

**PERFIS INFORMACIONAIS E PUBLICIDADE
COMPORTAMENTAL: DIREITO À AUTODETERMINAÇÃO
INFORMATIVA E A PROTEÇÃO DE DADOS PESSOAIS
NO AMBIENTE VIRTUAL**

**INFORMATIONAL PROFILES AND BEHAVIORAL ADVERTISING:
RIGHT TO INFORMATIVE SELF-DETERMINATION AND PROTECTION
OF PERSONAL DATA IN THE VIRTUAL ENVIRONMENT**

Raíssa Arantes Tobbin¹

Valéria Silva Galdino Cardin²

RESUMO

O presente artigo tem por objetivo analisar o direito à autodeterminação informativa, um direito fundamental e de personalidade, e a proteção de dados pessoais do usuário no ambiente virtual, tendo em vista a possibilidade de criação de perfis informacionais e de veiculação de publicidade comportamental. Para tanto, o trabalho utilizou o método hipotético-dedutivo, fundamentado em pesquisa e revisão bibliográfica de obras, artigos de periódicos, legislação, doutrina e jurisprudência aplicáveis ao caso. Como resultado, verificou-se que a criação de perfis informacionais e a veiculação de publicidade comportamental é cada vez mais frequente no ambiente virtual, mediante a coleta e o tratamento de dados pessoais do usuário. Neste sentido, é fundamental que o usuário tenha conhecimento e consinta acerca deste contexto, de forma a ter a sua privacidade, seus dados pessoais e seu direito à autodeterminação informativa respeitados, especialmente diante da possibilidade de compartilhamento de informações com empresas privadas e com o Estado.

PALAVRAS-CHAVE: Autodeterminação Informacional. Lei Geral de Proteção de Dados (LGPD). Direitos da Personalidade.

ABSTRACT

The purpose of this article is to analyze the right to informational self-determination, a fundamental and personality right, and the protection of the user's personal data in the virtual environment, in view of the possibility of creating informational profiles and serving

¹ Mestranda em Ciências Jurídicas pela Universidade CESUMAR; Graduada em Direito pela Universidade Paranaense (UNIPAR); Graduada em Letras – Português/Espanhol pela Universidade Estadual de Ponta Grossa (UEPG); Advogada no Paraná. Email: tobbinraissa@hotmail.com

² Pós-Doutora em Direito pela Universidade de Lisboa; Doutora e mestre em Direito das Relações Sociais pela Pontifícia Universidade Católica de São Paulo (PUCSP); Docente da Universidade Estadual de Maringá e no Programa de Pós-Graduação de Doutorado e Mestrado em Ciências Jurídicas pela Universidade CESUMAR; Pesquisadora pelo ICETI; Advogada no Paraná. Email: valeria@galdino.adv.br

behavioral advertising. For this, the work used the hypothetical-deductive method, based on research and bibliographic review of works, periodical articles, legislation, doctrine and jurisprudence applicable to the case. As a result, it was found that the creation of informational profiles and the transmission of behavioral advertising is increasingly frequent in the virtual environment, through the collection and treatment of the user's personal data. In this sense, it is essential that the user has knowledge and consents about this context, in order to have their privacy, personal data and their right to informational self-determination respected, especially in view of the possibility of leakage and sharing of information with private companies and with the State.

KEYWORDS: Informational Self-Determination. Personality Rights. General Data Protection Act (LGPD).

1 INTRODUÇÃO

Na sociedade pós-moderna, o domínio da informação passa cada vez mais a ser sinônimo de conhecimento, estratégia e poder. Além disso, a utilização da Internet, das redes sociais e dos demais aplicativos e dispositivos digitais é exponencialmente incentivada e necessária, inclusive para o exercício da cidadania. Neste cenário, todos os dias as pessoas entram em redes sociais, realizam compras on-line, se identificam, informam dados pessoais em sites e aplicativos e concordam com os termos de uso destes dispositivos.

O que se questiona é se o cidadão tem a real dimensão acerca de como os seus dados estão sendo utilizados no meio virtual e de qual o alcance desta vigilância digital. Quais dados estão sendo coletados? Como serão tratados? Poderão ser compartilhados com empresas privadas ou com o Estado? Estes dados não podem ser utilizados contra o próprio usuário no futuro? Tal temática ganha delineamento diante da possibilidade de criação de perfis comportamentais e informacionais – que seriam de grande valia para empresas privadas e para o Estado, diante da eventualidade de um Estado de vigilância.

Neste sentido, verifica-se que cresce a necessidade de proteção aos direitos fundamentais e de personalidade do indivíduo que utiliza o meio virtual, especialmente quanto à tutela de sua privacidade e, mais especificamente, em relação aos seus dados pessoais, tendo em vista o cenário atual de formação de *commodities* informacionais e ativos comerciais com base em dados pessoais coletados em rede.

Logo, o objetivo deste trabalho é analisar o direito à autodeterminação informativa, um direito fundamental e de personalidade, e a proteção de dados pessoais no meio digital, diante da necessidade de tutela do cidadão quanto à coleta, o armazenamento, o

tratamento e o compartilhamento destes dados. Para tanto, o presente trabalho utilizou o método hipotético-dedutivo, fundamentado em pesquisa e revisão bibliográfica de obras, artigos de periódicos, legislação, especialmente a Lei Geral de Proteção de Dados (LGPD), doutrina e jurisprudência aplicáveis ao caso.

2 COLETA DE DADOS NO AMBIENTE VIRTUAL E OS RISCOS DE PERFIS INFORMACIONAIS E DA PUBLICIDADE COMPORTAMENTAL

É parte do cotidiano do usuário do ambiente virtual o fornecimento e o preenchimento de uma série de formulários com seus dados pessoais para o acesso às facilidades proporcionadas pela Internet. Contudo, muitas vezes tais dados podem ser utilizados em desfavor do indivíduo, de forma a ofender seus direitos fundamentais e de personalidade, expondo-o a práticas discriminatórias com base na criação de perfis comportamentais e informacionais. Neste sentido, fundamental é investigar como se dá a coleta, o armazenamento e o tratamento dos dados coletados em rede.

De acordo com Doneda, atualmente, a informação, em si, “está ligada a uma série de fenômenos que cresceram em importância e complexidade de forma marcante nas últimas décadas”. Desta forma, “o que hoje a destaca de seu significado histórico é uma maior desenvoltura na sua manipulação, desde a coleta e tratamento até a comunicação da informação” e, uma vez ampliadas as capacidades de “armazenamento e comunicação de informações, cresce também a variedade de formas pelas quais ela pode ser apropriada ou utilizada”. (DONEDA, 2011, p. 92).

Como destacam Oliveira, Barros e Pereira, “a amplitude cada vez maior dos canais informacionais e comunicacionais pela Internet fazem com que muitos setores da sociedade se estruturam e também levem os indivíduos a divulgarem ou compartilharem seus dados pessoais” na rede, “espontaneamente ou captados por empresas ou geradoras informáticas que se utilizam desses dados para fins pacíficos ou prejudiciais, para o Estado e para o usuário”. (OLIVEIRA; BARROS; PEREIRA, 2017, p. 573).

Desta forma, para Doneda, “os bancos de dados que contêm dados pessoais, tão comuns em nossos dias, proporcionam uma nova definição dos poderes e direitos a respeito das informações pessoais e, conseqüentemente, sobre a própria pessoa”. Fato que “aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros”, perspectiva que “faz com que o estatuto jurídico desses dados se

torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo”. (DONEDA, 2011, p. 93). Conforme observa Roque:

os dados pessoais, na sociedade contemporânea, assumem importância estratégica cada vez maior. Podem ser utilizados em inúmeras aplicações, como o direcionamento de propagandas e anúncios específicos para o perfil de determinado consumidor, a partir das páginas que este visita na internet, ou a identificação da preferência ideológica ou mesmo sexual mediante análise dos gastos realizados pelo cartão de crédito, ou a investigação de doenças com maior probabilidade de se manifestarem durante a vida de determinado indivíduo, por meio da análise de seu material genético. Os exemplos são praticamente inesgotáveis e, cada vez mais, presentes no cotidiano – basta lembrar de seu smartphone, que sugere trajetos para o trabalho mesmo nos feriados. (ROQUE, 2019, p. 2).

Como pontuam Finkelstein, Federighi e Chow (2020, p. 2), os dados passaram a ser “um ativo de *marketing* indispensável em tempos de pandemia da COVID-19, uma vez que grande parte da população mundial está isolada em casa, sendo mais suscetível a receber publicidade por via digital”.

Para Machado e Ruaro, “a figura da publicidade desempenha, hoje, papel fundamental na lógica do consumo. Mais do que veicular informações acerca de um determinado produto, a publicidade tem o condão de despertar o desejo pelo mesmo”. Uma vez que “ela cria tendências, opiniões e até mesmo “necessidades” antes inexistentes, de modo que a sua utilização influencia diretamente no mercado”. Segundo os autores, atualmente, a “publicidade é pressuposto indispensável à atual lógica de consumo; publicidade e consumismo são dois fatores indissociáveis e extremamente presentes no cenário socioeconômico atual”. (MACHADO; RUARO, 2017, p. 422).

Segundo Souza e Amaral, “os *cookies* podem oferecer praticidade na navegação, porém, também têm potencial de trazer riscos à proteção dos dados do usuário, principalmente se o uso do dispositivo em que é feita a navegação é compartilhado”. Ainda, no que diz respeito aos *cookies* de terceiros, “suas funcionalidades são, basicamente, voltadas para a chamada publicidade comportamental, também conhecida como *behavioral advertising*”. (SOUZA; AMARAL, 2020).

O rastreamento de navegação “pode acarretar mapeamento do comportamento do usuário online, tornando-o suscetível às ações de *marketing* para as quais não deseja ser alvo”. É o caso do usuário que “navega em determinado site à procura de um serviço ou produto “X” e, após, no decorrer dos dias e de outras navegações, é “magicamente” bombardeado por propagandas de “X”. Isso ocorre porque por meio do registro de navegação (e da utilização de *cookies*), “os anúncios publicitários são personalizados, atrelando com precisão a abordagem

ao perfil do potencial consumidor”. Quando o usuário “navega na internet, há uma série de cliques que revelam informações sobre suas predileções, reduzindo os custos da ação publicitária”. (BIONI, 2019 *apud* SOUZA; AMARAL, 2020).

Tal prática possui grande relevância comercial hodiernamente, uma vez que os dados dos consumidores se transformam em verdadeiros elementos críticos para a publicidade e venda de bens de consumo. Com o avanço tecnológico, “permitiu-se a criação de perfis cada vez mais intrusivos sobre o potencial consumidor, monitorando-se constantemente o seu comportamento, a ponto de inferir [...] o seu estado emocional”, para “correlacioná-lo à mensagem publicitária”. (BIONI, 2019 *apud* SOUZA; AMARAL, 2020).

Assim, “os dados dos consumidores são colhidos a fim de se criar um perfil comportamental para que a publicidade seja direcionada baseada na forma como determinado consumidor age quando realiza compras”. Tem-se, assim, “a possibilidade de ter informações individualizadas sobre os consumidores, permitindo a ele guiar o fluxo informacional e a publicidade de forma particular para cada um”. (MAGRANI, 2019, p. 70-71).

Este processamento de dados não é tido como uma prática ilegal, contudo, inúmeras vezes o uso dos *cookies* “não é consentido pelo usuário, que não consegue ter clareza de que está sendo monitorado, tampouco sabe como adotar medidas que impeçam o rastreamento de sua navegação e comportamento online”. (SOUZA; AMARAL, 2020). Como pontua Camurça (2020, p. 124), “a inclusão digital ainda não é uma realidade global e, algumas técnicas como excluir *cookies*, visitar sites em modo anônimo e buscar ferramentas de DNT” são tarefas “difíceis para uma maioria dos usuários brasileiros. Nisto, o risco de manipulação se acentua”.

Conforme Magrani, “a publicidade comportamental é capaz de aumentar a assimetria de informação na relação de consumo, potencializar a discriminação entre os consumidores, minimizar a capacidade de escolha livre e autônoma do consumidor”, dentre outras consequências. (MAGRANI, 2019, p. 70-71). Portanto, de acordo com os hábitos e as preferências do usuário, pode ser “útil ou inoportuna, conforme diferentes entendimentos pessoais, mas que na prática pode ser considerada invasão de privacidade”. (ARAÚJO; CAVALHEIRO, 2014, p. 220).

Um dos casos paradigmas no cenário internacional acerca da necessidade de proteção de dados pessoais do usuário no ambiente virtual é o da compra pela empresa de consultoria *Cambridge Analytica* de dados de mais de 50 milhões de perfis da rede social

Facebook, tendo por objetivo a manipulação política das eleições presidenciais americanas de 2016 na esfera pública por meio da rede, mediante o envio de “mensagens direcionadas a eleitores específicos, manipulando sua opinião política através de um algoritmo que conseguia analisar os perfis individuais e determinar traços de personalidade ligados ao comportamento online do eleitor”, assim como “seus sentimentos e medos, direcionado o conteúdo de manipulação sociopolítica com base nesses fatores”. (MAGRANI, 2019, p. 161).

Tal contexto apenas evidencia que “o acesso à internet é, hoje, uma das principais fontes de dados para a publicidade comportamental, em especial a partir do *online profiling* (elaborações de perfis online)”. Neste sentido, verifica-se que “o histórico de navegação, as buscas realizadas em ferramentas de pesquisa, as compras online, praticamente tudo é considerado na hora de destinar uma publicidade personalizada aos gostos e interesses do consumidor de forma quase pessoal”. (MACHADO; RUARO, 2017, p. 429).

A problemática reside nas “conclusões tiradas de uma análise puramente dataísta”. Assim, surgem “problemas de vieses, de erros, de privacidade e de discriminação”, e apelos diretos ao tipo de personalidade pretendida (CAMURÇA, 2020, p. 124), o que propicia ofensas aos direitos fundamentais e de personalidade do indivíduo.

Como visto, a publicidade comportamental, mediante a criação de perfis informacionais de hábitos e preferências do indivíduo, pode ofender os seus direitos fundamentais e de personalidade. Principalmente porque não raro o usuário dificilmente tem o controle acerca da coleta, do armazenamento, do tratamento e de possíveis vazamentos e compartilhamentos de dados no ambiente virtual; ou dificilmente tem a real dimensão e do alcance da utilização destes dados pelo mercado financeiro, empresas privadas e pelo Estado.

3 TRATAMENTO DE DADOS E O DIREITO À AUTODETERMINAÇÃO INFORMATIVA

A possibilidade de utilização indevida de dados no ambiente virtual suscita uma série de questionamentos quanto à proteção dos direitos fundamentais e de personalidade do cidadão em rede. Neste cenário, essencial é analisar o direito à autodeterminação informativa do usuário, com o objetivo de que este possua maior controle quanto ao tratamento de seus dados no panorama hodierno de hiperconectividade.

De acordo com Sousa e Silva, “a necessidade de regular a crescente produção e circulação de dados e de informações surge a partir das transformações advindas com as

tecnologias da informação e comunicação (TICs)”, que possibilitam “o processamento massivo de dados capazes de facilitar o processo produtivo de tomada de decisões empresariais e gerar reflexos para a vida do cidadão e das instituições de forma geral”. O grande “volume da produção e circulação de dados e de informações tem conduzido ao surgimento de normas destinadas a aspectos da proteção da privacidade e de dados pessoais, em face da vulnerabilidade a que o titular dos mesmos tem sido exposto”. (SOUSA; SILVA, 2020, p. 2).

Acerca do direito à proteção de dados no ordenamento jurídico brasileiro, a Constituição Federal de 1988 garante a liberdade de expressão e o direito à informação, “que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade”. A texto constitucional proclama como invioláveis a intimidade e a vida privada (art. 5º, X), a interceptação de comunicações telefônicas, telegráficas ou de dados (art. 5º, XII). Ainda, instituiu o *habeas data* (art. 5º, LXXII), que “basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. (DONEDA, 2011, p. 103).

Isso é prova que a Constituição Federal reconhece “os efeitos da circulação e da não circulação da informação sobre os indivíduos e a sociedade e buscou regular esses efeitos por meio do estabelecimento de diversos direitos fundamentais”. (MENDES, 2018, p. 192).

O Código Civil prescreve que é inviolável a vida privada da pessoa natural (BRASIL, 2002) e o Código de Defesa do Consumidor (Lei nº 8.078/90) estabelece, no art. 43, “uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em “bancos de dados e cadastros”, implementando “uma sistemática baseada nos *Fair Information Principles* à matéria de concessão de crédito”. (DONEDA, 2011, p. 103).

Conforme Hoffmam e Cavalheiro (2011), com a Internet, “o direito fundamental a privacidade se vê frente as mais variadas situações, de onde se delineiam desafios jurídicos, para assegurar a efetiva proteção ao referido direito, conferido pela Lei Maior”. Aquela, “por se tratar de uma nova mídia por meio do computador, com incrível velocidade de transmissão”, consolidou-se como “meio de manifestações de opiniões, notícias, interações, propaganda, ou apenas uma opção de entretenimento”. A fluidez, com que se dá este cenário “é algo nunca antes visto na história das relações sociais, [...] devido à rápida interação em

rede, instituindo uma conexão de diversos usuários da Internet – internautas –, dos mais variados locais”. (*apud* ARAUJO; CAVALHEIRO, 2014, p. 212).

Diante da necessidade de 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”. Assim, “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. 94).

Como observa Doneda (2011, p. 92) a ampla utilização de dados pessoais para as mais variadas atividades, tais como: “identificação, classificação, autorização e tantas outras”, torna tais dados “elementos essenciais para que a pessoa possa se mover com autonomia e liberdade nos corredores do que hoje costumamos denominar de Sociedade da Informação”. Logo, “os dados pessoais chegam a fazer às vezes da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável”.

Neste sentido, verifica-se que “quaisquer dados e metadados que levem à identificação de uma pessoa podem ser utilizados para formar perfis informacionais que traduzam padrões comportamentais, que são de enorme valia tanto para empresas privadas quanto para o Estado”. Ainda, há a possibilidade de veiculação de dados pessoais no âmbito das empresas privadas, que podem transformar estes dados em ativos comerciais ou, como pontuou o Ministro Luiz Fux, do Supremo Tribunal Federal (STF), em sede de julgamento da ADI 6387, “verdadeiras *commodities* informacionais”. (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 2). Para Doneda:

o tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais. 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. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental. (DONEDA, 2011, p. 92).

De acordo com Roque (2019, p. 2-3), o grande problema é o “enorme risco de utilização dos dados pessoais – muitas vezes colhidos sem o consentimento de seus titulares –

para promover uma verdadeira devassa na vida privada”, uma vez que esses dados são submetidos “a tratamento por meio de algoritmos, a fim de realizar classificações, prognósticos ou mesmo julgamentos – que podem ser discriminatórios”, tendo em vista que “algoritmos frequentemente se baseiam em padrões passados, que podem ser o resultado de alguma distorção ou de injustiças da vida social”. Sem mencionar a possibilidade de que estes dados “tenham sido colhidos de forma incompleta, estejam desatualizados ou se encontrem equivocados”. (FRAZÃO, 2018 *apud* ROQUE, 2019, p. 3).

Diante dos questionamentos quanto ao tratamento de dados e a aplicabilidade e o funcionamento de algoritmos e dispositivos no ambiente virtual, surge a defesa do direito do usuário à autodeterminação informativa, com vistas a propiciar maior conhecimento e controle deste acerca da forma com que seus dados são utilizados e compartilhados em rede. Como pontuam Finkelstein, Federighi e Chow, o direito à autodeterminação informativa é:

um direito constitucional de personalidade que tem por objeto o poder do indivíduo sobre três aspectos: de decidir sobre a divulgação e o uso dos seus dados pessoais; de decidir sobre quando e dentro de quais limites esses dados podem ser revelados; e, por fim, de ter conhecimento sobre quem sabe e o que sabe sobre ele, além de quando e em que ocasião. Percebe-se que a utilização de dados pessoais, da forma como vem sendo feita pelo Poder Executivo em suas diversas esferas da Federação, não vem respeitando as noções mais elementares do Direito à Autodeterminação Informacional. (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 24).

Para os autores, tal direito reconhece “uma esfera inviolável da vida privada, da qual se supõe que a influência da autoridade pública deve ser removida”. Em 2020, o Supremo Tribunal Federal, em sede de julgamento da ADI 6387, declarou inconstitucional a Medida Provisória 954, que previa o compartilhamento de dados de empresas de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE) durante o período da pandemia do COVID-19. (FINKELSTEIN; FEDERIGHI; CHOW, 2020).

A Corte compreendeu que a MP não definia de forma clara “como e “para que” seriam utilizados os dados em questão, de forma que havia uma falta de explicação quanto à finalidade deste compartilhamento. Importante ressaltar que tal decisão observou exatamente os efeitos nefastos da possibilidade de surgimento de um eventual Estado de vigilância. (FINKELSTEIN; FEDERIGHI; CHOW, 2020).

Quanto à esta possibilidade, é imperioso ressaltar que é muitas vezes é o próprio usuário quem diariamente, e cada vez mais, expõe acontecimentos de sua vida e seus dados pessoais no ambiente virtual em troca das benesses proporcionadas por este espaço. Contudo,

visualiza-se que este concorda em utilizar certa rede social, em informar seus dados em determinado site, sem ter o conhecimento e a real dimensão de como estas informações serão tratadas por estes algoritmos e dispositivos. Não raro, tendo em vista a necessidade de acesso a conteúdo online, este acaba concordando com apenas um clique com todos os termos de uso do aplicativo, sem nem mesmo saber para que e como seus dados podem ser utilizados e/ou compartilhados.

Desta forma, verifica-se que a autodeterminação informacional é um direito que permite maior controle do usuário acerca de como seus dados são tratados no ambiente virtual, de modo que este deve também consentir com a possibilidade de que seus dados sejam utilizados ou não no âmbito da criação de *perfis* informacionais e da publicidade comportamental, tendo em vista a necessidade de proteção de seus direitos fundamentais e de personalidade, uma vez que tal perspectiva possibilita o aumento da assimetria em relação ao consumo, pode potencializar a discriminação entre usuários e diminuir a capacidade de escolha livre e autônoma do indivíduo em rede.

4 PERFIS INFORMACIONAIS E PUBLICIDADE COMPORTAMENTAL: DIREITO À AUTODETERMINAÇÃO INFORMATIVA NA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Diante dos possíveis contornos nefastos da criação de perfis informacionais e da publicidade comportamental à proteção dos dados pessoais do usuário no ambiente virtual, indispensável é examinar o direito à autodeterminação informativa à luz da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), com forte influência do Regulamento 2016/679, no âmbito da União Europeia, e que dispõe sobre o tratamento de dados pessoais, inclusive digitais, da pessoa natural ou jurídica, de direito público ou privado, tendo por objetivo proteger os direitos fundamentais de liberdade e privacidade, bem como o desenvolvimento da personalidade da pessoa natural.

Conforme Mendes, tal Lei “instituiu de forma inédita no país um regime geral de proteção de dados, consolidando e complementando o marco normativo da sociedade da informação em desenvolvimento no Brasil”, inaugurando um “modelo *ex-ante* de proteção de dados, fundado na ideia de que não existem mais dados irrelevantes em face do processamento automatizado e ubíquo de dados na sociedade da informação”. (MENDES, 2018, p. 186).

Como compreendem Sousa e Silva, a LGPD surge como “medida que busca estabelecer o controle sobre a circulação de dados e de informações, utilizando-se como um de seus fundamentos o princípio da autodeterminação informativa”, que dá aos seus titulares poderes “para decidir sobre o que será considerado ou não objeto de tratamento”. (SOUSA; SILVA, 2020, p. 2). Conforme prescreve o art. 2º da Lei Geral de Proteção de Dados, a disciplina da proteção de dados pessoais no Brasil tem como fundamentos:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;**
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018, grifo nosso).

Nos termos do art. 5º, incisos I e II, da LGPD, considera-se *dado pessoal* a “informação relacionada a pessoa natural identificada ou identificável”, enquanto dado sensível, são dados “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).

Tais conceitos permitem, segundo Sousa e Silva, “a compreensão sobre o que representam os dados pessoais, no domínio da produção e consumo”. Assim, “a informação não necessariamente apresenta-se disponível no formato ou estrutura desejável pelas instituições e empresas, pois muitas vezes elas estão “encobertas” nos dados”. Por esta razão, tornam-se necessários “processos que buscam deixá-la mais acessível e capaz de atender as necessidades de busca e uso, permitindo, assim, o gerenciamento dos mesmos, para que os sejam processados, tratados e convertidos em informação”. (SOUSA; SILVA, 2020, p. 5).

Segundo o art. 6º da Lei Geral de Proteção de Dados, as atividades de tratamento de dados pessoais devem observar a boa-fé e os seguintes princípios: *finalidade*, que proclama que o tratamento de dados deve seguir propósitos legítimos, explícitos e específicos, que devem informados ao usuário, de forma que não é legal o tratamento de modo incompatível com tais finalidades; a *adequação* prescreve que o tratamento de dados deve ser compatível com as finalidades que foram informadas ao usuário; e o princípio da *necessidade* pontua que o tratamento deve ser limitado ao mínimo necessário para as finalidades propostas, apenas com os dados pertinentes, de forma proporcional. (incs. I ao III). (BRASIL, 2018).

O princípio do *livre acesso* assegura ao usuário o direito de consulta gratuita e facilitada acerca do modo e da duração do processo de tratamento dos dados, assim como quanto à integralidade; o princípio da *qualidade dos dados* prevê que estes sejam exatos, claros, relevantes e atuais, conforme a necessidade para cumprir a finalidade do tratamento; e o princípio da *transparência* tem por objetivo garantir que as informações sejam claras, precisas e acessíveis quanto ao tratamento e seus agentes, de forma a observar o segredo comercial e industrial. (incs. IV ao VI). (BRASIL, 2018).

O princípio da *segurança* tem por escopo assegurar que serão utilizadas medidas técnicas e administrativas para a proteção dos dados de acesso não autorizado e de circunstâncias acidentais ou ilícitas de destruição, alteração, perda, difusão ou comunicação; o princípio da *prevenção* proclama que devem ser adotadas medidas de prevenção contra dados em razão do tratamento dos dados; o princípio da *não discriminação* pontua a impossibilidade de tratamento de dados para fins ilícito, discriminatórios ou abusivos; e o princípio da *responsabilização e prestação de contas* acentua a necessidade de o agente responsável pelo tratamento demonstrar a adoção de medidas capazes e eficazes à comprovação quando à observância das normas de tutela dos dados pessoais.(incs. VII ao X). (BRASIL, 2018).

O art. 11, inciso I, da LGPD prescreve que o tratamento de dados sensíveis apenas poderá ocorrer diante do consentimento específico do usuário; ou, sem o consentimento, conforme o inciso II, nas hipóteses:

- a) cumprimento de obrigação legal ou regulatória pelo controlador;
- b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- e) proteção da vida ou da incolumidade física do titular ou de terceiro;
- f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
- g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018).

A LGPD também confere, conforme o seu art. 12, §2º e art. 20, legitimação às organizações para a criação de perfis comportamentais, mediante ferramentas de inteligência artificial, “aceitando a viabilidade de ocorrerem processos decisórios sem revisão humana”,

bem como o uso compartilhado por órgãos e entidades públicas para o cumprimento de suas competências legais e entre esses e o setor privado, circunstância que acaba autorizando “o monitoramento permanente dos cidadãos, inclusive antecipando seus comportamentos futuros, e permite o seu condicionamento por tais organizações”. (MASSENO, 2020, p. 81).

Como observam Sousa e Silva, “o consentimento do titular, dentre os requisitos previstos no artigo 7º da LGPD, evidencia-se como o mais importante para o tratamento dos dados pessoais”, uma vez que “implica na permissão do titular dos dados para que possam ser coletados e tratados pelos agentes específicos, determinados na própria lei em comento”. (SOUSA; SILVA, 2020, p. 7). Para o compartilhamento de dados pessoais com outros controladores é exigida a permissão prévia e específica para este fim.

Assim, “o controle por meio do consentimento do titular, torna-se instrumento de garantia dos direitos de liberdade, intimidade e privacidade”, tendo em vista que “possibilita a mudança de eixo da estrutura da privacidade constituída pelo cidadão, informação e segredo, para o eixo da tríade cidadão, informação e controle”. (SOUSA; SILVA, 2020, p. 8).

Para Silva e Souza, o direito à autodeterminação informativa constitui “o direito do indivíduo de decidir, em princípio, sobre o uso de dados relacionados à sua pessoa”. Isto é, o “direito do indivíduo de decidir quem utiliza, para quem são repassados e com que finalidades os dados e informações pessoais são utilizados”. Essa afirmação “conduz ao entendimento de que a permissão do titular em todas as fases do processamento e utilização da informação a partir do consentimento torna-se importante” para definir “o sentido e o alcance do fundamento da autodeterminação informativa”. Uma vez que, “o referido termo, como instrumento de exteriorização do referido fundamento, possua aplicabilidade prática e possa cumprir seu papel com eficiência”. (SOUSA; SILVA, 2020, p. 11).

Como pontua Roque, os impactos do uso indevido de dados pessoais pode se revelar tanto no plano individual como coletivo. Conforme prevê o artigo 22 da LGPD, “a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, não só de forma individual, mas também coletivamente”. O artigo 42, *caput*, da LGPD “faz menção ao fato de que a violação à legislação de proteção de dados pessoais pode acarretar danos patrimoniais ou morais, inclusive coletivos”. Ainda, o “§3º do mesmo artigo estabelece que as ações de reparação por danos coletivos decorrentes da violação à proteção de dados pessoais podem ser exercidas coletivamente em juízo”. (ROQUE, 2019, p. 3-4).

Logo, “não só a tutela coletiva dos dados pessoais é admitida pela legislação pertinente – notadamente, pela Lei n.º 7.347/1985 (Lei da Ação Civil Pública) e pelos arts. 81 a 104 do Código de Defesa do Consumidor (CDC) –, como encontra-se contemplada expressamente pela LGPD”. (ROQUE, 2019, p. 4). Como lecionam Araujo e Carvalho, “garantir a privacidade do usuário traz consigo o questionamento acerca da legitimidade do titular dos dados pessoais, quanto à proteção dos mesmos contra qualquer ingerência externa”. Tal legitimação “se dá, a partir do conjunto dos seus dados, como nome, características físicas, idade, gostos e preferências, que constroem sua personalidade, sendo estas informações a identificação de uma determinada pessoa”. (ARAUJO; CAVALHEIRO, 2014, p. 214).

Para Dodena (2016) este contexto “ultrapassa a noção individualista e o eixo pessoa-informação-segredo, para abarcar uma dimensão maior, referente à coletividade, trazendo consigo a apreensão quanto à pessoa-informação-circulação-controle”, tratando-se da “dinâmica de um paradigma de vida pautado na comunicação e relacionamento com os demais – sociedade informacional”. (*apud* ARAUJO; CAVALHEIRO, 2014, p. 214).

Conforme analisado, verifica-se que diante da real possibilidade de utilização o dos dados pessoais dos usuários no ambiente virtual para fins de criação de verdadeiras *commodities* informacionais, fundamental é que o indivíduo tenha ciência, consinta e tenha controle acerca da forma com que seus dados são tratados e compartilhados por aplicativos e dispositivos em rede. Diante disso, essencial é a defesa do direito à autodeterminação informativa, uma vez que garante ao cidadão maior domínio acerca da proteção de seus dados pessoais em rede e, conseqüentemente, de sua privacidade e demais direitos fundamentais e de personalidade.

5 CONCLUSÃO

No contexto atual de hiperconectividade, é parte do cotidiano do usuário acessar redes sociais, sites de notícias, plataformas de *e-commerce* e veiculação de conhecimento e identificar-se, concordar com termos de uso de aplicativos e algoritmos, que progressivamente personalizam a experiência virtual, com base na criação de perfis informacionais e comportamentais. Desta forma, a coleta e o tratamento de dados pessoais do usuário passam a

ser conteúdo de grande valia para empresas privadas e para o Estado, uma vez que facilitam a compreensão acerca de estimativas do mercado financeiro, de consumo, promovendo a publicidade comportamental e direcionada, de forma que há também o risco de discriminação algorítmica, de uso indevido de dados ou compartilhamento e/ou vazamento de informações.

Logo, é essencial que os dados pessoais do cidadão sejam protegidos pelo Estado e pelo Direito, de forma a evitar que estes sejam utilizados para fins não democráticos ou que prejudiquem o indivíduo, por meio da deflagração de sua vida privada e intimidade, principalmente porque muitas vezes as pessoas não têm a real dimensão acerca de como esses dados são coletados, tratados e como podem ser utilizados para vigilância digital pelo mercado financeiro, âmbito trabalhista ou pela própria Administração Pública.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) estabelece uma série de princípios e requisitos para a coleta e o tratamento de dados do usuário, de forma a proteger a autodeterminação informativa do cidadão, direito fundamental e de personalidade essencial para a tutela do indivíduo no meio virtual. Assim, por meio deste direito, garante-se ao usuário o poder de decidir acerca da divulgação e do uso de dados; quando e dentro de quais limites estes podem ser compartilhados e de ter conhecimento quanto a quem sabe e o que sabe quanto a esses dados, bem como quando e em que oportunidade.

Por óbvio que é o próprio indivíduo que diariamente decide expor seus dados no ambiente virtual em troca dos benefícios proporcionados pela hiperconectividade. Todavia, este deve ter o direito de consentir ou não com a utilização e o tratamento de seus dados com o objetivo de formação de perfis informacionais e de veiculação de publicidade comportamental, uma vez que estes podem interferir em seu direito de escolha e autonomia em rede.

Além disso, pontua-se como necessário o fomento da discussão quanto ao consentimento para a utilização dos dados pessoais no ambiente virtual, tendo em vista que muitas vezes os termos de uso e de consentimento são acordados mediante apenas um clique do usuário, não raro em letras minúsculas, em abas que impedem a navegação e o acesso a conteúdo sem a confirmação positiva para coleta de dados do cidadão, que cada dia mais se vê obrigado à adoção dos meios digitais, inclusive para o exercício da própria cidadania.

Tais apontamentos são fundamentais tendo em vista a necessidade de segurança em rede, as consequências de atividades nefastas relacionadas ao tratamento de dados que discriminem, diminuam o poder de autonomia e/ou ampliem as desigualdades sociais. Logo, o

direito à autodeterminação informativa deve garantir ao cidadão a imposição de limites quanto à coleta, o armazenamento, o tratamento e o compartilhamento de dados pessoais no ambiente virtual, especialmente em razão da possibilidade de criação de perfis informativos e da publicidade comportamental e o risco de ofensa aos direitos fundamentais e de personalidade do usuário, entre eles, o direito à privacidade e à proteção de dados pessoais.

REFERÊNCIAS

- ARAUJO, Luiz Ernani Bonesso de; CAVALHEIRO, Larissa Nunes. A proteção de dados pessoais na sociedade informacional brasileira: o direito fundamental a privacidade entre a autorregulação das empresas e a regulação protetiva do internauta. **Revista do Direito Público**, Londrina, v. 9, n. 1, p. 209-226, jan./abr. 2014. Disponível em: <http://www.uel.br/revistas/uel/index.php/direitopub/article/view/16870>. Acesso em: 5 set. 2020.
- BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, [1990]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 5 set. 2020.
- BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 5 set. 2020.
- CAMURÇA, Lia Carolina Vasconcelos. **Sociedade de vigilância, direito à privacidade e proteção de dados pessoais**: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário. 2020. 221 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2020. Disponível em: http://repositorio.ufc.br/bitstream/riufc/51045/1/2020_dis_lcvcamur%c3%a7a.pdf. Acesso em: 5 set. 2020.
- DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em: 5 set. 2020.
- FINKELSTEIN, Claudio; FEDERIGHI, André Catta Petra; CHOW, Beatriz Graziano. **O Uso de Dados Pessoais no Combate à COVID-19**: Lições a partir da Experiência Internacional. *Revista Brasileira de Inteligência Artificial e Direito*, v. 1, n. 1, p. 1-31, jan./abr. 2020. Disponível em: <https://rbiad.com.br/index.php/rbiad/article/view/7/5>. Acesso em: 5 set. 2020.
- MACHADO, Fernando Inglez de Souza; RUARO, Regina Linden. Publicidade comportamental, proteção de dados pessoais e o direito do consumidor. **Conpedi Law Review**, v. 3, n. 2, p. 421-440, jul./dez. 2017. Disponível em: <https://indexlaw.org/index.php/conpedireview/article/view/3745>. Acesso em: 5 set. 2020.
- MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. Disponível em: <http://eduardomagrani.com/wp-content/uploads/2019/07/Entre-dados-e-robo%CC%82s-Pallotti-13062019.pdf>. Acesso em: 5 set. 2020.

- MASSENO, Manuel David. A segurança dos dados na LGPD brasileira: uma perspectiva europeia, desde Portugal. **Revista do Direito**, Santa Cruz do Sul, n. 59, p. 80-103, jan./abr. 2020. Disponível em: <https://online.unisc.br/seer/index.php/direito/article/view/14819>. Acesso: 5 set. 2020.
- MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. Disponível em: <http://dfj.emnuvens.com.br/dfj/article/view/655/905>. Acesso em: 5 set. 2020.
- OLIVEIRA, Rafael Santos; BARROS, Bruno Mello Correa de; PEREIRA, Marília do Nascimento. O direito à privacidade na internet: desafios para a proteção da vida privada e o direito ao esquecimento. **Revista da Faculdade de Direito da UFMG**, Belo Horizonte, n. 70, p. 561-594, jan./jun. 2017. Disponível em: <https://www.direito.ufmg.br/revista/index.php/revista/article/view/1863>. Acesso em: 5 set. 2020.
- ROQUE, André. A tutela coletiva dos dados pessoais na Lei Geral de Proteção de Dados Pessoais (LGPD). **Revista Eletrônica de Direito Processual – REDP**, Rio de Janeiro, ano 13, n. 2, maio/ago. 2019. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/redp/article/view/42138/30270>. Acesso em: 5 set. 2020.
- SOUSA, Rosilene Paiva Marinho de; SILVA, Paulo Henrique Tavares da. Proteção de dados pessoais e os contornos da autodeterminação informativa. **Informação & Sociedade: Estudos**, João Pessoa, v. 30, n. 2, p. 1-19, abr./jun. 2020. Disponível em: <https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/52483/30580>. Acesso em: 5 set. 2020.
- SOUZA, Dayane Caroline de; AMARAL, Flávia. Cookies e publicidade comportamental estão na mira da proteção de dados. **Consultor Jurídico**, 22 fev. 2020. Disponível em: <https://www.conjur.com.br/2020-fev-22/opiniao-cookies-publicidade-mira-protECAo-dados>. Acesso em: 5 set. 2020.
- UNIÃO EUROPEIA. **Regulamento (UE) 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). Bruxelas: Jornal Oficial da União Europeia, [2016]. Disponível em: https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-_protecao_de_dados.pdf. Acesso em: 5 set. 2020.

Submetido em 15.09.2020

Aceito em 22.09.2020.