke Moerel destaca a impressionante resiliência do setor empresarial ao deparar-se com obstáculos legais acerca da proteção de dados pessoais em países que possuem regulamentos mais rígidos, como os da União Europeia, em contraponto ao tratamento dispensado pelos Estados Unidos da América à matéria. Em situações como esta, a existência de um interesse superior – condicionado ou não por normas jurídicas – conduziria ao empenho a fim de exitosamente implantar tecnologias sob o princípio *privacy by design*, adequando-as à noção da primazia da proteção do indivíduo e apresentando inovações criativas para o atingimento do objetivo (RAVICHANDER et al., 2020).

Afirma Moerel que, diante da viabilidade concreta de adaptação, contentar-se com a obtenção do consentimento passa a ser o caminho mais fácil. Segundo a especialista, o esforço dispensado na busca do consentimento formalmente considerado (obtido não raro mediante sugestão do programador, na forma das cores usadas e da apresentação do produto ou serviço) poderia ser redirecionado em primeiro lugar, e desde o início, às práticas de segurança de dados embutidas no produto ou serviço (RAVICHANDER et al., 2020).

Segundo Magrani e Oliveira (2019), a proteção *by design* não pressupõe um modo de execução fixo. Em face do modelo de contrato telemático – um contrato de adesão por excelência – fala-se na adaptação de alguns aspectos do *Notice and Choice,* com a inclusão de mecanismos que possam fortalecer o consentimento fornecido pelo usuário. Alguns exemplos seriam: a exigência de descer a barra de rolagem até o fim dos termos para poder finalizar a adesão; insistir no formato de granulação dos termos, com destaque a um resumo das principais cláusulas do termo num formato simplificado (uma tabela, por exemplo); a programação de *pop-ups* a fim de alertar de forma imprevisível o consumidor sobre cláusulas que possam fugir à sua expectativa ou demandem um consentimento qualificado; a solicitação do consentimento nas diversas fases específicas do tratamento de dados e não só a partir de um aceite inicial e genérico etc. (LIMA, 2014; 2019).

Infelizmente, como pode ser inferido do estudo realizado nos capítulos anteriores, muitas dessas medidas, na prática, se apoiam ainda na suposição de que os usuários de fato leem os termos e que o que falta é a sua efetiva compreensão, ou que os usuários os leriam caso fossem instigados o suficiente ou provocados da forma correta ou imprevista. Não há de se negar a importância da disposição de um provedor em facilitar o acesso à informação pelo usuário (e a hipótese não deve ser nunca descartada), porém já restou demonstrada a relação peculiar deste com a figura dos termos, encarados como pouco necessários e de pouca

repercussão prática ou reais consequências jurídicas. Nesse sentido, pode-se facilmente antecipar que qualquer caixa de alerta ou notificação insistente, elementos advindos de alguma prática do *privacy by design*, vá ser prontamente repelida antes de perfazer eficazmente qualquer objetivo de informação.

Para além disso, medidas como o rearranjo das informações (pelo menos das principais) em configurações como a de perguntas e respostas ou tabelas com o intuito de simplificar as disposições e facilitar a sua internalização pelo indivíduo para que ele realize uma escolha consciente, padecem de um erro honesto e fundamental: a simplificação. Temos aí o paradoxo da transparência (*transparency paradox*). Segundo este conceito, a transparência de significado do que resta consignado nos termos conflita com a transparência da realidade prática das atividades a serem realizadas a partir do consentimento. Explicando melhor, apesar de os termos e políticas com a escrita simplificada e a leitura dinamizada tornem-se mais acessíveis aos usuários, as nuances das informações ocultadas em prol desta descomplicação são determinantes para que seja comunicado o panorama real de procedimentos como o tratamento de dados e assim fundamentar a decisão do usuário (NISSENBAUM, 2011). É justamente este panorama completo, verdadeiramente apreendido, que determinaria o consentimento esclarecido e é a garantia desta apreensão o maior desafio enfrentado pelos estudiosos da matéria.

Não obstante, vale afirmar que a metodologia do *privacy by design* deve perpassar todo o modelo de negócio, desde a interface do produto ou serviço até os procedimentos de coleta, tratamento e transferência de dados (LIMA, 2019). A privacidade deve integrar, assim, as prioridades dos agentes econômicos, atravessando, de ponta a ponta, a estrutura do negócio, estando a preocupação presente em todas as etapas dos projetos desenvolvidos, inclusive contando com métodos de anonimização e criptografia sempre que possível (MARRAFON; COUTINHO, 2020). Dessa forma, a adoção de salvaguardas no tratamento de dados e na proteção da privacidade dos indivíduos, além de necessária, deve ser estimulada e até exigida, e todos os métodos eleitos para tanto, mesmo que não sejam individualmente infalíveis, não são dispensáveis.

Em paralelo à metodologia *privacy by design*, temos a *privacy by default*. Como constatado por Cass R. Sunstein (2015), o que se estabelece em qualquer sistema como configuração *default* molda a própria experiência do usuário. A palavra "*default*", vale apontar, pode ser traduzida como "padrão", é a forma com que o sistema, aparelho ou funcionalidade é programado inicialmente a se comportar caso o usuário não assuma uma posição ativa e altere suas configurações. A *privacy by default* determina que as configurações

mais seguras de privacidade devem ser adotadas como padrão, com a mínima coleta de dados pessoais necessária ao funcionamento da plataforma, sem que seja demandada ação do usuário nesse sentido e sem que as funcionalidades do serviço ou produto sejam prejudicadas ou limitadas por isso (MARRAFON; COUTINHO, 2020). Segundo Sunstein:

> A conclusão é que, em matéria de privacidade na Internet, muito se depende da regra do padrão. Caso um navegador de internet torne padrão configurações que protegem a privacidade, o resultado será muito diferente daquele em que os indivíduos necessitem selecioná-las a cada acesso. Considere, por exemplo, a recente estrutura de escolha do Google Chrome. As pessoas podem selecionar "navegação anônima", mas ela não constitui a configuração padrão, e os usuários não podem facilmente torná-la padrão; a tecnologia não o facilita. Usuários precisam escolher selecionar a "navegação anônima" a cada acesso. Como resultado, as pessoas navegam anonimamente muito menos.[13] (SUNSTEIN, 2015, p. 31, tradução nossa)

De acordo com o autor, o padrão no qual os sistemas são programados gera enorme repercussão prática. Isto se daria por algumas razões, como pelo desconhecimento do usuário de que é facultada a ele a opção de alterar uma ou outra funcionalidade. Justifica este desconhecimento, no entanto, o caminho não tão claro que deve ser feito dentro da plataforma para acessar certas ferramentas, vindo a ser uma faculdade de difícil concretização. Em outros casos, modificar o padrão pode trazer desvantagens ao usuário, como a negativa de acesso a recursos específicos (SUNSTEIN, 2015).

Assevera Sunstein (2015) que por mais trivial que seja a escolha – o que não costuma ser o caso no inerentemente complexo contexto da tecnologia –, o mero fato de ser demandada uma postura ativa do indivíduo já torna menos atrativa a opção pela alteração, importando em adiamento por ele ou desprezo e recusa. Tal quadro ainda é agravado se a pessoa está ocupada, se a questão é de difícil compreensão ou envolve aspectos técnicos, quando a decisão não é óbvia ou quando o indivíduo simplesmente não possui preferência (e para decidir precisaria formá-la). A exigência de qualquer esforço, assunção de riscos pela escolha ou simplesmente a impressão de estar se colocando em sentido contrário à implícita recomendação de programadores especializados, os quais, tende-se a supor, agiriam no melhor interesse da experiência do usuário (posição subconscientemente recorrente, mas não por isso verdadeira), concorrem para estabilização das configurações originais, em prol de programações potencialmente invasivas (SUNSTEIN, 2015).

---

[13] "*The upshot is that in the domain of privacy on the Internet, much depends on the default rule. If a web browser defaults people into privacy-protective settings, the outcomes will be very different from what they will be if people have to select privacy settings every time. Consider, for example, the recent choice architecture on Google Chrome. People are allowed to select "Incognito," but it is not the default, and users cannot easily make it into the default; the technology does not facilitate that. Users must choose to select "go Incognito" every time they log on. As a result, people go Incognito a lot less*."

Assim, sistemas que baseiam em modelos *opt-out*[14] as escolhas do usuário a respeito de medidas de proteção à privacidade*,* na prática, fazem pouco para garantir ao usuário controle sobre seus dados. Adotado o sistema *opt-in*, no qual o usuário deve ativamente regular o fluxo de suas informação, decidindo que dados poderão ser tratados e para que finalidade, o quadro é revertido e o indivíduo recobra o controle, a sua autodeterminação informativa, e pode melhor fornecer o seu consentimento de forma específica. Além disso, sendo do interesse dos agentes do mercado que haja o compartilhamento de informação, o seu esforço será redobrado no sentido de facilitar a escolha, informar o usuário e garantir a continuidade desta relação de confiança a partir da diligência no cumprimento das normas legais e recomendações de entidades reguladoras, sendo contemplada neste processo a questão da minimização da vulnerabilidade do usuário ante o mercado (SOLOVE, 2004).

A situação de urgência em assegurar uma regulamentação na matéria é endossada, pois, mormente em se tratando do Brasil, não se pode dizer que haja uma cultura de proteção de dados. Num contexto como esse, a integração de práticas relacionadas à metodologia *privacy by design* e, por decorrência, *privacy by default* é ainda mais estimada, principalmente após analisada a influência das configurações padrão – que simbolizam a forma na qual os desenvolvedores da respectiva plataforma esperam que ela seja utilizada – e o seu potencial na efetivação da segurança do usuário ao utilizar as tecnologias cibernéticas.

Notam Marrafon e Coutinho (2020) que a LGPD sutilmente se posiciona em favor destas medidas eminentemente preventivas, no art. 6º, inciso VIII ("prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais"), e art. 46, § 2º ("As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução") (BRASIL, 2018). Fortuita também é a disposição do art. 55-J, VIII, da LGPD, que estabelece como competência da Autoridade Nacional de Proteção de Dados o estímulo à "adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais" (BRASIL, 2018).

O reconhecimento da LGPD quanto à importância do emprego da tecnorregulação – ou autorregulação do mercado por intermédio da tecnologia – manifestado nos citados

---

[14] O modelo *opt-out* faz com que o usuário necessite autonomamente desselecionar na plataforma eletrônica opções que fazem parte da sua configuração padrão, entre elas as que fazem com que dados sejam compartilhados. Caso não o faça, prevalecerá a configuração padrão e os dados serão compartilhados. Em oposição, a utilização do modelo *opt-in* na proteção à privacidade condiciona as atividades de tratamento de dados à concordância e seleção ativa do usuário.

dispositivos demonstra a importância da cooperação entre as atividades estatais e a regulamentação interna dos agentes econômicos. Ratifica-se, assim, que a proteção de dados deve vir como esforço comum, devendo ser destacado que qualquer desequilíbrio pode ser nocivo, a depender, ao desenvolvimento da tecnologia, às inovações e ao mercado, ou à sociedade, principalmente à autonomia e à privacidade desta. No lugar de antagonizar em absoluto o mercado e o Estado, em repúdio a qualquer imposição legal às atividades econômicas, importa que se alcance um ajuste ou entendimento equilibrado em prol dos direitos fundamentais da população, dotada das condições de cidadã e de consumidora.

É importante ressaltar que a busca pelo fortalecimento da privacidade não deve ser associada ao fim do mercado de dados. A problemática existente gira em torno da falta de legitimidade das transações e utilizações arbitrárias envolvendo estes dados, sem que o usuário tenha uma voz efetiva e consciente em qualquer das etapas do processo e ainda suporte as consequências da terceirização do seu controle e de sua pseudoautonomia. A receita advinda, em geral de forma indireta, da coleta dos dados consiste em relevante montante e, por isso mesmo, passa a adjetivar a economia como eminentemente informacional. Porém, alterações de caráter restritivo na base da cadeia desta economia, como algumas das propostas, apesar de apresentarem implicações sensíveis, não inviabilizam a utilização de dados para a otimização de produtos e serviços ou para o direcionamento de propaganda.

Segundo Moerel (2021), pesquisas apontam no sentido de que, quanto mais controle é dado aos indivíduos sobre suas informações, mais eles estarão dispostos a prover informações, corrigi-las e suplementá-las. Este seria o paradoxo do controle (*control paradox*), baseado na formação da relação de confiança do usuário com o agente no tratamento de seus dados.

Em sentido complementar a esta peculiaridade cognitiva, estudos apontam que a própria utilização do termo "*privacy policy*" (política de privacidade) nas plataformas digitais é capaz de equivocadamente assegurar aos usuários a existência de um patamar razoável relativo à proteção de dados (como um selo de qualidade), com uma maioria de participantes adultos sujeitos à pesquisa afirmando acreditar que a mera presença desta política desautorizaria o compartilhamento de dados com terceiros, além de garantir automaticamente uma série de direitos, como o direito à reparação de danos, de ser informado no caso de vazamentos, de assistência na eventualidade de ocorrência de roubo de identidade etc. (HOOFNAGLE; KING, 2008).

Esta perspectiva indica um nível de disposição – ainda que ingênua – do usuário a confiar nas plataformas digitais que acessa. No contexto de permanente abuso na utilização de

dados pessoais, tal confiança figura como conveniente aos agentes de tratamento. Não obstante, o quadro pode ser redirecionado. A confiança do usuário, associada ao paradoxo do controle, indica que haja de fato pertinência na regulamentação do mercado de dados, não consistindo obrigatoriamente a heterorregulação pelo Estado em óbice à inovação tecnológica ou à rentabilidade dos negócios digitais. Ainda, com o fortalecimento do consentimento (e a desmistificação de ideias tais quais a da existência da política de privacidade como selo de qualidade de tratamento de dados) torna-se possível vislumbrar um aumento na qualidade do direito à autodeterminação do indivíduo e na garantia de direitos fundamentais deste.

Como visto, figura a colaboração da tecnologia como indispensável à proteção da privacidade. No entanto, dados os interesses conflitantes entre mercado e sociedade, faz-se necessária uma intermediação entre as duas partes que garanta alguma harmonia nessa relação. A busca desta harmonia cabe ao Estado como parte terceira interventora. A sessão seguinte tratará dessa questão ao abordar a heterorregulação: a regulação da tecnologia e do mercado pelos entes estatais.

4.2 Heterorregulação: o Estado e a efetivação do direito à privacidade na sociedade da informação

A autorregulação da tecnologia é essencial para que seja elevado na sociedade o patamar de privacidade e proteção de dados. Entretanto, a despeito das inúmeras vantagens apresentadas pela inovação tecnológica e a velocidade com que novos mecanismos são criados e precisam ser contemplados pelo direito, estas não são justificativas para que agentes econômicos se evadam da regulação estatal. De outra forma, o recuo do direito em prol da regulação pela tecnologia seria culpado por colocar direitos individuais nas mãos de grandes agentes empresariais, sem transparência, sem meios eficazes de responsabilização ou filtro democrático. Assim, objetiva-se encontrar um formato regulatório que possibilite o estímulo à inovação e que ainda garanta os devidos direitos aos usuários dentro dos preceitos constitucionais, traçando parâmetros a partir dos quais aqueles agentes possam desenvolver suas atividades com rentabilidade e até exercer sua competência autorregulatória (FRAZÃO, 2018).

Para tanto, deve-se pensar no lugar do Estado como detentor da prerrogativa maior de normatização. Esta função, no caso em estudo, é exercida principalmente por meio da atividade legislativa, mais objetivamente, pela Constituição e normas infraconstitucionais. Nesse quadro, a Autoridade Nacional de Proteção de Dados (ANPD) – de criação muito

recente e que, por essa razão, ainda se encontra em processo de estruturação interna – terá papel fundamental no direcionamento das políticas públicas em matéria de dados no País, assim como no fornecimento de balizas para a interpretação da LGPD, e na fiscalização de agentes do mercado e do governo quanto ao cumprimento das normas.

Reconhecendo-se o quão recentes são tanto a Lei Geral de Proteção de Dados Pessoais quanto a Autoridade Nacional de Proteção de Dados, e apesar dos claros posicionamentos no sentido valorativo e procedimental trazidos com a promulgação da lei e consequente organização do modelo de abordagem à questão dos dados e da privacidade que antes restava fragmentado em legislações setoriais, verifica-se que o País se encontra, presentemente, em um contexto de interessante liberdade de regulamentação da matéria. Em função das prerrogativas concedidas à ANPD e de procedimentos da LGPD pendentes de serem estabelecidos pelo órgão, a atuação deste e o posicionamento que irá tomar ante as práticas do mercado e do governo será determinante para a consecução dos objetivos da lei.

Apoiado na oportunidade de amplo regramento e na possibilidade de definição de novos parâmetros para o tratamento de dados e utilização das plataformas digitais (cujos controladores apresentam condutas que não raro se distanciam das máximas constitucionais), abordaremos as concepções de Sloan e Warner, e a de Nissenbaum acerca do processo de elaboração de um sistema de normas atinente à proteção de dados que seja ao mesmo tempo eficiente e em conformidade com as expectativas de privacidade dos indivíduos, em contraste com o que se tem hoje com as práticas que sustentam a primazia da coleta do consentimento, nem sempre legítimo, refletidas no modelo *Notice and Choice*, a política de notificação.

Sobre a política de notificação, afirmam Sloan e Warner (2014a, p. 28, tradução nossa): "Nós não vemos qualquer maneira aceitável de resgatar o *Notice and Choice*"[15]. Em sentido semelhante coloca-se Nissenbaum (2011) ao afirmar que, independente do quão refinado for o sistema *Notice and Choice*, ele dificilmente resultará em aprimoramento da privacidade nas redes enquanto se mantiver alheio às particularidades da navegação (na internet) e às suas próprias limitações, já expostas neste trabalho. Segundo a autora, o modelo apresenta uma falha intrínseca: a presunção de que os indivíduos são capazes de compreender todos os fatos relevantes à sua escolha durante o ato da contratação pelo meio digital.

Apesar de enxergar como insuficientes as opções que importam em meras modificações no modelo em vigor, centradas na própria tecnologia, admite Nissenbaum (2011) que podem ser a melhor abordagem de transição enquanto uma alternativa de

---

15 "*We see no acceptable way to rescue Notice and Choice.*"

fortalecimento da privacidade não é desenvolvida. Na forma desta alternativa, sugere a autora o que chama de "normas informacionais" ("*informational norms*"). Em suma, essas normas seriam responsáveis por delimitar que tipo de informação pode ser revelada ou coletada em um determinado contexto, sendo este digital ou não (NISSENBAUM, 2010; 2011).

Ressalte-se que, nessa teoria, o sentido de norma ultrapassa quesitos como a formalização ou sanção, podendo compreender aquelas normas implicitamente aceitas, as explicitamente formuladas e sancionadas por autoridades e instituições, e até as impostas em sistemas jurídicos. Em geral, elas prescrevem, num dado contexto, os tipos de informação – condições de saúde, notas escolares, segredos íntimos, inserindo-se aqui também outras categorias de dados pessoais estudadas previamente –, os sujeitos envolvidos (quem transmite a informação, quem a recepciona e sobre quem ela trata) e os princípios sob os quais as informações são transmitidas (que determinam, entre outras coisas, se a informação deve ser repassada voluntariamente, consensualmente ou de forma mandatória) (NISSENBAUM, 2010).

Deve ser entendido, ainda, por "contexto" a representação abstrata de uma configuração social estruturada – ou esfera social individualizada – vivenciada no cotidiano, com características que evoluíram com o tempo, compreendendo papéis, relações, estruturas de poder, normas ou regras, e valores internos (objetivos, fins, propósitos). São exemplos os contextos de educação, do ambiente de trabalho, o religioso, familiar, médico, comercial etc. Nesse sentido, as normas informacionais definem também obrigações, prerrogativas e privilégios associados a papéis específicos assumidos em um contexto, bem como orientam valorativamente comportamentos como aceitáveis ou inaceitáveis (NISSENBAUM, 2010).

No que diz respeito às normas informacionais de contexto específico, explica Nissenbaum:

> Em um contexto de assistência médica, por exemplo, pacientes esperam que seus médicos mantenham informações pessoais relativas à saúde como confidenciais, ainda que aceitem a possibilidade de serem elas compartilhadas com especialistas quando necessário. A expectativa dos pacientes seria violada e estes provavelmente restariam surpresos e consternados caso descobrissem que seus médicos teriam vendido as informações para uma agência de marketing. Nessa situação, dir-se-ia que as normas informacionais para o contexto de assistência médica teriam sido violadas.[16] (NISSENBAUM, 2011, p. 33, tradução nossa)

[16] "*In a health care context, for example, patients expect their physicians to keep personal medical information confidential, yet they accept that it might be shared with specialists as needed. Patients' expectations would be breached and they would likely be shocked and dismayed if they learned that their physicians had sold the information to a marketing company. In this event, we would say that informational norms for the health care context had been violated.*"

Na elaboração da sua argumentação aplicada ao contexto da internet, apoia-se a autora – por meio da sua teoria da "integridade contextual" ("*contextual integrity*") – em microssistemas de normas informacionais (também contextualizados) que no decorrer do tempo tiveram a oportunidade de amadurecer e evoluir, agregando, internalizando e aperfeiçoando questões tais quais o legítimo interesse, a moral, princípios políticos e os propósitos e valores, todos próprios e específicos aos contextos a que se direcionam (NISSENBAUM, 2011).

Para tanto, defende Helen Nissenbaum a conexão e o paralelismo entre as atividades que ocorrem nos meios digitais e as estruturas previamente existentes da vida social, rejeitando a noção de que a construção de um sistema de proteção à privacidade na internet deve ser tida como uma iniciativa de todo apartada daquela empregada à sua proteção no cotidiano fora das redes. O reconhecimento dessa correspondência possibilitaria o estabelecimento de referências e pontos de partida para uma regulamentação mais adequada, alinhada às expectativas sociais já existentes e compatíveis com as instituições análogas em propósito e em função àquelas da rede. Segundo a autora, as operações em rede, em sua maioria, seriam transposições de relações do mundo físico. Por essa razão, reafirma a falta de adequação do modelo *Notice and Choice*, visto que, em se tratando de privacidade, a internet não seria um "território virgem" para que sujeitos pudessem conceber regulamentações próprias a cada transação. (NISSENBAUM, 2011).

Nesse sentido, normas informacionais específicas a um contexto poderiam ser estendidas às correspondentes atividades digitais. Não havendo uma referência contextual anterior em que se embasar, Nissenbaum concebe, por meio da sua teoria, que os parâmetros das normas informacionais sejam traçados a partir da moral humanística e as tradições políticas das democracias liberais contemporâneas. A abordagem da integridade contextual, de derivação heurística, segundo a autora, "[…] sugere que identifiquemos contextos, examinemos as arraigadas normas informacionais, apuremos os fluxos desviantes, e avaliemos estes fluxos sob a luz da ética geral e princípios políticos, além dos propósitos e valores específicos aos contextos"[17] (NISSENBAUM, 2011, p. 38, tradução nossa).

Consoante sua obra, o desafio da proteção à privacidade na contemporaneidade não decorre de qualquer caráter distintivo das plataformas cibernéticas em si, mas do descontrole do fluxo de informação gerado a partir da captura, análise e disseminação em

---

[17] "[...] *suggests that we locate contexts, explicate entrenched informational norms, identify disruptive flows, and evaluate these flows against norms based on general ethical and political principles as well as context specific purposes and values*."

grande escala dos dados nas redes, que agem como mediadoras na utilização das novas tecnologias (NISSENBAUM, 2011). Declara ainda Nissenbaum que "o que mais importa para as pessoas não é simplesmente **restringir** o fluxo de informação, mas garantir que ele flua **apropriadamente**, e um direcionamento para este fluxo apropriado é dado aqui por meio do enquadramento da integridade contextual"[18] (NISSENBAUM, 2010, p. 2, tradução nossa, grifos da autora), um adendo relevante ao conceito proposto por Westin de privacidade como liberdade positiva.

Em harmonia com o pensamento de Nissenbaum, Sloan e Warner (2014a) defendem a competência das normas informacionais para os fins de proteção à privacidade desde que elas atinjam o patamar de "normas de valor ótimo" ("*value-optimal norms*"), afirmando que a partir desse ponto poder-se-ia considerar o consentimento fornecido pelos usuários nas redes como livres e esclarecidos. Para os autores, uma norma alcançaria o valor ótimo quando, à luz dos valores de membros do grupo ao qual governam, haja conformação de todos, idealmente, ou quase todos estes membros, sendo a norma a melhor justificável dentre as alternativas (ou tanto quanto aquelas melhores). Em suma, será ótima a norma desde que não haja alternativa de norma mais benéfica, análise feita a partir dos valores da sociedade.

Sloan e Warner (2014a) associam à ideia de valor ótimo da norma a noção do ideal de completude normativa ("*norm completeness*"), alcançada, segundo os autores, quando não houver atividade que sopese privacidade e objetivos conflitantes (em geral, os interesses do mercado) sobre a qual não incida ao menos uma norma informacional de valor ótimo. Afirmam eles que a prática relativa às operações tradicionais – isto é, fora das redes – adquiriu ao longo dos séculos um caráter próximo da completude normativa, dando origem a relevantes normas de valor ótimo, após consolidarem-se nas sociedades de forma mais ou menos homogênea e amplamente regulada. Pense-se nas operações de compra e venda, por exemplo, que possuem vasto regramento em diversos atos normativos que abarcam, em geral, todas as suas peculiaridades e imprevistos. Em contraste, o rápido avanço das tecnologias e as constantes inovações não seriam favoráveis ao atingimento desta completude normativa no que diz respeito às relações no meio digital, visto que ultrapassam em velocidade as atividades regulamentadoras e o próprio movimento de absorção e adequação da sociedade, gerando situações para as quais faltam normas informacionais de valor ótimo.

---

[18] "*What people care most about is not simply **restricting** the flow of information but ensuring that it flows **appropriately**, and an account of appropriate flow is given here through the framework of contextual integrity*."

Por outro lado, ressaltam Sloan e Warner (2014b) que a medida certa entre o resguardo da privacidade e os interesses contrapostos a ele não está simplesmente oculta entre valores existentes em uma sociedade, aguardando ser trazida à luz; ela precisa ser concebida. Asseveram que os valores de uma sociedade não compõem um sistema consistente, sólido, mas sim um esboço capaz de embasar inclusive posições e visões opostas, ao mesmo tempo que deixam de contemplar suficientemente muitas áreas. Por essa razão, também, constatam que a agilidade da inovação tecnológica seria um entrave para a criação das referidas normas regulamentadoras, em função de não oportunizar (em tempo hábil) a consolidação de valores.

Apesar de autônomas, pode ser evidenciado um elo entre a abordagem dos autores e a de Helen Nissenbaum na teoria desta sobre a integridade contextual, que fomenta a verificação da identidade entre situações do mundo real e do mundo virtual para os fins da regulamentação. Nesse sentido, seria possível a aplicação da bagagem de experiência normativa produzida em séculos de história – a saber, nas transações de produtos e prestações de serviços – na concepção de uma regulamentação (ou, mais apropriadamente, várias) para a privacidade na internet, notadamente para ajustar o fluxo disruptivo de dados pessoais. "Essa visão da privacidade online também implica que contextos, não a economia política, devem determinar restrições ao fluxo de informação"[19] (NISSENBAUM, 2011, p. 43, tradução nossa).

Com a utilização de normas informacionais já existentes como parâmetro, esta regulamentação do meio digital, então, já seria concebida em um estágio próximo do que se teria por uma norma informacional de valor ótimo da doutrina de Sloan e Warner, em função da consonância com as expectativas sociais em contextos específicos análogos. Nesse seguimento, é relevante entender também, segundo Frazão (2018), a medida em que a tecnologia pode por vezes mudar a essência dos serviços ofertados, não sendo inviabilizado, porém, uma comparação com o propósito de adaptação das realidades.

Assim sendo, as normas informacionais de contexto específico, adquirindo o caráter de normas de valor ótimo dentro de um sistema em que haja completude normativa (cobertura ampla do máximo de possibilidades dentro daquele contexto, abarcando peculiaridades, imprevistos, exceções etc.), assegurariam manifestações de consentimento livre e informado. Isto se daria, pois, dada a conformação da regulamentação com os valores da sociedade (segundo a própria noção de valor ótimo), o sopesamento entre a privacidade e

---

[19] "*This view of online privacy also implies that contexts, not political economy, should determine constraints on the flow of information*."

os interesses de mercado restaria aperfeiçoado de uma forma em que as expectativas do usuário como membro da sociedade e pessoa humana detentora de direitos fundamentais seriam atendidas dentro do contexto em que se opera a relação e, por consequência, o fluxo de informação.

Note-se que a ideia confronta aquela que pressupõe a capacidade e responsabilidade única do titular de zelar por seus dados. Na existência de um sistema que ampara suas decisões, limitando paternalisticamente o próprio arbítrio do indivíduo em prol de seus direitos fundamentais, garante-se uma margem de segurança dentro da qual tanto os usuários quanto os agentes de mercado podem transacionar, adotando mais ou menos restrições ao fluxo de dados. Definindo-se o mais concretamente possível este espaço para negociação, com o mapeamento das possíveis repercussões e quais delas seriam adequadas ou inadequadas ao referente contexto, dá-se maior precisão à atividade de fiscalização e efetivação das normas, viabilizando o sistema regulatório.

As análises dos autores articuladas até aqui apresentam-se eminentemente no plano retórico, com propostas teóricas com o fito de alcançar o ideal de regulação sistêmica da ingerência da tecnologia na sociedade. Sob o ponto de vista da dimensão prática, as posições dos autores são ambiciosas e muitas vezes pressupõem uma coordenação singular entre Estado, sociedade e mercado, bem como o nivelamento na complexidade de valores e expectativas dentro da sociedade, e a correspondência preponderante de contextos da vida dentro e fora das redes que possibilite a analogia adequada para a elaboração de normas informacionais.

Apesar disso, diante da carência de regulação, essas perspectivas funcionam precisamente como contraponto à realidade e inferem caminhos alternativos que podem ser explorados, verificados (ou rejeitados) e adaptados ante os obstáculos e conflitos com que venham a se deparar. As teorias contribuem, uma vez que provocam o pensamento sobre situações em que o consentimento está presente e tentam dissecar os elementos que o configuram, como valores, costumes, expectativas, normas implícitas, a fim de replicar o processo com foco no mundo digital.

Dito isto, para que uma situação ideal como essa comece a tomar forma de maneira orgânica, sugerem Sloan e Warner (2014b) que haja pressão por parte dos usuários para que os responsáveis pela coleta de dados adaptem as suas políticas de privacidade a fim de buscar maior proteção aos dados pessoais do indivíduo, preservando a integridade de sua personalidade. Esta pressão se operaria por meio de tecnologias – efetivas, acessíveis,

transparentes em seus efeitos e de ampla adesão dos usuários –, aptas a, da forma quase perfeita[20], bloquear o fluxo de dados aos agentes coletores.

O consequente declínio sensível dos dados apurados pelas plataformas interferiria na renda auferida com o mercado de dados, e isto obrigaria, caso tomasse dimensão tão relevante quanto esperada pelos autores, uma reestruturação das políticas internas de tratamento de dados pessoais, visando a uma conformação às expectativas dos usuários insubmissos (uma maioria). Em outras palavras, a iniciativa dos usuários de, autonomamente, buscar ferramentas capazes de protegê-los da imiscuição na sua privacidade por parte dos agentes de tratamento teria impacto econômico direto, reforçando a expressiva inquietação da sociedade com as práticas do mercado. Como resultado, ter-se-ia um pacto forçado de adesão à proteção da privacidade, com a busca de adequação suficiente às demandas populares para que se viabilizasse a rentabilidade do negócio sem a necessidade de abrir mão do compromisso com os direitos dos seus usuários. Com o tempo, segundo os autores, a nova dinâmica entre as partes não seria simplesmente aceita, mas se tornaria aceitável, incorporando-se enfim a proteção à privacidade e aos dados pessoais nas práticas da rede (SLOAN; WARNER, 2014b).

É de se notar que, enquanto Nissenbaum, como apresentado, sustenta sua proposta teórica em uma definição abrangente de norma – que engloba tanto aquelas implícitas, quanto explícitas, emanadas ou não por autoridade ou governo, acompanhadas ou não de sanção por descumprimento –, Sloan e Warner dirigem seus esforços para a garantia de uma norma eminentemente social e informal. Em sua obra, utilizam a definição de norma como a regularidade comportamental em um grupo – com origem em acordos, costumes ou leis – que causa um sentimento comum de dever (como obrigação moral). Exemplificam os autores: o compromisso fomentado por uma lei proibitiva de que não se deve permitir que o amigo dirija após ingerir bebida alcoólica, sendo de reiterada conformidade em um grupo, também gera uma responsabilidade comunitária e "senso comum" de que, mesmo que lei não houvesse, tal comportamento de amigo "responsável" continuaria a ser o mais adequado (SLOAN; WARNER, 2014b).

Apesar de Nissenbaum aceitar a possibilidade de se ter uma norma de caráter jurídico como norma informacional de contexto específico, segundo Sloan e Warner, para além da atuação estatal, a norma (para ser tida como tal) deverá corresponder a um

---

[20] Note que há ainda embasamento no ideal mesmo em propostas que pretendem ter um maior nível de pragmatismo.

compromisso mais profundo, que, no caso em tela, dadas as suas complexidades, não poderá será promovido a partir de simples heterorregulação. Em uma situação como essa, afirma a dupla que, sem a ameaça por parte do Estado de responsabilizar os negócios não aderentes às práticas conforme regulamentadas, não haverá o regular cumprimento, esvaziando os propósitos da regulamentação. Não se deveria, assim, depender de constrangimento legal, fiscalização e sancionamento, por serem métodos dispendiosos, dificultosos e incertos, diferentemente do cumprimento voluntário, uma expressão efetiva da "norma" (regularidade comportamental generalizada), como entendida pelos autores (SLOAN; WARNER, 2014b).

Uma solução para essa questão – o que não é surpresa – é justamente a conscientização da sociedade, capaz de gerar o que Sloan e Warner (2014b) tratam como "compromisso com a privacidade" ("*commitment to privacy*"). Em suas palavras: "Sem um compromisso com a privacidade, nossas estratégias de geração de normas funcionam somente quando a estratégia de maximizar o lucro de um negócio consiste na conformação com a norma criada por meio de um estatuto de boas práticas; de outra forma, o negócio […] irá dissentir"[21] (SLOAN; WARNER, 2014b, p. 334, tradução nossa).

No pensamento dos autores, esses esforços em conscientização seriam capazes inclusive de convencer os agentes por trás das tomadas de decisão no mercado a internalizar a responsabilidade quanto ao respeito à privacidade (fortalecendo, por exemplo, movimentos como o do *privacy by design*), a despeito dos custos deste substancial ajuste, orientando-os a uma prática que, aperfeiçoada com o tempo, pode dar origem a uma norma de valor ótimo e em consonância com a expectativa social, moldada também em função da promoção de iniciativas educacionais para a população.

Quanto a estratégias para a realização desse processo educacional e conscientizador, é sugerida a edição de normas que tornem mandatória aos respectivos agentes de tratamento a prestação de contas quanto às suas práticas de processamento de dados, em relatórios periódicos e de amplo acesso à população endereçados ao órgão governamental responsável pela proteção de dados pessoais, no Brasil, a Autoridade Nacional de Proteção de Dados (ANPD). Tais relatórios seriam de maior serventia à imprensa e a grupos ou organizações de defesa à privacidade e dados pessoais, que, aí sim, poderiam publicizar as informações de forma efetiva a fim de fazê-las chegar à população (SLOAN; WARNER, 2014b). Ressalte-se que a hipótese está completamente de acordo com o

---

[21] "*Without a commitment to privacy, our norm-generation strategies work only when a business's profit-maximizing strategy is to conform to the norm created through a best practices statutes; otherwise, the business […] will defect*."

consignado no art. 55-J, inciso X, da LGPD, que dispõe sobre as competências da ANPD, segundo o qual cabe a esta "dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial" (BRASIL, 2018).

Consoante mesmo rol de competências, temos que cabe à ANPD a promoção do conhecimento pela população das normas e políticas públicas sobre proteção de dados pessoais e medidas de segurança (art. 55-J, VI), além de ser responsabilidade do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – componente da ANPD – a disseminação à população de conhecimento sobre a proteção de dados pessoais e sobre privacidade (art. 58-B, V) (BRASIL, 2018).

No que disserta Parentoni (2019), a ANPD guarda semelhanças estruturais e funcionais com a correspondente autoridade uruguaia, a *Unidad Reguladora y de Control de Datos Personales* (URCDP), em funcionamento há pouco mais de uma década. Registre-se que o Uruguai possui lei específica para a proteção de dados pessoais desde 2004, e desde 2008 possui uma lei geral sobre a matéria, estando ao menos dez anos à frente do Brasil no quesito de regulamentação (PARENTONI, 2019). Ainda, o Uruguai é o único Estado sul-americano integrante do Digital Nations, grupo de dez países[22] que se autodeclaram estar à frente em matéria de governança digital (DIGITAL NATIONS, c2020). Ao espelho da experiência uruguaia com a própria autoridade de proteção de dados, a atuação da Autoridade Nacional de Proteção de Dados no Brasil possui grande potencial de impacto na instrução da população sobre os temas que justificaram a sua criação.

Assim sendo, em cumprimento as suas funções estabelecidas por lei, deve a ANPD ter como uma das suas bases justamente a instrução da sociedade sobre as problemáticas envolvendo dados pessoais e direitos correlatos. Para tanto, mais do que pertinente que sejam realizados eventos de conscientização e workshops com segmentos diversos da população, de faixas etárias variadas, professores de escolas, profissionais da área da tecnologia e relacionadas, servidores públicos, etc. com foco nas práticas de coleta de dados, iniciativas do mercado para fortalecer a proteção da privacidade, e ferramentas e técnicas a serem utilizadas para salvaguarda individual. Tal como foi empreendido pela URCDP, cabe também a expansão da acessibilidade a esses eventos, com a realização de

---

[22] São estes: Estônia, Israel, Coreia do Sul, Nova Zelândia, Reino Unido, Canadá, Uruguai, México, Portugal e Dinamarca.

cursos on-line pelo portal da ANPD na internet, eventos acadêmicos, incluindo a participação de especialistas nacionais e estrangeiros (PARENTONI, 2019).

Outra referência de atuação são os Estados Unidos da América, que contam com a *Federal Trade Commission* (FTC), agência federal com a missão de "proteger os consumidores e a concorrência"[23] (UNITED STATES OF AMERICA, 2021a), e também acumula a função de proteção de dados pessoais. Em sua página da internet é possível, além de fazer denúncias de roubo de identidade, fraudes e golpes (UNITED STATES OF AMERICA, 2021a), visualizar e solicitar gratuitamente, e em grande número, cartilhas sobre privacidade, proteção de dados pessoais e medidas de segurança nas redes. Da mesma forma, anualmente são realizadas convenções (ao exemplo da PrivacyCon) que reúnem acadêmicos, pesquisadores, representantes do mercado e do governo para discutir sobre estes temas (UNITED STATES OF AMERICA, 2021b).

Vê-se que a ANPD, apresenta papel capital na condução a melhores práticas de proteção à privacidade e proteção de dados nas esferas da sociedade, do mercado e do próprio governo[24]. O amplo alcance de suas competências – que lhe concedem funções de orientação, elaboração de pesquisas, estudos e relatórios, edição de normas e diretrizes, realização de auditorias, aplicação de sanções etc. –, assim como as experiências de outros países, antecipam o seu potencial de atuação e de sucesso na consecução dos objetivos regulamentadores a que se propõe.

Nesse sentido, ao enfrentar desafios como o fluxo informacional desenfreado nas redes, a objetificação de componentes da personalidade do indivíduo pelo mercado, e a ignorância dos indivíduos na administração de seus dados pessoais, pede-se uma regulamentação ampla, efetiva e supervisionada, aliada aos esforços educativos direcionados à sociedade e ao mercado. Estes esforços educativos na forma de políticas públicas devem ressaltar a existência e a importância dos direitos constitucionais à privacidade e intimidade, abarcando inclusive alertas sobre golpes, fraudes, crimes informáticos e exposição indevida na internet (PARCHEN; FREITAS, 2016). No que declaram Sloan e Warner, "a despeito de

---

[23] "*Protecting consumers and competition*."

[24] Discute-se se a organização – ainda passível de modificação – da Autoridade Nacional de Proteção de Dados como órgão público inserido formalmente na estrutura da Presidência da República não teria impacto na sua independência técnica, funcional e decisória, principalmente em matéria de fiscalização da própria Administração. Conclusões sobre esta questão hão de ser diligentemente postergadas para momento em que a atuação da ANPD esteja melhor consolidada. (BRASIL, 2018; PARENTONI, 2019)

possíveis entraves no caminho, a sociedade necessita que o compromisso com a privacidade esteja em primeiro lugar"[25] (SLOAN; WARNER, 2014b, p. 334, tradução nossa).

Dessa forma, ainda que sejam garantidos inúmeros direitos aos titulares de dados, é necessário que políticas referentes a tratamentos de dados pessoais tornem-se relevantes ao olhar público de forma que haja pressão para além da ocasionada pela fiscalização governamental, que seja advinda dos próprios titulares dos dados, esclarecidos de sua posição e das operações e transações realizadas ao custo de seus direitos mais íntimos. Tal transição no olhar sobre o direito à autodeterminação informativa, que suplantaria a passividade dos sujeitos, colaboraria com o objetivo da norma de conferir ampla proteção ao cidadão no que diz respeito à proteção de seus dados pessoais, ao passo que tem repercussão na forma com que agentes de tratamento de dados elaboram os seus termos e manejam informações.

Esta é inclusive a posição do atual presidente da Autoridade Nacional de Proteção de Dados, Waldemar Gonçalves Ortunho Júnior. Afirma ele que o principal objetivo nos primeiros anos de atuação da ANPD será a promoção de uma mudança de cultura relativa aos dados pessoais no Brasil, no que diz respeito à posição do titular dos dados e também das empresas. Miriam Wimmer, diretora do Conselho Diretor da ANPD, declara que a Autoridade pretende ser tão transparente e aberta quanto possível, utilizando-se de instrumentos formais, como o Conselho Nacional de Proteção de Dados, e informais, como workshops, grupos de trabalho e reuniões (ORTUNHO JÚNIOR; WIMMER, 2021). Ressalte-se que a edição de qualquer ato normativo pelo órgão deve ser precedida de consulta pública, audiência pública e análise de impacto regulatório, conforme art. 55-J, § 2º, da LGPD (BRASIL, 2018), o que de fato é capaz de oportunizar esta experiência participativa proposta.

Além dos investimentos em políticas públicas com a finalidade de educação da sociedade e dos agentes empresariais, a estratégia regulatória pode combinar medidas de incentivo a comportamentos desejáveis, trazendo um diferente estímulo para a conformação com as diretrizes propostas que não seja a ameaça de punição pelo órgão estatal. Estas podem ser medidas de benefícios fiscais ou isenções direcionadas a empresas que demonstrem uma ativa preocupação com a privacidade e a proteção de dados dos seus consumidores e usuários, por meio, a título de exemplo, da cooperação com o órgão regulador e da adoção do princípio *privacy by design* de ponta a ponta no funcionamento da empresa e de seus produtos. A iniciativa poderia inclusive auxiliar a mudança de cultura do mercado em direção à percepção

---

[25] "*Despite the possible hurdles in the way, society needs the commitment to privacy to come out on top*."

da privacidade como ideal de operação, bem como elemento de competitividade e vantagem econômica (BIONI, 2017).

Pode-se perceber que, em campos como o da tecnologia, o direito adquire um importante papel de metarregulação. Isto significa a responsabilidade de as normas jurídicas determinarem uma orientação sobre processos deslocados do Estado que também criam regulações específicas. Enquanto a autorregulação da tecnologia estabelece-se como aliada essencial na busca pela efetivação de direitos fundamentais, subsiste a necessidade da criação, a partir do direito, de um quadro normativo, ético e valorativo dentro do qual as decisões dos agentes econômicos sobre tecnologia e dados podem ou devem operar com o intuito de equilibrar a tensão entre privacidade, liberdade e utilidade (MAGRANI; OLIVEIRA, 2019; MARRAFON; COUTINHO, 2020).

Em sentido semelhante, ressalta ainda a professora Ana Frazão (2019) que não se deve esperar que a lei resolva todos os problemas relacionados à proteção de dados pessoais:

> Diante das limitações naturais da heterorregulação, as suas normas e garantias só ganharão efetividade caso haja a concorrência proveitosa da autorregulação ou corregulação, da regulação pela tecnologia e também das soluções do mercado, quando estas reforcem o protagonismo do próprio titular, valorizando o seu consentimento sempre que este for de fato livre, informado e compatível com a natureza existencial do objeto da negociação. (FRAZÃO, 2019, p. 46)

Em harmonia com a colocação pertinente da autora, para a garantia da efetividade e aplicação da Lei Geral de Proteção de Dados no Brasil e a consecução de seus objetivos, parece não bastar a previsão legal acerca do protagonismo do titular dos dados em decidir sobre as operações realizadas com seus dados. Mais do que isso, faz-se necessária a colaboração entre entidades públicas e privadas para a elaboração de um arcabouço regulatório neste tema da privacidade, de forma a contemplar as peculiaridades dos mercados em consonância com os objetivos almejados pelo Estado em proteção à sociedade, equacionados os interesses das três partes.

Para que se chegue a esse ponto, o reconhecimento do alto custo social imposto pelo contexto do mercado de dados é imperioso (PARCHEN; FREITAS, 2016). A dignidade humana, os direitos da personalidade e a própria democracia são postos em risco quando direitos fundamentais são ameaçados, ainda mais quando há uma desídia conjuntural quanto à sua importância, significado e profundidade. Não é construtivo que se tenha uma sociedade passiva, submetida a abusos constantes e, em algum nível, escancarados como os relativos à utilização arbitrária de dados pessoais. Nessa perspectiva, busca-se elementarmente a estruturação de uma consciência coletiva, um compromisso com a privacidade em âmbito

superior, que perpasse a organização do Estado, a operação do mercado e o comportamento do indivíduo, capaz de conceber um novo modelo, tão melhor quanto factível, sobre o qual atualmente só se teoriza e se fantasia.

5 CONCLUSÃO

Em seu artigo intitulado “Does improved technology mean progress?” (em livre tradução: “O aprimoramento da tecnologia significa progresso?”), Leo Marx (1987) faz críticas à adoção impensada das novas tecnologias. À época, criticava o autor a visão eminentemente tecnocrata de que as inovações científica e tecnológica seriam a base para o progresso em geral. Como se avanços em potência, produtividade e racionalidade encontrassem, em si, a própria finalidade, enquanto outras matérias acompanhariam esta autoproclamada evolução. Entre estas outras matérias estariam as questões sociais, políticas e culturais, associadas a valores então relegados a segundo plano em favor do “progresso”. Em conclusão à obra, e buscando responder o questionamento proposto em seu título, declara o autor:

> O aprimoramento da tecnologia significa progresso? Sim, com certeza **poderia** significar exatamente isso. Mas somente se nós estivermos dispostos e habilitados a responder a próxima pergunta: progresso em direção a quê? O que é isto que queremos que nossa tecnologia conquiste? O que queremos além de tão imediatos, limitados objetivos, como conquistar produtividade, reduzindo custos financeiros, e eliminando o problemático elemento humano dos nossos espaços de trabalho? Na ausência de respostas a essas questões, aprimoramentos tecnológicos podem muito bem se revelar incompatíveis com o genuíno progresso, isto é, o progresso social.[26] (MARX, 1987, p. 42, tradução nossa, grifo do autor)

Assim como ocorre com as preocupações de Warren e Brandeis acerca da impetuosa ação da imprensa sobre a vida privada, capitalizadas pela popularização das máquinas fotográficas, observa-se a oportunidade de estabelecer novo paralelo da contemporaneidade com o ceticismo de Marx quanto ao progresso diretamente associado ao avanço tecnológico, em detrimento do próprio elemento humano.

No decorrer desta produção foram expostos alguns elementos particulares à sociedade informacional, entre os quais o seu elemento adjetivante: a informação e sua relevância. Esta relevância perpassa a sociedade, o mercado e os governos. Hoje, o poder deriva da informação. Concorre para isso, também, o contexto de amplo e difuso monitoramento em que se insere a sociedade informacional.

---

[26] “*Does improved technology mean progress? Yes, it certainly **could** mean just that. But only if we are willing and able to answer the next question: progress toward what? What is that we want our new technologies to accomplish? What do we want beyond such immediate, limited goals as achieving efficiencies, decreasing financial costs, and eliminating the troubling human element from our workplaces? In the absence of answers to these questions, technological improvements may very well turn out to be incompatible with genuine, that is to say social, progress.*”

Em específico, tratou-se de uma recorrente relação jurídica à qual os indivíduos habitualmente se submetem: a relação travada por meio dos acordos telemáticos, aqueles realizados por meios digitais. Os acordos telemáticos apresentam características que remontam às peculiaridades do contrato de adesão, entre elas a fixação prévia e unilateral das cláusulas, sua uniformidade para que possibilite a contratação de um grande número de pessoas e, pela mesma razão, a sua virtual imutabilidade. Eles são travados diariamente por usuários das redes, podendo ser considerados até como indispensáveis à navegação nos meios digitais, visto que cada plataforma apresenta termos próprios com os quais o indivíduo necessita concordar (em expresso ou de forma tácita) como condição para a sua fruição.

Os acordos telemáticos, concluídos com o intermédio dos Termos e Condições, Políticas de Privacidade ou documentos correlatos, versam sobre as regras de utilização das respectivas plataformas, mas também, notadamente, sobre procedimentos de tratamento de dados (operações como coleta, transferência, utilização, exibição e exclusão de dados, entre outras). A deficiência do elemento de voluntariedade na decisão de contratar, no entanto, deve ser frisada. Cada vez mais, com a digitalização das relações, o acesso às plataformas virtuais torna-se mais essencial à realização do indivíduo como ser social, além de condicionar o acesso a uma infinidade de serviços e oportunidades. Ainda, estudos apontam que os usuários que se manifestam em concordância com os termos dos contratos o fazem sem sequer ter lido os documentos, gerando um consentimento de legitimidade questionável. Essa relação de certa vulnerabilidade e dependência que se estabelece entre o indivíduo inserido na sociedade da informação e as redes faz com que aquele seja transfigurado em produto no mercado de dados.

O manifesto desequilíbrio na relação do indivíduo com os agentes econômicos, com os quais necessita contratar, e o eminente desamparo informativo generalizado da população acabam por apresentar relevante repercussão cognitiva, prática e jurídica, a despeito da sutileza da imiscuição dos agentes econômicos nas esferas íntimas dos indivíduos. Em função da inevitável inserção na sociedade informacional, marcada pela utilização das tecnologias cibernéticas, restam os indivíduos – agora “datificados” – atravessados por sugestões, modulações, direcionamentos, propostas, convites, e sujeitos ao impacto de decisões, respostas, limitações e recusas em sua vivência nas redes. Tudo relacionado com a digitalização das relações e, em última análise, do próprio ser humano. Sua personalidade digital o antecipa e o que os sistemas depreendem desta construção algorítmica é tido como arriscadamente determinante na condução da sua vida familiar e do seu futuro educacional, profissional e econômico.

Apoiando-se na natureza contratual e, por consequência, jurídica dos contratos telemáticos, estabeleceu-se como peça chave para a coleta e comercialização de dados pessoais o consentimento do usuário. Viu-se, no entanto, que o fato de os usuários não terem o costume de ler os termos a que se submetem, a inerente complexidade desses termos, a capacidade cognitiva limitada do ser humano, a indispensabilidade do acesso às plataformas digitais, entre outros fatores, minam a legitimidade do consentimento colhido pelo sistema concebido para tal, o sistema *Notice and Choice*. Daí, pode-se inferir a situação delicada na qual se encontra o mercado e a ampla comercialização de dados pessoais, alicerçados, de forma generalizada, sobre manifestações de vontade desprovidas de segurança, certeza, conhecimento ou consciência.

Este é um dos lados da sociedade da informação que demonstra a relevância da proteção dos dados pessoais, do direito de autodeterminação informativa – o poder de ingerência do titular dos dados sobre o que fora produzido de informação sobre ele – e da instrução das populações sobre as repercussões fáticas da sua permissão (consentimento) quanto à coleta desses mesmos dados. Reafirme-se a importância de salvaguardar todos esses aspectos da existência humana num contexto em que atores econômicos proclamam a morte iminente e inevitável da privacidade, a despeito de seu caráter de direito fundamental, de compor um repertório de diretrizes superiores que devem direcionar a organização do Estado.

Nesse seguimento, foi ressaltada a dupla dimensão do instituto do consentimento na contemporaneidade: a de legitimidade e a de legitimação. Primeiramente, ao conceber a prerrogativa de decisão sobre as operações de tratamento de dados pessoais ao seu próprio titular, garantiu-se que o consentimento do usuário – responsável por embasar as respectivas relações contratuais travadas com os agentes do mercado – alicerçaria o mercado de dados, dando-lhe legitimidade. Por outro lado, a falta de regulamentação estatal específica das relações entre os provedores e os usuários possibilitou a proliferação de termos e práticas abusivas por parte dos agentes de tratamento. Estes, sob a égide do consentimento genérico e irrefletido do usuário, passaram a ter em mãos um instrumento de ampla legitimação de suas atividades, inclusive as futuras, sobre as quais o indivíduo carece de esclarecimentos.

De fato, lidar com a fugacidade da tecnologia e a infinitude de possibilidades trazidas por ela é de grande complexidade. O direito, por previsivelmente não cumprir de forma precisa um papel preditivo, faz-se elástico para abarcar as situações que surgem com o tempo. O presente trabalho almejou desenvolver uma discussão que surgiu a partir da diversificação do uso das redes e das novas formas de capitalização sobre a atividade corriqueira de usuários da internet. Todo esse quadro, é claro, só foi possível com o desenvolvimento tecnológico.

Mas a questão de Marx, mais de trinta anos depois, ainda ecoa. Estaria a sociedade, dessa forma, progredindo?

Em vista da situação de precarização do direito à privacidade na forma de lesão ao direito à proteção de dados pessoais, notadamente no Brasil, foram exploradas por último algumas medidas práticas e abordagens teóricas que propunham dar condição à efetivação desses direitos. A exposição foi dividida entre medidas de autorregulação (relativa ao mercado) e heterorregulação (relativa ao Estado). Na forma da autorregulação do mercado, destacou-se a importância da adoção do princípio *privacy by design*, que trata da adoção ampla de um parâmetro de proteção à privacidade, desde a concepção de projetos, passando pelo tratamento de dados e funcionamentos de produtos e prestações de serviço (aplicação de ponta a ponta).

Quanto à heterorregulação por parte do Estado, foi destacada a sua função de normatização, além de articuladas e correlacionadas as teorias de Nissenbaum acerca das normas informacionais e integridade contextual, e as de Sloan e Warner sobre as normas de valor ótimo e a completude normativa. Depreende-se desta análise que fluxos de informações verificados no cotidiano fora das redes, com os quais a população já está habituada, podem, sob uma ótica contextual, servir de guia a uma eventual regulamentação informacional que parta, por analogia e paralelismo, das relações já existentes, as quais possuem semelhança com aquelas do meio digital. Por terem origem em situações do convívio social em geral bem estabelecidas, tais normas informacionais, transfiguradas e adaptadas ao meio digital, aproximar-se-iam da expectativa e de valores dos grupos sociais, e seriam aptas, assim, a dar legitimidade à utilização de dados pessoais. Apesar de constatada a natureza eminentemente retórica das teorias, verificou-se a sua importância para lançar luz sobre caminhos diversos do sistema *Notice and Choice*, enraizado nas práticas de mercado e na cultura digital.

Como saldo, afirmou-se a necessidade da criação de uma cultura de proteção de dados no País – operação na qual a Autoridade Nacional de Proteção de Dados (ANPD) ocupa um papel importante – a fim de estimular o cumprimento de medidas, atuais e futuras, impostas pelo Estado e instruir a população para que esta também realize uma cobrança dos agentes de mercado sobre sua autorregulação e adequação aos preceitos constitucionais e direitos fundamentais de seus usuários.

Vê-se que, apesar de o desenvolvimento da tecnologia ter proporcionado à sociedade revoluções nos setores de transportes, da saúde, da energia, do comércio, da comunicação, do entretenimento, entre tantos outros, não se deve perder de vista o custo social desses avanços. Resgatando a ideia de Leo Marx por um instante, há de se constatar que, com os privilégios trazidos pelas novas tecnologias, seguiram-se problemáticas lesivas à existência do

indivíduo neste mundo moderno e transformado. Assim, se o que se quer é atingir o "progresso", precisa-se definir as bases para esse progresso, seus fundamentos, diretrizes e limites. Precisa-se significar o próprio "progresso". A depender, se o progresso que se pretende alcançar for inclusivo, democrático e, acima de tudo, humano, é interessante que as práticas de mercado ante os seus consumidores e o papel do Estado responsável por regulamentá-las sejam repensados, e que uma discussão mais profunda a esse respeito encontre espaço nos mais diversos cenários sociais, com o fito de garantir um progresso que não é só tecnológico, mas social.

REFERÊNCIAS

AN OVERVIEW of licenses: shrink-wrap vs. click-wrap vs. Browse-wrap licenses. **Odinlaw**. Raleigh: c2020. Disponível em: <https://odinlaw.com/overview-licenses-shrink-wrap-vs-click-wrap-vs-browse-wrap-licenses/>. Acesso em: 26 fev. 2021.

ASTONE, Daniel; FERES, Marcos V. C. Inovação e arranjos de propriedade intelectual no desenvolvimento do software livre. In: ZANATTA, Rafael A. F.; PAULA, Pedro C. B. de; KIRA, Beatriz (org.). **Economias do compartilhamento e o direito**. Curitiba: Juruá, 2017. p. 347-371.

BAROCAS, Solon; NISSENBAUM, Helen Fay. Big data's end run around procedural privacy protections: recognizing the inherent limitations of consent and anonymity. **Communications of the ACM**, v. 57, n. 1, p. 31-33, nov. 2014. Disponível em: <https://dl.acm.org/doi/10.1145/2668897>. Acesso em: 17 mar. 2021.

BIONI, Bruno Ricardo. Como o Brasil pode inovar na proteção de dados pessoais. **Globo**, São Paulo, 20 mar. 2017. Valor. Disponível em: <https://valor.globo.com/opiniao/coluna/como-o-brasil-pode-inovar-na-protecao-de-dados-pessoais.ghtml>. Acesso em: 16 mar. 2021.

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

BIONI, Bruno Ricardo; ALVES, Fabricio da Mota Alves. **A importância da PEC de proteção de dados mesmo após o histórico julgamento do STF**. Jota, São Paulo, 16 jun. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-importancia-da-pec-de-protecao-de-dados-mesmo-apos-o-historico-julgamento-do-stf-16062020>. Acesso em: 06 mar. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 14 jan. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 8 fev. 2021.

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

BRASIL. Senado Federal. **Proposta de Emenda à Constituição nº 17, de 2019**. Altera 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. Brasília, DF: Senado Federal, 2019. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acesso em: 06 mar. 2021.

BRASIL SOFREU mais de 2,6 bilhões de ciberataques no primeiro semestre de 2020. **Security Report**, Rio de janeiro, 24 ago. 2020. Disponível em: <https://www.securityreport.com.br/destaques/brasil-sofreu-mais-de-26-bilhoes-de-ciberataques-no-primeiro-semestre-de-2020/#.YD1J-Nxv_IU>. Acesso em: 01 mar. 2021.

BRUNO, Fernanda. Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas. **Revista Fronteiras**. São Leopoldo, v. 8, n. 2, p. 152-159, maio/ago. 2006. Disponível em: <http://revistas.unisinos.br/index.php/fronteiras/article/view/6129>. Acesso em: 22 fev. 2021.

BRUNO, Fernanda et al. O oráculo de Mountain View: o Google e sua cartografia do ciberespaço. **E-Compós**, v. 6, jun. 2006. Disponível em: <https://doi.org/10.30962/ec.91>. Acesso em: 22 fev. 2021.

BRUNO, Fernanda. O Google e a nossa privacidade: jogos eletrônicos e perfis psicológicos. **Dispositivos de visibilidade e subjetividade contemporânea.** 20 maio 2007. Disponível em: http://dispositivodevisibilidade.blogspot.com/2007/05/o-google-e-nossa-privacidade-jogos.html. Acesso em: 22 fev. 2021.

BRUNO, Fernanda. O fim da privacidade em disputa. **Dispositivos de visibilidade e subjetividade contemporânea**. 24 jan. 2010. Disponível em: <http://dispositivodevisibilidade.blogspot.com/2010/01/o-fim-da-privacidade-em-disputa.html>. Acesso em: 19 fev. 2021.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza X. De A. Borges. Rio de Janeiro: Zahar, 2003.

RAVICHANDER, Abhilasha et al. The role of active privacy management in a world where the consent model breaks down. In: **Computers, privacy & data protection international conference**. Evento realizado pela Forham Center on Law and Informational Policy, 23 jan. 2020. Disponível em: <https://www.youtube.com/watch?v=SSuysO_nSyI>. Acesso em 9 fev. 2021.

DATA is giving rise to a new economy. **The economist**. 6 maio de 2017. Disponível em: <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy>. Acesso em: 01 mar. 2021.

DEMELLO, Marco. Mundo vive pandemia de ciberataques e Brasil está despreparado, diz CEO de empresa que descobriu megavazamento. **BBC news Brasil**, Londres, 12 fev. 2021. Entrevista concedida a Nathalia Passarinho. Disponível em: <https://www.bbc.com/portuguese/brasil-56048010>. Acesso em: 01 mar. 2021.

DIGITAL NATIONS. **Digital nations: leading digital governments**, c2020. Página inicial. Disponível em: <https://www.leadingdigitalgovs.org/>. Acesso em: 11 mar. 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço jurídico journal of law**. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 16 jan. 2021.

EDWARDS, Lilian; HATCHER, Jordan S. Consumer privacy law 2: data collection, profiling and targeting. In: EDWARDS, L.; WAELDE, C. (Org.). **Law and the Internet**. Oxford: Hart Publishing, 2009. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1435105>. Acesso em 13 jan. 2021.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito.** São Paulo, v. 88, p. 439-459, 1993. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 7 jan. 2021.

FERRAZ JÚNIOR, Tércio Sampaio. **Introdução ao estudo do direito**: técnica, decisão, dominação. 10. ed. rev., atual. e ampl. São Paulo: Atlas, 2018.

FRAZÃO, Ana. Plataformas digitais e os desafios para a regulação jurídica. In: PARENTONI, Leonardo (coord.); GONTIJO, Bruno Miranda; LIMA, Henrique Cunha Souza (orgs.). **Direito, tecnologia e inovação**. Belo Horizonte: D'Plácido, 2018. v. 1. p. 635-669.

FRAZÃO, Ana. Direitos básicos dos titulares de dados pessoais. **Revista do advogado**, São Paulo, v. 39, n. 144, p. 33-46, nov. 2019. Disponível em: <https://www.aasp.org.br/revista-do-advogado/>. Acesso em: 13 jan. 2021.

FREITAS, Cinthia Obladen de Almendra. Tratamento de dados pessoais e a legislação brasileira frente ao profiling e à discriminação a partir das novas tecnologias. **Revista de direito, governança e novas tecnologias**, v. 3, n. 2, p. 18-38. jul/dez. 2017. Disponível em <https://www.indexlaw.org/index.php/revistadgnt/article/view/2430/pdf>. Acesso em: 01 mar. 2021.

GATT, Adam. Eletronic commerce – click-wrap agreements: the enforceability of click-wrap agreements. **Computer law & security review**. v. 18, n. 6, p. 404-410, 2002. Disponível em: <https://edisciplinas.usp.br/pluginfile.php/2056275/mod_resource/content/1/enforceability%20of%20clickwrap%20%28Adam%20Gatt%29.pdf>. Acesso em: 14 jan. 2021.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. 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. Disponível em: <http://dx.doi.org/10.5380/rfdufpr.v47i0.15738>. Acesso em: 17 mar. 2021.

GOMES, Orlando. **Contratos**. BRITTO, Edvaldo (coord.); AZEVEDO, Antonio Junqueira de; MARINO, Francisco Paulo de Crescenzo (atualizadores). 26. ed. Rio de Janeiro: Forense, 2009.

HOOFNAGLE, Chris Jay; KING, Jennifer. **What californians understand about privacy online**. 2008. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262130>. Acesso em: 17 mar. 2021.

HUGHES, Eric. **A cypherpunk's manifesto**. 1993. Disponível em: <https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt>. Acesso em 18 jan. 2021.

ORTUNHO JÚNIOR, Waldemar Gonçalves; WIMMER, Miriam. Foco inicial será criar cultura de dados, diz presidente da ANPD. **Jota**, Brasília, 26 jan. 2021. Entrevista concedida a Guilherme Pimenta e Alexandre Leoratti. Disponível em: <https://www.jota.info/tributos-e-empresas/mercado/cultura-de-dados-presidente-anpd-26012021>. Acesso em: 12 mar. 2021.

KOROBKIN, Russel. Bounded rationality, standard form contracts, and unconscionability. **The university of Chicago law review**. v. 70, n. 4, p. 1203-1295, 2003. Disponível em: <https://www.jstor.org/stable/1600574>. Acesso em: 7 fev. 2021.

LAFER, Celso. **A reconstrução dos direitos humanos**: um diálogo com o pensamento de Hannah Arendt. São Paulo: Companhia das Letras, 1991.

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

LIMA, Cíntia Rosa Pereira de. O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos. In: ROVER, Aires José Rover; CELLA, José Renato Gaziero; AYUDA, Fernando Galindo (org.). **Direito e novas tecnologias I [Recurso eletrônico on-line] conpedi/UFPB**. Florianópolis: Conpedi, 2014. p. 343-365. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=981322808aba8a03>. Acesso em: 13 jan. 2021.

MACEDO JÚNIOR, Ronaldo Porto. Privacidade, mercado e informação. **Justitia**, São Paulo, v. 61, n. 185/188, p. 245-259, jan./dez. 1999. Disponível em: <https://core.ac.uk/download/pdf/79074338.pdf>. Acesso em: 8 fev. 2021.

MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. We are big data: new technologies and personal data management. **Cyberlaw by CIJIC**, Lisboa, n. 5, mar. 2018. Disponível em: <http://eduardomagrani.com/en/we-are-big-data-new-technologies-and-personal-data-management/>. Acesso em: 01 mar. 2021.

MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. A internet das coisas e a lei geral de proteção de dados: reflexões sobre os desafios do consentimento e do direito à explicação. **Revista do advogado**, São Paulo, v. 39, n. 144, p. 80-89, nov. 2019. Disponível em: <https://www.aasp.org.br/revista-do-advogado/>. Acesso em: 13 jan. 2021.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Princípio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. **Revista eletrônica direito e política, programa de pós-graduação stricto sensu em ciência jurídica da UNIVALI**, Itajaí, v. 15, n. 3, 3º quadrimestre de 2020. Disponível em: <https://siaiap32.univali.br/seer/index.php/rdp/article/view/17119>. Acesso em 18 mar. 2021.

MARX, Leo. Does improved technology mean progress?. **Technology review**. p. 33-42, Jan. 1987. Disponível em: <https://raphiinconcordia.files.wordpress.com/2015/05/readings-1-does-technology-mean-progress.pdf>. Acesso em: 22 mar. 2021.

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

MOEREL, Lokke. How to monetize data: rules of the road and ethical dilemmas. In: SMITH, Peter; COCKBURN, Tom (ed.). **Global business leadership development for the fourth industrial revolution**. London: IGI Global, 2021. p. 95-104.

MONTEIRO, Renato Leite; BIONI, Bruno. Que tal uma pizza de tofu com rabanetes? você vai adorar. **Jusbrasil**, 15 jun. 2015. Disponível em: <https://renatoleitemonteiro.jusbrasil.com.br/artigos/198336962/que-tal-uma-pizza-de-tofu-com-rabanetes-voce-vai-adorar>. Acesso em: 01 mar. 2021.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do advogado**, São Paulo, v. 39, n. 144, p. 47-53, nov. 2019. Disponível em: <https://www.aasp.org.br/revista-do-advogado/>. Acesso em: 13 jan. 2021.

NISSENBAUM, Helen Fay. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

NISSENBAUM, Helen Fay. A contextual approach to privacy online. **Dædalus, the journal of the american academy of arts & sciences**, v. 140, n. 4, p. 32-48, fall, 2011. Disponível em: <https://ssrn.com/abstract=2567042>. Acesso em: 06 mar. 2021.

OBAR, Jonathan A.; OELDORF-HIRSCH, Anne. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. **Information, communication & society**, p. 1-20, 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465>. Acesso em: 26 fev. 2021.

OLIVEIRA, Ana Paula de et al. A lei geral de proteção de dados brasileira na prática empresarial. **Revista jurídica da escola superior de advocacia da OAB-PR.** Curitiba, ano 4, n. 1, não paginado, maio 2019. Disponível em: <http://revistajuridica.esa.oabpr.org.br/a-lei-geral-de-protecao-de-dados-brasileira-na-pratica-empresarial/>. Acesso em: 16 mar. 2021.

PAESANI, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil. ed. 6. São Paulo: Atlas, 2013.

PARCHEN, Charles Emmanuel; FREITAS, Cinthia Obladen de Almendra. Big data e mineração de dados sob a ótica do direito constitucional à privacidade e intimidade. In: FREITAS, Cinthia Obladen de Almendra; BARRETO JUNIOR, Irineu Francisco Barreto; BOFF, Salete Oro (coord.). **Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização conpedi/unicuritiba**. Florianópolis: Conpedi, 2016. p. 133-151. Disponível em: <http://conpedi.danilolr.info/publicacoes/02q8agmu/96gn7y36/Qrc0QP9Dr3LgMIVS.pdf>. Acesso em: 15 mar. 2021.

PARENTONI, Leonardo. Autoridade nacional de proteção de dados brasileira: uma visão otimista. **Revista do advogado**, São Paulo, v. 39, n. 144, p. 209-219, nov. 2019. Disponível em: <https://www.aasp.org.br/revista-do-advogado/>. Acesso em: 11 mar. 2021.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

RIVERO, Jean; MOUTOUH, Hugues. **Liberdades públicas**. Tradução de Maria Ermantina de Almeida Prado Galvão. São Paulo: Martins Fontes, 2006.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. **Direito, estado e sociedade**, Rio de Janeiro, n. 36, p. 178-199, jan/jun. 2010. Disponível em: <http://direitoestadosociedade.jur.puc-rio.br/media/8ruaro_rodriguez36.pdf>. Acesso em: 15 jan. 2021.

SILVA, José Afonso da. **Teoria do conhecimento constitucional**. São Paulo: Malheiros, 2014.

SILVEIRA, Sérgio Amadeu da. **Tudo sobre tod@s**: redes digitais, privacidade e venda de dados pessoais. São Paulo: Edições SESC, 2017.

SLOAN, Robert H.; WARNER, Richard. Beyond notice and choice: privacy, norms and consent. **Suffolk university journal of high technology law**, v. 370, 2014a. Disponível em: <https://www.researchgate.net/publication/256054650_Beyond_Notice_and_Choice_Privacy_Norms_and_Consent>. Acesso em: 11 mar. 2021.

SLOAN, Robert H.; WARNER, Richard. **Unauthorized access**: the crisis in online privacy and security. Boca Raton: CRC Press, 2014b.

SOLOVE, Daniel J. **The digital person**: technology and privacy in the information age. New York: New York University, 2004.

STROINK-SKILLRUD, Donata. Clickwrap vs. Browsewrap: why placement matters. **Termageddon**. Chicago: 25 abr. 2020. Disponível em: <https://termageddon.com/clickwrap-vs-browsewrap/>. Acesso em: 26 fev. 2021.

SUNSTEIN, Cass R.; JOLLS, Christine; THALER, Richard H. A behavioral approach to law and economics. **Stanford law review**, v. 50, p. 1471-1550, 1998. Disponível em: <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=12172&context=journal_articles>. Acesso em: 8 fev. 2021.

SUNSTEIN, Cass R. **Choosing not to choose**: understanding the value of choice. New York: Oxford University Press, 2015.

TVERSKY, Amos; KAHNEMAN, Daniel. Judgment under uncertainty: heuristics and biases. **Science**, new series, v. 185, n. 4157, p. 1124-1131, 1974. Disponível em: <http://links.jstor.org/sici?sici=0036-8075%2819740927%293%3A185%3A4157%3C1124%3AJUUHAB%3E2.0.CO%3B2-M&origin=JSTOR-pdf>. Acesso em: 8 fev. 2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation)**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 14 jan. 2021.

UNITED STATES OF AMERICA. **Federal Trade Commission**, 2021a. Página inicial. Disponível em: <https://www.ftc.gov>. Acesso em: 15 mar. 2021.

UNITED STATES OF AMERICA. **Federal Trade Commission**, 2021b. News & events. Privacycon 2021. Disponível em: <https://www.ftc.gov/news-events/events-calendar/privacycon-2021>. Acesso em: 15 mar. 2021.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, Boston, v. 4, n. 5, p. 193-220, dec. 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em 14 jan. 2021.

WESTIN, Alan F. **Privacy and freedom**. Nova York: Atheneum, 1967. Disponível em: <https://archive.org/details/privacyfreedom00west/mode/2up>. Acesso em 14 jan. 2021.