

INSTRUMENTOS DE PROTEÇÃO DE DIREITOS FUNDAMENTAIS NA LEI GERAL DE PROTEÇÃO DE DADOS: A FINALIDADE NO TRATAMENTO DE DADOS PESSOAIS E A INVERSÃO NA LÓGICA DA FISCALIZAÇÃO

CÍNTIA BACCARIN¹

LUCIANA LOPES CANAVEZ²

SUMÁRIO: 1. INTRODUÇÃO. 2. A SOCIEDADE E SEUS DADOS NO UNIVERSO DIGITAL 3. A PROTEÇÃO DOS DADOS PESSOAIS. 3. A IMPORTÂNCIA DA FINALIDADE E DA FISCALIZAÇÃO PARA A PROTEÇÃO DOS DADOS PESSOAIS. CONSIDERAÇÕES FINAIS. REFERÊNCIAS.

RESUMO: A sociedade atual, por causa dos avanços da tecnologia, passou a produzir e armazenar informações em grande escala no universo digital. A partir disso, os dados pessoais tornaram-se peça necessária na engrenagem da economia digital, e novos desafios foram surgindo para a proteção de direitos fundamentais de seus titulares. Em resposta, a Ciência Jurídica vem abordando a temática com maior maturidade. Assim, por meio da metodologia dedutiva-bibliográfica, o artigo demonstrou a importância da proteção de dados pessoais e como o Supremo Tribunal Federal e a Lei Geral de Proteção de Dados (Lei n. 13.709/18) vêm cuidando do assunto. Dessa forma, compreende-se a importância de se delimitar a finalidade para realização do tratamento de dados pessoais, assim como a relevância da fiscalização, feita por cada um dos titulares desses dados e pelas empresas possuidoras desses dados. Demonstrou-se que ambos instrumentos são indispensáveis para a efetiva

¹ Mestranda em Direito pela Faculdade de Ciências Humanas e Sociais (FCHS) da Universidade Estadual Paulista “Júlio de Mesquita Filho” (UNESP). E-mail: cinthia.baccarin@unesp.br. ORCID ID: <http://orcid.org/0000-0003-1777-4929>

² Doutora em Direito pela Faculdade Autônoma de Direito de São Paulo. Mestre em Direito pela Universidade de Franca. Professora assistente vinculada ao Departamento de Direito Privado, de Processo Civil e do Trabalho da Faculdade de Ciências Humanas e Sociais (FCHS) da Universidade Estadual Paulista “Júlio de Mesquita Filho” (UNESP). E-mail: luciana.canavez@unesp.br. ORCID ID: <https://orcid.org/0000-0002-3953-7433>

proteção de dados pessoais e outros direitos fundamentais e, conseqüentemente, para promover maior confiança nas pessoas e nas relações entre empresas.

PALAVRAS-CHAVE: Direitos fundamentais. Lei Geral de Proteção de Dados. Finalidade. Tratamento de dados. Fiscalização inversa.

INSTRUMENTS FOR THE PROTECTION OF FUNDAMENTAL RIGHTS IN THE GENERAL DATA PROTECTION LAW: THE PURPOSE IN THE PROCESSING OF PERSONAL DATA AND THE INVERSION IN SUPERVISORY LOGIC

ABSTRACT: Through advances in technology, today's society has started to produce and store information on a large scale in the digital universe. From this, personal data became a necessary part of the digital economy, while new challenges were emerging for the protection of fundamental rights of their holders. In response, Legal Science has been addressing the theme with greater maturity. Thus, through the deductive-bibliographic methodology, the article demonstrated the importance of protecting personal data and how the Federal Supreme Court and the General Data Protection Law (Law No. 13,709 / 18) has been taking care of the matter. In this way, it is understood the importance of delimiting the purpose for the treatment of personal data, as well as the relevance of the inspection, made by each one of the holders of this data and made by the companies that own this data. Both instruments have been shown to be indispensable for the effective protection of personal data and other fundamental rights and, consequently, to promote greater trust in people and in relationships between companies.

KEYWORDS: Fundamental rights. General Data Protection Law. Purpose. Processing of data. Reverse inspection.

INTRODUÇÃO

Estudiosos já conseguem analisar historicamente as diversas formas de organização social e suas modificações até hoje. Bruno Ricardo Bioni descreve

que a sociedade atual está vivendo sob uma forma de organização cujo elemento nuclear é a informação. De modo geral, o foco para o desenvolvimento econômico não são mais os recursos como a terra, a produção ou a oferta de serviços, que outrora marcaram as sociedades agrícola, industrial e pós-industrial.³ Assim, atualmente, a sociedade vive, molda-se e propulsiona a economia por meio da informação.

Essa nova lógica social foi consolidada devido à evolução tecnológica nas últimas décadas, já que foram criados meios eficazes de processamento e transmissão de informações em grande quantidade e velocidade.⁴ Um sintoma disso, há oito anos, em junho de 2013, foram as manifestações iniciadas na cidade de São Paulo contra o aumento da tarifa de ônibus, mas que posteriormente se alastraram por todo o território nacional com várias outras reivindicações sociais.⁵ Nessas manifestações, a democracia e a cidadania foram exercidas por uma corrente de informações - em sua maioria pelas redes sociais - que permitiram a união de pessoas, a disseminação dos protestos e a organização de estratégias. Dentre este e outros exemplos é que se justifica a caracterização que a coletividade atualmente recebe: sociedade da informação.

O computador, o celular e a internet, embora não sejam as únicas, são as principais ferramentas para essa nova forma de organização social, substituindo as morosas informações gravadas e transmitidas somente por meios físicos, como o papel e o livro. Essas informações são codificadas em um alfabeto binário, ou seja, introduzidas em computadores em formatos de digitação, áudio e vídeo. Além disso, o acesso à internet possibilitou o acúmulo e a transmissão de informações de maneira inimaginavelmente maior e em tempo imediato.

Contudo, o processamento/organização da informação é tão importante quanto ela própria, já que o conhecimento a ser utilizado como impulso para as atividades empresariais será produzido a partir deste mecanismo.⁶ Por exemplo,

³ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. p. 33.

⁴ *Ibidem*. p. 34.

⁵ JUDENSNAIDER, Elena; LIMA, Luciana; ORTELLADO, Pablo; POMAR, Marcelo. **Vinte centavos: a luta contra o aumento**. São Paulo: Editora Veneta, 2013.

⁶ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. p. 38.

empresas que obtenham, dentre outras informações, o conhecimento sobre os hábitos de consumo dos seus clientes, conseguem empreender com mais eficiência no mercado em relação àquelas que não detenham esse embasamento.

Dessa forma, para que funcione a engrenagem econômica, baseada em informações, grande quantidade delas rotineiramente são registradas na internet, seja por meio de cliques em *websites* ou cadastros em perfis, e ficam armazenadas em bancos de dados de empresas, organizações e/ou do governo. “No ambiente tecnológico atual, toda informação eletronicamente transmitida é gravada, podendo vir a ser processada, identificada e combinada numa unidade de análise coletiva ou individual”⁷.

Não são apenas nomes, números de identificação - RG e CPF -, endereços ou fotos que permitem a identificação de alguém. Também acessos a sites, conversas com representantes de operadoras telefônicas, cadastros em farmácias em troca de desconto e a utilização de aplicativos em smartphones são situações cotidianas que deixam igualmente registros de dados pessoais.⁸ A junção de pequenas informações deixadas vão retratar cada personalidade, identificando características, gostos e predileções. A partir disso, sistemas processam esses dados, calculam todas as informações, retornam com um resultado e, assim, decisões são tomadas e vidas impactadas. Toda essa sistemática se torna gradativamente maior em uma sociedade dependente, movida e orientada por fluxo de dados.

Nessa perspectiva, a vulnerabilidade dos usuários da internet, sendo titulares de dados pessoais, cresceu na mesma proporção da inovação tecnológica, principalmente em relação à vida privada e à intimidade. Conseqüentemente, o avanço tecnológico desencadeou novos desafios para a Ciência Jurídica e para a proteção dos direitos fundamentais. A sociedade hiperconectada necessita agora de meios eficazes de proteção dos dados que

⁷ CASTELLS, Manuel. **A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2003. p. 191.

⁸ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, n. 2, v. 12, p. 91-108, jul./dez. 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 10 fev. 2021. p. 93.

fornece e produz no mundo virtual, fato que justifica a importância do Direito Digital⁹, cujos ramos de atuação passam pelo contencioso, consultivo, contratual e compliance.

Feitas essas breves considerações iniciais, de modo geral, é importante considerar que as mudanças promovidas pela tecnologia não podem passar despercebidos pela Ciência Jurídica; do contrário, haveria uma lacuna entre a realidade e as normas jurídicas. Para isso, o Direito precisa estar em harmonia, acompanhar esses avanços da sociedade e deve se adequar, ou, pelo menos, pensar e encarar os novos desafios regulatórios emergentes.

Ademais, um alerta à sociedade faz-se necessário para que ela se conscientize da importância de se ter e defender direitos e valores, que estão se esvaindo socialmente, mas podem ser aspirados no mundo do Direito e aplicados no contexto da internet.

Neste artigo, far-se-á uma análise crítica dedutiva¹⁰ a respeito da importância da proteção de dados pessoais no mundo virtual, bem como um estudo da resposta legislativa a essa problemática e seus efeitos na defesa dos direitos fundamentais, utilizando, para isso, o método de procedimento de pesquisa bibliográfica.¹¹

2 A SOCIEDADE E SEUS DADOS NO UNIVERSO DIGITAL

Tecnicamente, quando um dispositivo informático, seja um smartphone, smartwatch, tablet, notebook, computador, video game, drone, entre outros, se conecta à internet, ele pode ser identificado. Entre a máquina e a internet existe uma conexão indicada por um número chamado internet protocol (IP). O número de IP poderá ser descoberto a partir do momento em que se questiona o

⁹ MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Org). **Direito digital: direito privado e internet**. 2. ed. São Paulo: Editora Foco, 2019.

¹⁰ MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003. p. 91.

¹¹ *Idem*, 2002. p. 71.

responsável por determinada conexão. Entretanto, muitas vezes há falta de interesse, escassez de infraestrutura ou poucos recursos financeiros e tecnológicos para proceder a uma investigação.

O acesso à internet é viabilizado por meio de um provedor, que seriam as empresas Vivo Telefônica, Tim, Net e outras. Para que um usuário se conecte ao mundo virtual, é preciso um provedor de acesso, que identifica o acesso com um número de IP. Portanto, essa operacionalização possibilita constatar quem, quando e a que horas se estabeleceu uma conexão com a internet.

Na década de 90, era comum obter pouca ou nenhuma informação dos internautas. Dessa forma, o anonimato era um padrão, porque “os protocolos Internet não exigem que você credencie quem é você antes de usar a Internet”¹². Os dados de identificação ficavam somente nos registros dos provedores de acesso para fins de realização dos contratos. Na época, “a privacidade era protegida pelo anonimato da comunicação na Internet e pela dificuldade de investigar as origens e identificar o conteúdo de mensagens transmitidas com o uso de protocolos da Internet”¹³.

Mudanças significativas foram ocorrendo a partir da década seguinte, de forma que o anonimato passou a ser quase impossível.

Aplicações de *software* podem ser superpostas em camadas a protocolos da Internet, tornando possível identificar rotas de comunicação e conteúdo. Com o uso dessas tecnologias, é possível violar a privacidade, e uma vez que se torna possível relacionar indivíduos com processos específicos de comunicação em contextos institucionais específicos, todas as formas tradicionais de controle político e organizacional podem ser lançadas sobre o indivíduo em rede.¹⁴

¹² LESSIG, Lawrence. **Code**: version 2.0. Nova Iorque: Basic Books, 2006. p. 35.

¹³ CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 187.

¹⁴ *Ibidem*, p. 189.

Isso se deu, em grande parte, pela criação de uma nova geração de serviços de rede. São os chamados geradores de conteúdo, como Facebook, Twitter, Instagram, WhatsApp, redes sociais em geral, que permitiram a interação entre indivíduos titulares de dados pessoais registrados em um perfil social.

Facebook é uma das principais redes sociais online – que atualmente conta com mais de 2,27 bilhões de usuários mensais ativos em todo globo – e passou a adotar a partir de 2012 a chamada *real-name policy*, estabelecendo como pré-condição à elaboração de um perfil individual no site, o uso da “identidade verdadeira”, isto é, deve a pessoa empregar o prenome e sobrenome com os quais é identificada em sua vida cotidiana.¹⁵

Para além do monitoramento de acessos dos usuários, proporcionados pelos protocolos de internet, tornou-se possível identificar e acompanhar hábitos de navegação, preferências, ou mesmo a localização geográfica. Não é sem motivo que a Google comprou em 2013, pela quantia de US\$ 1,1 bilhão, o aplicativo Waze, que captura a geolocalização de seus usuários.¹⁶

Há sempre uma exposição quando se trata do mundo virtual. A interação com os websites e aplicativos geradores de conteúdo, seja por meio de imagens, sons, check-ins, pesquisas, curtidas ou compartilhamentos, permite que tudo seja identificado, registrado, computado, lido e interpretado naquilo que se intitula de big data.

Everyone knows that the Internet has changed how businesses operate, governments function, and people live. But a new, less visible technological trend is just as transformative: "big data."

¹⁵ MACHADO, Diego; DONEDA, Danilo. Direito ao anonimato na internet: fundamentos e contornos dogmáticos de sua proteção no direito brasileiro. (Outubro 20, 2018). **Revista de Direito Civil Contemporâneo**, [no prelo/forthcoming]. Disponível em: <https://ssrn.com/abstract=3698938>. Acesso em: 6 fev. 2021, p. 3.

¹⁶ COLOME, Jordi Pérez. “Criei o Waze para resolver a perda de tempo no trânsito, mas agora vejo que o problema é pior”. **El país**, 14 out. 2019. Disponível em: https://brasil.elpais.com/brasil/2019/10/10/tecnologia/1570717218_742251.html#:~:text=O%20Google%20comprou%20o%20Waze,bilh%C3%B5es%20de%20reais. Acesso em: 5 fev. 2021.

Big data starts with the fact that there is a lot more information floating around these days than ever before, and it is being put to extraordinary new uses. Big data is distinct from the Internet, although the Web makes it much easier to collect and share data. Big data is about more than just communication: the idea is that we can learn from a large body of information things that we could not comprehend when we used only smaller amounts.¹⁷

Uma característica importante do big data é a capacidade de transformar em dados muitos aspectos do mundo que nunca foram quantificados antes, o que foi denominado por Kenneth Cukier e Viktor Mayer-schoenberger de datafication ou dataficação. Por exemplo, a localização foi transformada em dados, primeiro por meio das coordenadas de latitude e longitude, e recentemente com o sistema de satélite GPS. "Even friendships and "likes" are datafied, via Facebook"¹⁸.

Essa tecnologia faz com que informações e interações registradas sejam interpretadas e se tenha insights a respeito delas. Então, se na rede social alguém curte muitas postagens a respeito de comida, por exemplo, há uma tendência de que isso seja transmitido a *players* do mercado de fornecimento de alimentos, como o Ifood ou Uber Eats, para que eles consigam alcançar e atrair esse usuário. Ou ainda, se um internauta deixa cliques em conteúdos de esportes, há uma tendência de que ele receba publicidade referente a esse tema, e assim por diante com qualquer assunto ou preferência. Dessa forma, ocorre a leitura das interações por poderosos algoritmos - processos matemáticos de interpretação.

A economia digital é baseada nesses exemplos de situações descritas acima. Seria a customização daquilo que é ofertado para adequá-lo ao máximo ao gosto do cliente, com base em dados que ele mesmo forneceu. Quando a plataforma do Netflix é acessada, por exemplo, logo são sugeridas séries, filmes e documentários baseados nos gostos do assinante. Portanto, um algoritmo faz

¹⁷ CUKIER, Kenneth; MAYER-SCHOENBERGER, Victor. The Rise of Big Data: how it's changing the way we think about the world. *Foreign Affairs*, [S.l.], n. 3, v. 92, may/june 2013. Disponível em: <https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data>. Acesso em: 9 fev. 2021. p. 28.

¹⁸ *Ibidem*, p. 29.

a leitura daquilo que já foi assistido, seleciona as mídias ainda não vistas da mesma categoria e expõe logo no início do catálogo.

[...] o desenvolvimento fundamental foram as tecnologias de coleta de dados associadas à economia do comércio eletrônico. Em muitos casos, a principal fonte de rendimentos das companhias de comércio eletrônico são a publicidade e o marketing [...]. Por um lado, elas recebem os lucros das faixas de publicidade que podem exibir para seus usuários. Por outro, vendem os dados de seus usuários para seus clientes para fins de marketing, ou os utilizam elas próprias para melhor mirar seus clientes. Em todos os casos, informação preciosa deve ser colhida de cada clique no website.¹⁹

A customização acontece com tudo na economia digital. Isso não quer dizer que seja ruim em uma perspectiva, porque haverá uma melhora na experiência do indivíduo. Dessa forma, as empresas preferem oferecer uma experiência personalizada para possivelmente fidelizar o cliente. Um dos desafios é sempre oferecer a melhor vivência para quem estiver clicando, acessando e consumindo. Em contrapartida, para tanto, necessariamente é preciso, de alguma forma, invadir a privacidade daquela pessoa, porque haverá a coleta de dados pessoais e o seu processamento segundo os interesses do comércio. Nesse sentido, em outra perspectiva, “os riscos também estão presentes, podendo ser o *big data* manipulado por determinados atores em busca de atingir determinadas finalidades”²⁰.

A leitura massiva de dados invade a privacidade na medida em que precisa ser analisada a partir de interações e informações pessoais deixadas na internet. Mas “a maioria das pessoas abre mão de seus direitos à privacidade para ter condições de usar a Internet. Uma vez que se renunciou a esse direito

¹⁹ CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 193.

²⁰ NETTO, Adhemar Della Torre; OLIVEIRA, Alfredo Emanuel Farias de. Big Data e proteção de direitos fundamentais: perigos da má utilização da técnica e uma proposta para o resgate do ideal sofista de paideia no campo da educação. **Revista de Direito e as Novas Tecnologias**, [S.l], n. 3, v. 2, abr./jun. 2019. p. 2.

à proteção da privacidade, os dados pessoais tornam-se propriedade legítima das firmas de Internet e de seus clientes”²¹.

Justamente em contextos como o anteriormente relatado é que pode haver um abuso na invasão de privacidade. Além da perda da intimidade, o indivíduo poderá ser discriminado, eliminado de um processo seletivo ou tolhido de uma cobertura de seguro de vida ou plano médico, entre outras situações. Deste modo, é claramente possível entender a necessidade de se ter meios efetivos para a proteção de dados pessoais, já que, normalmente, os indivíduos não sabem o que acontece com suas informações pessoais após inseri-las na internet e, tampouco que elas poderão ser usadas em seu desfavor.

Além de não saberem o destino dos seus dados, as pessoas também são facilmente atraídas desavisadamente. O download e a utilização de aplicativos ou compras por websites, dentre outras interatividades, geralmente são procedimentos muito rápidos, porque as empresas da economia digital não querem dificultar o ingresso do usuário. A lógica se baseia na conquista de uma grande movimentação de clientes a partir do acesso facilitado ao aplicativo ou à compra online. Então, pedir comida em casa, assistir a seriados, comprar produtos ou serviços somente agradará ao cliente pela praticidade. Caso seja preciso efetuar um cadastramento longo e cheio de textos e documentos, o cliente acaba desistindo. Para que seus produtos e serviços sejam consumidos de forma atrativa, as empresas simplificam o acesso a eles.

Contudo, o acesso a produtos e serviços de forma simplificada indica que usuários não estão se atentando para todas as condições de atendimento das empresas. Isso porque os termos de uso (que informam regras internas de funcionamento) e as políticas de privacidade (que informam sobre privacidade dos dados dos usuários) geralmente são longos²². À vista disso, não há atenção devida a esclarecimentos e avisos pertinentes, como preço, prazos, validade, requisitos e, principalmente, privacidade.

²¹ CASTELLS, *op. cit.*, p. 193.

²² Ver WAZE. **Waze Use Terms**. Disponível em: <https://www.waze.com/pt-BR/legal/privacyem>. Acesso em: 9 fev. 2021. E WAZE. **Waze Privacy Policy**. Disponível em: <https://www.waze.com/pt-BR/legal/tos>. Acesso em: 9 fev. 2021.

Toda página da internet, aplicativos, empresas em geral, deveriam ter uma política de privacidade contendo informações claras e transparentes, tendo em vista que ela representa a declaração da empresa a respeito do tratamento dos dados pessoais. Existem milhares de conexões entre empresas que oferecem entre si produtos e serviços para dar melhores insights, melhores perspectivas sobre seu consumidor e de como fazê-lo voltar a comprar. Ou seja, existe um mercado de marketing bastante criativo e com ferramentas bastante poderosas entre as empresas. Normalmente, o consumidor, pessoa física titular dos dados, não sabe dessa movimentação. Quando alguém fornece seus dados a uma empresa, na verdade pode estar compartilhando com várias outras. Por esse motivo, as políticas de privacidade são tão importantes e vão fornecer às pessoas transparência quanto ao tratamento de seus dados.

Um caso sintomático da obscuridade e complexidade na política de privacidade ficou conhecido por escândalo Cambridge Analytica.²³ Nas eleições estadunidenses de 2016, a campanha política de Donald Trump foi impulsionada por players do mercado que coletaram dados pessoais cruciais para a vitória, visto que conheciam eleitores potencialmente suscetíveis a mudar de opinião, e o faziam. Esse caso foi noticiado como escândalo, porque até então, usuários do Facebook não esperavam ter seus dados compartilhados e usados em uma campanha eleitoral.

Esclarecendo um pouco melhor os fatos, na plataforma do Facebook há diversos Quizzes, jogos interativos por meio de perguntas, como testes de personalidade e autoconhecimento. Normalmente o título instiga o jogador com perguntas como “Você tem uma boa inteligência emocional?”, “Com que grande líder você se parece?” ou “Que herói da Marvel você é?”. Existem vários players que desenvolvem esse tipo de conteúdo e os vinculam ao Facebook. No caso Cambridge Analytica, a coleta de dados foi feita através do Quiz “This is your digital life”, desenvolvido por um pesquisador de Cambridge que prometia mostrar para quem respondesse às questões, os amigos da rede social que mais

²³ FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. **Revista Direito em Debate**, n. 53, v. 29, p. 182-195, maio 2020. Disponível em: <https://doi.org/10.21527/2176-6622.2020.53.182-195>. Acesso em: 12 fev. 2021.

curtiram ou menos curtiram suas publicações. Assim, os dados coletados foram passados para a campanha eleitoral de Donald Trump.

Embora o fato aparente ser um vazamento de dados, na verdade houve uma relação jurídica entre as partes envolvidas, que não foi comunicada de maneira clara para os usuários do Facebook. O fato reforçou a busca em defesa da proteção dos dados pessoais.

Uma política de privacidade deveria conter detalhadamente todas as informações a respeito do fluxo de dados. Entretanto, utilizava-se uma linguagem sem clareza e recheada de conteúdo jurídico, dificultando a compreensão imediata e eficiente do público. Na verdade, o desafio da política de privacidade é justamente dar informação para o titular sem revelar totalmente a intenção do destino de seus dados.

Todos os grandes players da tecnologia têm essa política de privacidade, porém não é fácil de ser compreendida. Dessa forma, no escândalo Cambridge Analytica, embora a política de privacidade do Facebook mencionasse que os dados pessoais eram transmitidos a terceiros, não estava claro o suficiente para que os usuários soubessem que colaborariam com a campanha eleitoral do presidente dos Estados Unidos. Não é natural presumir que, ao acessar uma rede social, contribui-se com uma campanha política.

3 A PROTEÇÃO DOS DADOS PESSOAIS

Conforme visto até aqui, os avanços tecnológicos conquistados pela sociedade globalizada e cibernética, em especial os processos automatizados de tratamento e customização de dados pessoais, podem ser utilizados de modo a ferir direitos fundamentais. A causa disso é justamente a existência de exposição e a utilização indevida ou até abusiva de dados pessoais, consoante vários exemplos citados. “Daí resulta ser necessária a instituição de mecanismos

que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade”²⁴.

A rede Internet não pertence a ninguém, não pertence a qualquer indivíduo ou qualquer país, não pode ser entendida dentro dos princípios da posse e da propriedade. Ela é apenas um instrumento de comunicação em escala mundial e deve ser aberta e colaborativa. Se, em seus primórdios, a Internet gerou em algumas pessoas a fantasia de que nela se podia praticar uma liberdade quase absoluta, não há mais dúvidas de que hoje existe uma consciência de que ela precisa de regras, de disciplina legal e de segurança jurídica.²⁵

A privacidade e a proteção de dados pessoais são importantes para o início de algum controle sobre os passos e rastros deixados pelas pessoas, que são constantemente monitorados. Esses dados pessoais projetam identidades - quem são, como são vistos ou julgados - por isso tão importante serem protegidos. Proteção no sentido de ditar as regras, estabelecer o que pode ou não ser feito com essas informações, de forma a promover a ética nas relações sociais e o respeito à dignidade da pessoa humana.

A informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encerra toda a complexa problemática em torno dessa relação, porém pode servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade.²⁶

²⁴ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, n. 2, v. 12, p. 91-108, jul./dez. 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 10 fev. 2021. p. 92.

²⁵ ARAÚJO, Marcelo Barreto de. **Comércio eletrônico; Marco Civil da Internet; Direito Digital**. Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC, 2017. p. 83.

²⁶ DONEDA, *op. cit.*, p. 94.

Em maio de 2020, em julgamento histórico, o Supremo Tribunal Federal (STF) reconheceu a proteção de dados pessoais como um direito fundamental, simbolizando um grande avanço mediante a urgência que o tema demanda. O Tribunal, por maioria de votos, declarou a inconstitucionalidade da Medida Provisória n. 954/2020, que previa o compartilhamento de dados dos usuários de serviços de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para a produção de estatísticas durante a pandemia do novo coronavírus.²⁷

O acórdão dispõe que “a proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, que envolvem uma tutela jurídica e âmbito de incidência específicos”²⁸. Além disso, deixa claro que o entendimento foi extraído da “interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do habeas data (art. 5º, LXXII), todos previstos na Constituição Federal de 1988”²⁹.

Ademais, em seu voto, o Ministro Luís Roberto Barroso elencou as seguintes medidas necessárias a serem adotadas para que o compartilhamento de dados pessoais - para fins de produção de estatísticas, de acordo com o caso -, fosse compatível com o direito à privacidade:

- 1) a finalidade da pesquisa for precisamente delimitada;
- 2) o acesso for permitido na extensão mínima necessária para a realização dos seus objetivos;
- 3) forem adotados procedimentos de segurança suficientes para prevenir riscos de acesso desautorizado, vazamentos acidentais ou utilização indevida.³⁰

²⁷ BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Ação Direta de Inconstitucionalidade 6387/DF - Distrito Federal. Relatora: Ministra Rosa Weber. **Pesquisa de Jurisprudência**, Acórdãos, 7 maio 2020. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf>. Acesso em: 11 fev. 2021.

²⁸ (ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11-11-2020 PUBLIC 12-11-2020).

²⁹ *Ibidem*.

³⁰ *Ibidem*, p. 50.

A importância do direito fundamental à proteção de dados pessoais vai além da proteção à esfera privada. Ele gera confiança nos cidadãos, no fomento de políticas públicas e nas atividades comerciais que fazem uso de dados para seus modelos de negócios. Assim, conforme assegura Bruno Ricardo Bioni, “a proteção de dados pessoais permite disciplinar a liberdade, a inovação e o desenvolvimento. E, em um cenário em que dados pessoais projetam a maneira como cada indivíduo é visto no mundo, permite também o exercício de direitos e da cidadania”³¹. Ele continua seu raciocínio dizendo que, “historicamente, normas de proteção de dados pessoais sempre tiveram a dupla função de não só garantir a privacidade e outros direitos fundamentais, mas também fomentar o desenvolvimento econômico”³².

No Brasil, até 2018, não havia uma lei específica para falar de proteção de dados. O que havia até então era uma série de normas, diretrizes, portarias, comunicações, orientações e até algumas leis esparsas que, de alguma forma, abordam de forma genérica e tangencial o tema.

O Código de Defesa do Consumidor³³, por exemplo, dispõe sobre banco de dados e cadastros de consumidores, entretanto, é mais voltada para a perspectiva do consumidor, o que não engloba muitos outros casos que envolvem dados pessoais. A própria Constituição Federal³⁴ trata dos direitos à privacidade e à intimidade e do sigilo das comunicações telefônicas e de dados, conforme se depreende de uma leitura do artigo 5º, embora a palavra privacidade não esteja expressa. Ainda, o Código Penal³⁵ visa coibir a inserção de dados falsos em sistemas de informática ou banco de dados da Administração Pública, bem como proteger a violação de informações sigilosas e de dispositivos

³¹ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. p. 108.

³² BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. p. 108.

³³ BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 9 fev. 2021.

³⁴ BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988. **Diário Oficial da União**, Poder Legislativo, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm. Acesso em: 9 fev. 2021.

³⁵ BRASIL. Decreto-Lei n. 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Poder Executivo, Rio de Janeiro, RJ, 7 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 9 fev. 2021.

informáticos, este inserido, em 2012, pela Lei nº 12.737³⁶, conhecida como Lei Carolina Dieckmann. Por fim, a Lei nº 12.965/2014, ou Marco Civil da Internet, que “estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil”³⁷.

Em 2018, surgiu a Lei nº 13.709³⁸ ou Lei Geral de Proteção de Dados (LGPD) para dar um norte a questões especificamente envolvendo tratamento e proteção de dados pessoais. Havendo normas em contrário, normas mais específicas ou situações que extrapolam a generalidade dessa lei, será preciso analisar com cautela e recorrer a interpretações, decidindo-se pela aplicação da lei anterior ou posterior, a lei genérica ou mais específica - todos os mecanismos e ferramentas para solucionar conflitos de normas. Contudo, a Lei Geral de Proteção de Dados está posta, portanto, é necessário entendê-la.

As leis de proteção de dados minaram ao redor do mundo em razão dos cenários já relatados. Na década de noventa, a União Europeia já demonstrava preocupação com o assunto, pois se descobriu que a interação entre indivíduos e tecnologia ocasionava situações de violação da privacidade. Na época, uma diretiva foi editada para tratar de proteção de dados pessoais. A Diretiva 46/1995³⁹ vigorou por mais de vinte anos e, como diz o nome, era um direcionamento para que os países integrantes da União Europeia atuassem conforme algumas regras e pudessem dar maior clareza sobre o tratamento dos

³⁶ BRASIL. Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm#art2. Acesso em: 9 fev. 2021.

³⁷ BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm#art32. Acesso em: 9 fev. 2021.

³⁸ BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Poder Executivo, Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 9 fev. 2021.

³⁹ UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e Conselho da União Europeia, de 24 de outubro de 1995. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**, Parlamento Europeu e Conselho da União Europeia, Luxemburgo, 24 out. 1995. Disponível em: <http://data.europa.eu/eli/dir/1995/46/oj>. Acesso em: 9 fev. 2021.

dados pessoais toda vez que isso fosse feito, em especial com o uso de recursos tecnológicos.

A discussão, na União Europeia, foi amadurecendo com o tempo e várias instâncias foram sendo provocadas, inclusive o Parlamento Europeu. Em 2016, foi aprovado o General Data Protection Regulation (GDPR)⁴⁰, que entrou em vigor em maio de 2018. O surgimento do GDPR foi importantíssimo para que, no Brasil, a Lei Geral de Proteção de Dados viesse à tona, porque entendeu-se que as interações da economia digital – de uma leitura através do big data – eram desconhecidas pelos indivíduos e violadoras de direitos fundamentais.

Pouco antes do Marco Civil ser aprovado, em 2013, Edward Snowden, agente da National Security Agency (NSA), dos Estados Unidos, revelou para o mundo a existência de um esquema de espionagem internacional. A partir de um software utilizado pelo governo estadunidense, líderes de Estados por todo o mundo eram vigiados secretamente. Naquela ocasião, falava-se, inclusive, que a presidente do Brasil, Dilma Rousseff, fora alvo dessa espionagem. Diante disso, o projeto de lei acabou sendo sancionado em uma espécie de resposta ao escândalo Snowden.

Em 2015, o Ministério da Justiça abriu, pela segunda vez, uma consulta pública⁴¹ e nova rodada de perguntas foi feita a respeito de como deveria ser um projeto de lei sobre a temática em questão. Logo após, em 2016, foi aprovado o General Data Protection Regulation, na União Europeia, que entrou em vigor a partir de 2018, ano em que veio à tona o escândalo Cambridge Analytica e, em sequência, o surgimento da Lei Geral de Proteção de Dados no Brasil.

O que vem à mente das pessoas quando se fala em proteção de dados são situações referentes a vazamentos. Comumente manchetes informam sobre

⁴⁰ UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 9 fev. 2021.

⁴¹ BRASIL. Ministério da Justiça e Cidadania. Pensando o Direito, 2007. **Debates públicos**. Governo Federal, Secretaria de Assuntos Legislativos. Disponível em: <http://pensando.mj.gov.br/debates/>. Acesso em: 9 fev. 2021.

clientes querendo processar empresas em razão de vazamento de dados. Os temas realmente estão relacionados, pois os dados eventualmente vazados deveriam estar, de certa forma, protegidos.

Contudo, o surgimento da Lei de Proteção de Dados não veio apenas em razão de vazamentos. A questão de customizar perfis não é propriamente um vazamento, mas um acordo comercial entre as empresas que vão fazer leitura conjunta de dados para oferecer produtos e serviços mais personalizados. Embora os vazamentos existam com bastante frequência e a proteção de dados deva coibir ao máximo esses eventos, a LGPD está longe de ser uma lei que trata exclusivamente deste tipo de problema.

A Lei n. 13.709/2018 é uma lei que exige nova postura na cultura interna das empresas, para que elas adotem certas práticas ao realizarem tratamento de dados pessoais, portanto, uma lei de governança e compliance, possíveis práticas adotadas por empresas, que dizem respeito ao seu funcionamento interno, e que valorizam, conseqüentemente, sua imagem. Governança e compliance têm estrita relação com políticas, normas, regras e padrões, na medida em que se deve estar em conformidade com elas.

Ademais, a nova lei não é detalhista em processos e ferramentas, ou seja, não existe uma lista que prevê com detalhes todas as práticas ou ações para todas as circunstâncias internas. Entretanto, ela estabelece, de maneira geral, princípios a serem respeitados e direitos e deveres a serem seguidos (contemplando hipóteses de legalidade para o tratamento de dados).

Conseqüentemente, a Lei Geral de Proteção de Dados se preocupa com a coleta (presencial, por telefone, e-mail, aplicativo, etc.), armazenamento, processamento e utilização dos dados pessoais. Logo, para que uma empresa tenha um programa efetivo de proteção de dados pessoais em consonância com a lei, deverá fazer um grande mapeamento dos bancos de dados de todos os setores dentro dela.

4 A IMPORTÂNCIA DA FINALIDADE E DA FISCALIZAÇÃO PARA A PROTEÇÃO DOS DADOS PESSOAIS

Até este ponto podemos entender a extrema quantidade de informações pessoais que são produzidas no universo digital e que a sua leitura massiva é um importante combustível para a economia da sociedade atual. Por serem expressão da personalidade dos indivíduos e, considerando os riscos de serem ilícita e abusivamente utilizados, os dados pessoais devem ser protegidos para uma efetiva tutela da dignidade da pessoa humana.

Ademais, feitas as considerações sobre o reconhecimento da proteção de dados pessoais como um direito fundamental e sobre o que a LGPD representa, é importante destacar que os princípios que regem a lei vão fortalecer a cultura de proteção das informações pessoais.

No artigo 6º está elencado o rol de dez princípios contemplados pela lei. Dentre eles estão os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.⁴²

O princípio da finalidade (inciso I) é definido pela “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”⁴³. Compreende-se que a finalidade vai reger todo o fluxo de dados, devendo ela ter um propósito dentro da legalidade, não ser genérica e tampouco encoberta do titular. Estão intimamente ligados a ela os princípios da adequação (inciso II), da necessidade (inciso III) e da qualidade dos dados (inciso V).

O tratamento de dados deve ocorrer em compatibilidade (adequação) com a finalidade, limitado ao mínimo necessário (necessidade), ou seja, de forma

⁴² BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Poder Executivo, Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 9 fev. 2021.

⁴³ *Ibidem*.

proporcional e sem excessos em relação à finalidade e dotado de exatidão, clareza, relevância e atualização para que se cumpra essa finalidade estabelecida. Ademais, o princípio da não discriminação (inciso IX) também está relacionado com a finalidade, pois, devendo ser ela legítima, seria impossível realizar um tratamento de dados para fins discriminatórios ou abusivos.⁴⁴

Os princípios do livre acesso (inciso IV) e da transparência (inciso VI) são garantias aos titulares dos dados pessoais de que terão uma consulta facilitada e gratuita sobre a forma e duração do tratamento e sobre a integralidade de seus dados pessoais, sendo que essas informações necessariamente deverão ser claras e precisas.⁴⁵

Por fim, os princípios da segurança (inciso VII), prevenção (inciso VIII) e responsabilização e prestação de contas (inciso X) são medidas a serem adotadas pelo agente de tratamento (controlador e operador). A segurança requer técnica e administração para que não ocorram acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão dos dados pessoais. A prevenção requer medidas para o impedimento de danos em virtude do tratamento de dados pessoais. Além disso, é necessário que o agente demonstre a existência e a efetividade do programa de proteção de dados pessoais.⁴⁶ A efetividade depende da demonstração de tudo que é feito, ou seja, deve estar tudo documentado e, de fato, incorporado à cultura da empresa.

Muito tem sido falado - e dada a devida importância - em relação ao consentimento do titular dos dados pessoais para a realização de tratamento pelos agentes. O consentimento vem definido na lei como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”⁴⁷ (artigo 5º, XII).

⁴⁴ *Ibidem*.

⁴⁵ BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Poder Executivo, Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 9 fev. 2021.

⁴⁶ *Ibidem*.

⁴⁷ *Ibidem*.

Desde que a Lei Geral de Proteção de Dados foi aprovada, notícias e postagens buscaram informar às pessoas, como um alerta, sobre eventuais violações às quais seus dados possam estar expostos. Em sua maioria, as notícias enfatizam somente a invasão da privacidade, na intenção de advertir o titular dos dados pessoais e o agente de tratamento. Com isso, vem ocorrendo uma hipervalorização do consentimento. Por hipervalorização do consentimento entende-se a disseminação de uma compreensão equivocada de que a anuência do titular seria a única forma capaz de permitir que o agente de uma empresa realize o tratamento de suas informações pessoais.

Dessa forma, enquanto o titular passou a acreditar que seus dados estariam protegidos de qualquer tratamento se não houvesse o seu consentimento, as empresas entenderam estar condicionadas às decisões do titular.

Com essa perspectiva, o desafio é divulgar a importância de não se ter apenas um olhar negativo e desanimador com as questões envolvendo tratamento de dados pessoais, mas um olhar positivo aos meios, que possibilitem uma boa relação com essa questão. Como já mencionado em momento anterior, a sociedade atual depende desse processamento de informações pessoais, pois são fundamentais para o desenvolvimento econômico, seja para oferecer a melhor relação possível entre cliente e produto/empresa ou mesmo para o aprimoramento de políticas públicas.

Em vista disso, entende-se que o mais adequado é ter uma proteção de informações pessoais que gere confiança. Ou seja, antes de se preocupar somente com o consentimento, uma atenção deve ser dada para outros instrumentos que vão impedir a superexposição indevida de perfis e, ao mesmo tempo, disciplinar a conduta de emprego de dados pessoais. Um mapeamento e planejamento com qualidade e transparência faria as pessoas confiarem com mais tranquilidade nos gerenciadores de dados pessoais.

Nesse sentido, é indispensável difundir e enaltecer com mais afinco a importância da finalidade para o tratamento de dados, que tem sido ignorada. A definição do fluxo de dados - para que estão sendo tratados determinados dados,

qual o propósito e destinação - é circunstância que necessariamente deve estar bem esclarecida na política das empresas. Somente assim gera-se confiança, levando as pessoas a compartilharem seus dados e consentirem para os mais variados tipos de tratamento. Além disso, as empresas vão desfrutar de boa reputação, vantagem competitiva e bom relacionamento com terceiros.

Não foi em vão que a própria Lei Geral de Proteção de Dados destacou a finalidade como um princípio (artigo 6º, I) e, como visto, outros princípios (artigo 6º, II, III, e V) estão intimamente ligados a ela. Tão grande sua importância, vários outros artigos da lei se referem à finalidade, por exemplo, a própria definição de consentimento (artigo 5º, XII). Além disso, o STF destacou a finalidade precisamente delimitada como uma medida necessária a ser adotada para um compartilhamento de informações pessoais compatível com o direito à privacidade. Em vista do exposto, considera-se a finalidade um importante instrumento previsto na LGPD para a concretização da proteção de dados pessoais, e assim vemos no acórdão do Supremo Tribunal Federal:

O tratamento e compartilhamento de informações devem respeitar direitos e garantias individuais, sendo precedidos de uma adequada especificação das finalidades e medidas de segurança. Como observado pelo Tribunal Constitucional alemão no julgamento da Lei do Censo de 1983, perfeitamente transponível ao caso ora analisado, o Estado deve coletar somente a informação que seja realmente necessária para as finalidades legais [...].⁴⁸

Por outra via, não será um fiscal que vai de porta em porta fiscalizar cada empresa que está se adequando às normas de proteção aos dados pessoais. Quem deve fiscalizar é o próprio titular dos dados ou mesmo as próprias empresas ao solicitarem e cobrarem a política de proteção de privacidade uma das outras.

⁴⁸ (ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11-11-2020 PUBLIC 12-11-2020) p. 72.

Então, o titular dos dados que vai a uma rede de supermercados ou uma rede de drogarias, faz uso de um plano de saúde, de uma linha telefônica celular ou de uma TV a cabo, ou seja, que vai fazer grande movimentação de informações pessoais, ele mesmo deve questionar essas empresas. Na medida em que elas não cumprirem a lei, o titular poderá chamar órgãos responsáveis por essa tutela, como o Ministério Público, o PROCON e a Agência Nacional de Proteção de Dados (ANPD), para que dêem concretude à defesa do seu direito.

Tratando-se das relações interempresariais, muitas vezes as empresas não fazem diligências para saber quem é aquele terceiro com quem vai negociar. Geralmente, não se questionam as práticas internas a respeito de segurança da informação e o acesso e processamento de dados pessoais. Então, com o surgimento da Lei Geral de Proteção de Dados, é urgente que exista uma cobrança de adequação à proteção dos dados das pessoas, cujo objetivo seria promover uma cultura de conscientização ou mesmo de fiscalização.

Em perspectiva, tem-se uma inversão na lógica da fiscalização na medida em que será exercida pelos próprios personagens do mercado de informações, tanto pelos titulares de dados pessoais quanto pelos agentes de tratamento, e não por órgãos encarregados. A partir disso, espera-se uma mudança de postura por toda a sociedade também no âmbito da fiscalização, que será um instrumento eficaz para tutelar a liberdade, a privacidade, os dados pessoais e para promover a inovação, o desenvolvimento e a cidadania.

CONSIDERAÇÕES FINAIS

A primeira vez que o direito à privacidade apareceu conceituado foi no ano de 1890 no texto “The Right to Privacy”⁴⁹, de Samuel Warren e Louis Brandeis. Na época, a privacidade surgiu como direito ao isolamento ou direito

⁴⁹ WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=28#metadata_info_tab_contents. Acesso em: 4 mar. 2021.

de estar só.⁵⁰ Mas, em um novo contexto social, globalizado e cibernético, seria essa concepção de privacidade pela qual se pretende lutar? A sociedade mudou muito, de maneira que, ao lado da privacidade, a proteção de dados pessoais tornou-se cada vez mais uma necessidade.

Na atual sociedade da informação, dados pessoais são tratados para as mais diferentes finalidades, tornando-se a engrenagem para muitos negócios, em especial no universo digital. Destaca-se a importância de se ter um olhar crítico e entender os pontos negativos da utilização das informações pessoais por empresas e governos, mas também os benefícios que podem ser retirados do big data, como a personalização de experiências, o desenvolvimento de inovação e aprimoramento de políticas públicas.

Depois de tantos escândalos envolvendo vazamentos e comercialização de informações pessoais, é de suma importância notar a maturidade com que a temática vem sendo tratada na Ciência Jurídica.

Assim, de maneira otimista, o surgimento da Lei Geral de Proteção de Dados possibilitará uma mudança cultural em relação à proteção de dados pessoais. Os titulares de dados terão a chance de despertar-se para que conheçam mais seus direitos e o valor que possuem e, portanto, exercê-los, fiscalizá-los e defendê-los, principalmente com o reconhecimento da proteção de dados pessoais como um direito fundamental autônomo. Por outro lado, os agentes que controlam o tratamento de informações pessoais deverão respeitar limites e planejar políticas internas adequadas aos deveres impostos pela lei, proporcionando mais informação e transparência.

Dessa forma, finalidade(s) bem delimitada(s) pelos agentes de tratamento de dados pessoais e fiscalização, seja por parte dos titulares desses dados e/ou das empresas, foram considerados instrumentos imprescindíveis para a efetiva proteção de dados pessoais e, conseqüentemente, para promover a confiança nas pessoas e nas relações interempresariais.

⁵⁰ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. p. 102.

A lei trouxe instrumentos poderosos e essenciais para um futuro mais equilibrado em relação à utilização de informações processadas, já que dados formam o alicerce de uma nova economia. E não são quaisquer dados, são justamente aqueles retirados de pessoas humanas, que têm sua dignidade a ser respeitada.

Por fim, o estudo demonstra a relevância de um tema pelo qual vale se interessar, conhecer a fundo e lutar em defesa de direitos.

REFERÊNCIAS

ARAÚJO, Marcelo Barreto de. **Comércio eletrônico; Marco Civil da Internet; Direito Digital**. Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC, 2017.

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

BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988. **Diário Oficial da União**, Poder Legislativo, Brasília, DF, 5 out. 1988.

Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm.

Acesso em: 9 fev. 2021.

BRASIL. Decreto-Lei n. 2.848, de 7 de dezembro de 1940. Código Penal.

Diário Oficial da União, Poder Executivo, Rio de Janeiro, RJ, 7 dez. 1940.

Disponível em: [http://www.planalto.gov.br/ccivil_03/decreto-](http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm)

[lei/del2848compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm). Acesso em: 9 fev. 2021.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**, Poder

Executivo, Brasília, DF, 11 set. 1990. Disponível em:

http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 9 fev.

2021.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de

dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 30 nov. 2012. Disponível em:

http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm#art2.

Acesso em: 9 fev. 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. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 23 abr. 2014. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm#art32. Acesso em: 9 fev. 2021.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Poder Executivo, Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 9 fev. 2021.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Ação Direta de Inconstitucionalidade 6387/DF - Distrito Federal. Relatora: Ministra Rosa Weber. **Pesquisa de Jurisprudência**, Acórdãos, 7 maio 2020. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf>. Acesso em: 11 fev. 2021.

BRASIL. Ministério da Justiça e Cidadania. Pensando o Direito, 2007. **Debates públicos**. Governo Federal, Secretaria de Assuntos Legislativos. Disponível em: <http://pensando.mj.gov.br/debates/>. Acesso em: 9 fev. 2021.

CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

COLOMÉ, Jordi Pérez. “Criei o Waze para resolver a perda de tempo no trânsito, mas agora vejo que o problema é pior”. **El país**, 14 out. 2019. Disponível em: https://brasil.elpais.com/brasil/2019/10/10/tecnologia/1570717218_742251.html#:~:text=O%20Google%20comprou%20o%20Waze,bilh%C3%B5es%20de%20reais. Acesso em: 5 fev. 2021.

CUKIER, Kenneth; MAYER-SCHOENBERGER, Victor. The Rise of Big Data: how it's changing the way we think about the world. **Foreign Affairs**, [S.], n. 3, v. 92, may/june 2013. Disponível em: <https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data>. Acesso em: 9 fev. 2021.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, n. 2, v. 12, p. 91-108, jul./dez. 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 10 fev. 2021.

DONEDA, Danilo. **Da privacidade à Proteção de Dados**. Rio de Janeiro: Renovar, 2006.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. **Revista Direito em Debate**, n. 53, v. 29, p. 182-195, maio 2020. Disponível em: <https://doi.org/10.21527/2176-6622.2020.53.182-195>. Acesso em: 12 fev. 2021.

JUDENSNAIDER, Elena; LIMA, Luciana; ORTELLADO, Pablo; POMAR, Marcelo. **Vinte centavos**: a luta contra o aumento. São Paulo: Editora Veneta, 2013.

LESSIG, Lawrence. **Code**: version 2.0. Nova Iorque: Basic Books, 2006.

MACHADO, Diego; DONEDA, Danilo. Direito ao anonimato na internet: fundamentos e contornos dogmáticos de sua proteção no direito brasileiro. (Outubro 20, 2018). **Revista de Direito Civil Contemporâneo**, [no prelo/forthcoming]. Disponível em: <https://ssrn.com/abstract=3698938>. Acesso em: 6 fev. 2021.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Técnicas de pesquisa**. 5. ed. São Paulo: Atlas, 2002.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Org). **Direito digital**: direito privado e internet. 2. ed. São Paulo: Editora Foco, 2019.

NETTO, Adhemar Della Torre; OLIVEIRA, Alfredo Emanuel Farias de. Big Data e proteção de direitos fundamentais: perigos da má utilização da técnica e uma proposta para o resgate do ideal sofista de paideia no campo da educação. **Revista de Direito e as Novas Tecnologias**, [S.l.], n. 3, v. 2, abr./jun. 2019.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**, Luxemburgo, 24 out. 1995. Disponível em: <http://data.europa.eu/eli/dir/1995/46/oj>. Acesso em: 9 fev. 2021.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 27 abr. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 9 fev. 2021.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=28#metadata_info_tab_contents. Acesso em: 4 mar. 2021.

WAZE. **Waze Use Terms**. Disponível em: <https://www.waze.com/pt-BR/legal/privacyem>. Acesso em: 9 fev. 2021.

WAZE. **Waze Privacy Policy**. Disponível em: <https://www.waze.com/pt-BR/legal/tos>. Acesso em: 9 fev. 2021.