Política de *cookies* e a "crise do consentimento": Lei Geral de Proteção de Dados e a autodeterminação informativa

Cookie policy and the "consent crisis": Brazilian General Data Protection Law and informative self-determination

Raissa Arantes Tobbin*

Valéria Silva Galdino Cardin**

REFERÊNCIA

TOBBIN, Raissa Arantes; CARDIN, Valéria Silva Galdino. Política de *cookies* e a "crise do consentimento": Lei Geral de Proteção de Dados e a autodeterminação informativa. *Revista da Faculdade de Direito da UFRGS*, Porto Alegre, n. 47, p. 241-262, dez. 2021. DOI: https://doi.org/10.22456/0104-6594.113663.

RESUMO

O artigo tem por objetivo analisar a política de cookies no ambiente virtual nos termos da Lei Geral de Proteção de Dados, com base no direito à privacidade e na autodeterminação informativa. Para tanto, a pesquisa utilizou o método hipotético-dedutivo, fundamentado em revisão bibliográfica. Como resultado, verificou-se que a atual política de cookies ainda está muito longe de proteger os dados pessoais do usuário, especialmente porque os termos de uso dos aplicativos e de páginas acessadas por meio da Internet dificultam ao cidadão comum a compreensão acerca de como estes poderão ser utilizados futuramente pelo Estado e por empresas privadas no âmbito da monetização de dados propiciada pelo capitalismo de vigilância, contexto que evidencia uma "crise do consentimento" e a necessidade de proteção da autodeterminação informativa, tendo em vista a relação assimétrica entre os usuários e os agentes de tratamento de dados.

PALAVRAS-CHAVE

Algoritmos. Inteligência artificial. Consentimento. Direitos da personalidade. Lei Geral de Proteção de Dados.

ABSTRACT

The article aims to analyze the cookie policy in the virtual environment under the terms of the Brazilian General Data Protection Law, based on the right to privacy and informational self-determination. The research adopted the hypothetical-deductive method, based on a bibliographic review. As a result, it was found that the current cookie policy is still a long way from protecting the user's personal data, especially since the terms of use of the applications and pages accessed in the Internet make it difficult for people to understand how their personal data can be used in the future by the State and private companies in the scope of data monetization provided by surveillance capitalism, a context that highlights a "consent crisis" and the need to protect the informational self-determination, in view of the asymmetrical relationship between users and data processing agents.

KEYWORDS

Algorithms. Artificial intelligence. Consent. Personality rights. Brazilian General Data Protection Law.

*Mestranda em Ciências Jurídicas pela Universidade Cesumar (UNICESUMAR); Graduada em Direito pela Universidade Paranaense (UNIPAR); Graduada em Letras – Português/Espanhol pela Universidade Estadual de Ponta Grossa (UEPG); Advogada no Paraná.

**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 (UEM) e no Doutorado e Mestrado do Programa de Pós-Graduação em Ciências Jurídicas pela Universidade Cesumar (UNICESUMAR); Pesquisadora pelo Instituto Cesumar de Ciência, Tecnologia e Inovação (ICETI); Advogada no Paraná.

SUMÁRIO

1 INTRODUÇÃO

O objetivo do presente artigo é analisar o consentimento do usuário na Lei de Geral de Proteção de Dados diante da política virtual da utilização de cookies, com respaldo no direito à privacidade e na autodeterminação informativa. De início, destaca-se que os *cookies* e os *spams* não são práticas digitais ilegais ou que ferem dispositivos da legislação brasileira se utilizados com base em abordagem ética e não-discriminatória. Contudo, verifica-se que a massificação do seu uso poderia repercutir em direitos fundamentais e da personalidade que são essenciais para o desenvolvimento do indivíduo e para a preservação da sua dignidade humana, dentre eles, o direito à privacidade e à autodeterminação informativa, diante da necessidade de proteção de dados pessoais, sobretudo porque cada vez mais o cidadão necessita utilizar a Internet e aplicativos e dispositivos tecnológicos para as atividades diárias, de trabalho, para estudos e para o próprio exercício da cidadania.

O trabalho justifica-se tendo em vista a amplitude atual da utilização do ciberespaço e da necessidade de controle de práticas digitais destoantes da legislação pátria, especialmente do disposto na Constituição Federal de 1988 e na Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), que prevê como essencial a tutela da privacidade do usuário e de seus dados. Ainda, é fundamental a análise do instituto do consentimento na LGPD e sua abrangência com vistas a dar mais liberdade e autonomia para o usuário acerca do controle de suas informações e se este consegue tutelar o cidadão diante do cenário hodierno do capitalismo de vigilância, monetização de dados e de utilização e compartilhamento indevido destes com o escopo de manipulação ideológica e política, fins antidemocráticos e de consumo. Além disso, é essencial visualizar que a temática de proteção de dados ganhou ainda mais relevo diante da crise de saúde pública provocada pela pandemia da COVID-19, que obrigou a população mundial a cumprir regras de isolamento social ante a inexistência de cobertura de imunização até o presente momento e a se comunicar, trabalhar, estudar e exercer sua cidadania pela via digital. Logo, também ficou mais vulnerável aos entraves existentes acerca da utilização de algoritmos e dispositivos de inteligência no mundo virtual pelas empresas ligadas ao ramo da tecnologia e ao mercado financeiro.

No primeiro capítulo do desenvolvimento, o trabalho analisará as principais características das políticas de cookies utilizadas no ambiente virtual, de modo a examinar para que serve tal prática e como esta se dá em rede, além dos seus eventuais riscos aos direitos fundamentais e de personalidade do cidadão. No segundo capítulo, será analisado o instituto do consentimento, presente na Lei Geral de Proteção de Dados, e se este é hábil a garantir maior poder ao usuário acerca do controle de seus dados pessoais em rede, de modo a se insurgir contra práticas antiéticas, antidemocráticas, bem como a utilização e o compartilhamento indevidos.

Posteriormente, serão examinados o direito à privacidade e à autodeterminação informativa e seus delineamentos no contexto pós-moderno, de modo a verificar a importância da proteção e efetivação destes para a tutela dos dados pessoais dos indivíduos, que representam atualmente o principal insumo do mercado tecnológico e financeiro e que podem ser considerados expressão direta da personalidade, uma vez que refletem as preferências, os gostos, interesses, desejos e conteúdo acessado e engajado em rede com base na experiência virtual do usuário. Para tanto, a pesquisa utilizou o método hipotético-dedutivo, fundamentado em pesquisa e revisão bibliográfica de obras, artigos de periódicos, legislação, doutrina e jurisprudência aplicáveis ao caso.

2 A POLÍTICA DE COOKIES NO AMBIENTE VIRTUAL

Nos últimos anos, houve um crescimento exponencial de políticas de *cookies* no ambiente virtual para fins de manutenção do mercado financeiro e tecnológico e que repercute em importantes direitos fundamentais e de personalidade do usuário, ganhando atenção da seara jurídica, com vistas a preservar a privacidade do indivíduo, bem como a sua dignidade.

De acordo com França (2015, p. 96) o *cookie* é um "pequeno arquivo de texto armazenado pelo navegador (web browser), funcionando como uma 'carteira de identidade' do usuário, permitindo a memorização de dados e o reconhecimento de hábitos de navegação", de modo que podem ser convertidos em importantes informações para a manutenção de sites e a veiculação de publicidade personalizada mediante mecanismo de vigilância da atividade do usuário em rede. Os *cookies* são arquivos que são depositados no computador do indivíduo pelo site acessado e que possibilitam a identificação deste usuário com o intuito de facilitar a funcionalidade da página e o monitoramento da navegação, de forma que podem ser oriundos das páginas visitadas, de outras entidades (*cookies* de terceiros), apagáveis (*cookies* de sessão)

ou persistentes (*cookies* permanentes) (CASTELLUCCIA, 2012, p. 23-24). Os principais tipos de *cookies* seriam (i) os do próprio domínio (primários ou *first party cookies*); (ii) os definidos por terceiros (denominados *third party cookies*), os que somente funcionam enquanto estiver aberta determinada página (*cookies* de sessão ou *session cookies*) e os que atuam mesmo depois que o *site* ou página for fechada (*cookies permanentes*) (ALDEIAS, 2012 *apud* FRANÇA, 2015, p. 98).

Em tese, o usuário pode gerenciar e bloquear os *cookies*. Contudo, Castelluccia (2012, p. 23-24) observa que existem *cookies* complexos, como os *supercookies* e os *evercookies*. Os *supercookies* levam em consideração elementos dos navegadores e gerenciam os dados do internauta, contornando o controle deste acerca do que é ou não coletado e deletado. Enquanto os *evercookies* podem manipular o armazenamento temporário de informações (cachê) e permanecer no computador mesmo que aparentemente deletados.

A utilização de *cookies* e de *spams* não é ilegal, uma vez que traz muitos benefícios aos usuários no ambiente virtual. Todavia, tal uso tem se dado de forma "desenfreada e desregulada, acarretando prejuízos de tempo, dinheiro e invasão de privacidade para o usuário" (PRATES, 2014, p. 42). Segundo Prates, muito embora as mudanças de entendimento, são constantes os abusos em relação ao envio de *spams* e à utilização de *cookies*, contexto que muitas vezes passa despercebido pelas pessoas que utilizam a Internet e que, na maioria das vezes, não possuem conhecimento técnico para verificar se estão sendo monitoradas. Neste cenário, a falsa ideia de anonimato no ambiente virtual favorece tais políticas, principalmente como ferramentas de envio de vírus e práticas de cibercrimes (PRATES, 2014, p. 42).

Os *advertinsing cookies* são os utilizados para produzir publicidade comportamental, com base no conteúdo acessado e engajado pelo usuário. E os mais difíceis de controlar são os *cookies* de terceiro (*third party advertising*), que são instalados por domínios diversos do site acessado. Assim, dificilmente é possível saber quem irá coletar tais informações e como estes dados serão utilizados. Tais *cookies* seriam o elemento-chave no processo do âmbito de monetização de dados, principalmente porque é mais difícil evitar o rastreamento (FRANÇA, 2015).

Conforme Oliveira e Silva (2018, p. 313) atualmente, os dados pessoas adquiriram status "de ativos intangíveis, tornando-se estratégicos para os negócios no setor. Empresas como Google, Amazon, Uber e Netflix possuem os dados de seus clientes como o principal ativo de sua atividade empresarial." Ainda, os autores afirmam que é um erro acreditar em serviços

gratuitos na rede, uma vez que a disponibilização de produtos é geralmente "paga" com a coleta dos dados pessoais por meio do cadastramento e aceite dos termos de uso, que geralmente são extensos, com tamanho de fonte pequena, possuem linguagem técnica distante do usuário e podem facilmente serem aceitos com o simples clique, principalmente se estiverem barrando o acesso do usuário ao conteúdo pretendido, importante e/ou necessário.

Como explica Castelluccia (2012), o mercado que monetiza dados é composto por três tipos de agentes, que são responsáveis por manter a dinâmica e o fluxo de dados pessoais nos anúncios *online*, quais sejam: o anunciante (*advertiser*), o veiculante (*publisher*) e o agenciador (*adnetwork*). O anunciante é o que possui um produto ou serviço e o expõe em páginas e aplicativos de terceiros em determinada mídia, que são os veiculantes. Tal contato é promovido geralmente por uma agência, que se responsabiliza pela coleta e pelo posicionamento dos anúncios, recebendo uma contrapartida financeira com base no número de *clicks* que o anúncio atraiu. O rastreio pela *web* pode ocorre por meio de um conjunto de expedientes tecnológicos, tais como: aplicações de *javascript*, *cookies* de navegador e técnicas de *browser fingerprinting*.

Segundo Magrani (2019, p. 35) este mercado explora a "personalização e customização automática de conteúdo nas plataformas digitais", capitalizando a filtragem por meio dos *cookies* e dos processos de *retargeting* ou mídia programática (*behavioral retargeting*). É a chamada publicidade comportamental, fundamentada na experiência *online* personalizada do usuário:

> (...) na linha de como os mecanismos de navegação estão se configurando, a internet estaria se transformando em um espaço no qual é mostrado o que se acha que é de nosso interesse. Assim, quase sempre nos é ocultado aquilo que de fato desejamos ou eventualmente precisamos ver. Desse modo, pode-se dizer que a *filter bubble* pode implicar restrições a direitos fundamentais como acesso à informação, liberdade de expressão, bem como à própria autonomia dos indivíduos, sendo prejudicial de forma geral, podemos dizer, para o debate e a formação de consenso na esfera pública conectada [...] o problema reside na forma e no excesso da filtragem, tanto por parte das empresas quanto dos próprios indivíduos que, sem ter consciência, se limitam e se afastam de pontos de vista divergentes dos seus, empobrecendo, assim, o valor do debate na esfera pública virtual. Por isso argumenta-se que os filtros-bolha limitam os usuários ao que desejam (ou desejariam) segundo, na maior parte das vezes, uma predição algorítmica. Isso dificulta o acesso às informações que deveriam ou precisariam ser vistas para o enriquecimento do debate democrático (MAGRANI, 2019, p. 159).

De acordo com Finkelstein, Federighi e Chow (2020), os dados são verdadeiras *comodities informacionais*, conforme pontuou o Ministro Luiz Fux, do Supremo Tribunal Federal (STF), em sede de julgamento da ADI 6387. Além disso, os dados, por ocasião da pandemia da COVID-19, se tornaram "um ativo de marketing indispensável", uma vez que

parte da população mundial passou a cumprir recomendações de isolamento social em casa, ficando mais suscetível à publicidade pela via digital, de modo que o *e-commerce* passou a ser fundamental para a continuação do comércio e para a contenção de prejuízos.

O controle do ciberespaço no contexto pós-moderno objetiva "identificar e classificar perfis por meio do acompanhamento e monitoramento das informações trocadas na web, para diagnosticar tendências e interesses, buscando personalizar e direcionar a publicidade" (FACHINI; FERRER, 2019, p. 236) mediante a coleta, a utilização e o compartilhamento de dados pessoais pelo Estado e por empresas privadas, que dominam o processo de tratamento de dados e, na maioria das vezes, possuem interesses particulares distintos do público.

Explica Doneda (2011, p. 93) que o tratamento de dados, especialmente em processos automatizados, é uma atividade de risco, que pode se concretizar diante da possibilidade de exposição ou utilização indevida e abusiva de dados. É possível também que os dados coletados são sejam corretos ou representem de forma errônea o seu titular. Ainda, é possível o compartilhamento de dados com terceiros sem o prévio consentimento do usuário. Diante disso, seriam fundamentais mecanismos que possibilitassem à pessoa conhecer e ter controle sobre seus próprios dados, que seriam expressão de sua personalidade, o que explica o motivo pelo qual a proteção de dados ser considerada por diversos ordenamentos jurídicos ao redor do mundo como instrumento crucial para a proteção da pessoa humana e como um direito fundamental.

Conforme pesquisa desenvolvida por Pelau, Niculescu e Stanescu (2020), os usuários geralmente estão dispostos a fornecer seus dados para obter as benesses concedidas pela rede. Além disso, tendem a acreditar que as outras pessoas a sua volta são mais vulneráveis à manipulação de dados do que eles e compreendem tal risco como geral e não individual. Visualiza-se também que as consequências de tal risco também são pouco perceptíveis ao cidadão comum, já que também abrangem conceitos tecnológicos, ações de mercado e a compreensão da necessidade de proteção de dados, direito à privacidade e à autodeterminação informativa, que, em um primeiro momento, podem parecer inatingíveis diante de um simples aceite de *cookies* ou coleta de dados em uma página comum da Internet acessada em poucos segundos.

Deste modo, verifica-se que a política de *cookies* pode ser tanto benéfica como maléfica para o usuário em rede e que, por mais que tais estratégias de monitoramento *online* e direcionamento de conteúdo com base no comportamento possam ser, em tese, controladas e

bloqueadas, há certos tipos de *cookies* cuja regulação e abrangência são mais complexas, bem como menos acessíveis ao cidadão que desconhece os ditames do mercado tecnológico fundamentado no capitalismo de vigilância, fundado na vigilância excessiva do cidadão para fins de consumo e controle social (ZUBOFF, 2019; TOBBIN; CARDIN, 2020).

Assim, é necessário analisar como se dá o consentimento acerca da utilização de políticas de *cookies* pelo usuário, principalmente tendo como norte a Lei Geral de Proteção de Dados, de modo a assegurar maior liberdade e autonomia ao indivíduo para o gerenciamento de seus dados, bem como para a proteção de seus direitos à privacidade, à autodeterminação informativa e a preservação de sua dignidade humana em recintos norteados pela inteligência artificial, algoritmos e técnicas de *learning machine*.

3 CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS

Em setembro de 2020, entrou em vigor, no Brasil, a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), com o intuito de dispor sobre o tratamento de dados pessoais, inclusive no meio digital, por pessoa natural ou jurídica, de direito público ou privado, com o objetivo de tutelar os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade do cidadão.

Dispõe o artigo 2º, incisos I a VII, da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), que a disciplina da proteção de dados pessoais no Brasil tem como fundamentos: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

De acordo com o art. 6º da LGPD, o tratamento de dados deve observar a boa-fé e os princípios da *finalidade* (propósitos legítimos, específicos, explícitos e informados); da *adequação* (compatibilidade do tratamento com a finalidade informada); da *necessidade* (limitação ao mínimo necessário e à finalidade, com apenas os dados pertinentes, de forma proporcional e não excessiva); do *livre acesso* (garante a consulta gratuita e facilitada pelos usuários acerca do tratamento, bem como da integralidade dos dados); da *qualidade* (assegura a exatidão, atualização, clareza e relevância dos dados, de acordo com a necessidade de cumprimento da finalidade) (BRASIL, 2018).

Há também os princípios da *transparência* (assegura aos titulares informações claras, precisas e acessíveis acerca do tratamento de dados, observado o segredo comercial e industrial); da *segurança* (medidas técnicas que protejam os dados da utilização indevida, de acidentes ou atividade ilícita de destruição, alteração, perda, comunicação ou difusão); da *prevenção* (adota medidas para prevenir danos em virtude do tratamento dos dados); da *não discriminação* (impossibilidade de tratamento com base em vieses discriminatórios, abusivos ou ilícitos) e da *responsabilização e prestação de contas* (demonstração acerca da adoção de medidas de proteção e da eficácia destas) (BRASIL, 2018). Tais princípios demonstram que a coleta e o tratamento devem ser específicos, possuir uma finalidade, serem consentidos, adequados, observar o direito à igualdade e os direitos da personalidade, tais como o direito à privacidade e à autodeterminação informativa, e que o vazamento e o compartilhamento ilícitos devem ser punidos, tendo em vista a necessidade de transparência, segurança e prevenção de ofensas ao usuário.

Nos termos do art. 7º, incisos I a VIII, da LGPD o tratamento de dados pessoais somente poderá ser realizado:

> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018).

O art. 8º da LGPD menciona que o consentimento do titular para o tratamento de dados deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade; além disso, é vedado o tratamento de dados pessoais mediante vício de consentimento e este deverá referir-se às finalidades determinadas, de forma que autorizações genéricas são nulas

(§§3º e 4º do art. 8) (BRASIL, 2018). Como observam Lugati e Almeida (2020) ao longo da LGPD, o consentimento é tratado exaustivamente, sendo citado 35 vezes.

Como pontua Doneda (2016), o consentimento deve ser específico e não um cheque em branco concedido pelo usuário ao coletor de dados, de modo a possibilitar ofensas diante de interpretações extensivas. É o consentimento o instrumento essencial para o cidadão exercer o seu direito à autodeterminação informativa, com liberdade e autonomia, de modo que confere ao titular a prerrogativa de concordar ou não com a utilização e o tratamento de seus dados (LUGATI; ALMEIDA, 2020). De qualquer modo, o art. 11 da LGPD permite que:

> os dados pessoais sensíveis, aí incluídos os dados referentes à saúde, sejam tratados sem o consentimento do titular, quando tal tratamento for indispensável, além de outras hipóteses, à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos, à proteção da vida ou da incolumidade física do titular ou de terceiro, bem como à tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Isso não quer dizer que as outras previsões legais da Lei 13.709/2018 não são aplicáveis ao tratamento de dados realizados nas referidas hipóteses. Ao contrário, os direitos dos titulares continuam garantidos, assim como, também devem ser observados, conforme apontado acima, os princípios elencados no artigo 6° da LGPD (MODESTO; EHRHARDT JUNIOR, 2020, p. 151).

Conforme aponta Bioni (2020), no *General Data Protection Regulation* (GDPR), no âmbito da União Europeia, o consentimento é tido como uma ação afirmativa ou declaração, de modo que a manifestação de vontade do titular é posta em destaque. No item 42, o GDPR demonstra a importância do consentimento informado, que é o conhecimento por parte do usuário acerca da finalidade do tratamento de seus dados, evidenciando a importância da autodeterminação informativa e da participação deste no processo de tratamento. Os itens 60 e 61 do GDPR impõem acerca da necessidade de que o titular seja informado quanto a perfis e riscos gerados pelo tratamento de dados, as consequências do não fornecimento do consentimento e de que os responsáveis demonstrem como os dados serão utilizados. Os *cookies* aparecem de forma expressa no GDPR, sendo citados como elementos que potencializam a identificação e a formação de perfis, sendo mencionados pelas Diretivas 2002/58/CE e 2009/136/CE, com o intuito de harmonizar a política de *cookies* de terceiros ao uso publicitário de dados pessoais (OLIVEIRA; SILVA, 2018).

Para Sousa e Silva (2020, p. 17), o consentimento é uma forma de controle acerca dos dados e informações no ambiente virtual, já que permite que instituições e titulares de dados e informações "possam, por meio de um percurso do consentimento, e das formalidades observadas a partir desses elementos, conhecer onde, como, porque e para que, as instituições

utilizam seus dados e informações.” Conforme Faleiros Júnior e Basan (2020), o caso da empresa “Decolar.com” é um exemplo no que se refere à utilização de dados pessoais de usuários para fins de discriminação algorítmica sem o prévio e devido consentimento, uma vez que foi condenada em razão de diferenciação no preço de acomodações e negativa de oferta de vagas conforme a localização geográfica do consumidor. Apesar do avanço tecnológico e da legislação atual protetiva dos dados pessoais, é visível ser um desafio garantir que o consentimento em rede cumprirá de fato os moldes da Lei Geral de Proteção de Dados.

Neste sentido, Lugati e Almeida (2020, p. 24) demonstram a dificuldade que há na possibilidade de determinar se o consentimento é mesmo livre, tendo em vista a massificação de propagandas que influenciam a vontade e criam necessidades nos usuários, bem como se os termos de adesão permitem uma escolha por parte do titular sobre a utilização de seus dados, pois este gradativamente necessita consentir com tais termos para se inserir na sociedade. Os autores citados também mencionam que termos como “Eu aceito”, “Concordo” e “Sim” não seriam hábeis para expressar o consentimento “inequívoco”, uma vez que este ensejaria uma ação que indicasse a anuência do titular, de forma ativa, e não passiva (LUGATI; ALMEIDA, 2020, p. 24-25):

> quanto aos termos de uso e políticas de privacidade de serviços oferecidos na Internet, é fácil perceber que são demasiadamente longos e o clique no “eu aceito” ao final no texto claramente não reflete a real manifestação de vontade do usuário [...].

Conforme aponta Sansana (2018), um estudo da Universidade de Stanford verificou que cerca de 97% dos usuários entrevistados não liam os termos de uso, contratos e políticas no ambiente virtual, especialmente em razão da necessidade de priorização de ganhos imediatos, uma vez que não aceitação geraria a impossibilidade de acesso a produtos, serviços e informações relevantes. A não aceitação significaria a exclusão do usuário do universo e do conteúdo disponível em rede, uma vez que a participação do indivíduo no cenário digital depende do seu acesso à informação. Para Bioni (2020), haveria, então, uma falsa possibilidade de escolha e a consequente concordância do usuário, se rendendo ao mercado informacional de modo tão automático que, muitas vezes, tal ato nem mesmo seria hábil de racionalização. Tal exclusão se acentua principalmente se o acesso a certo conteúdo é fundamental para as atividades cotidianas, como as relacionadas ao trabalho, estudos, ou seja, que são essencialmente importantes ou imprescindíveis para que o indivíduo exerça a sua cidadania, sua atividade laboral, dê continuidade à sua educação, etc., contexto em que não parece mais

ser uma escolha do usuário, já que navegar na Internet deixou há muito tempo de ser lazer, divertimento e opção para ser obrigação e necessidade.

De igual modo, para Magrani (2019, p. 79), o atual modelo de consentimento do usuário tem sido ineficaz diante dos recorrentes abusos constantes nos termos de uso de provedores, de modo a ofender os direitos humanos. Ainda, o autor compreende que a velocidade com que as informações circulam na Internet e frequência com que os indivíduos necessitam acessar a rede dificulta um "consentimento expresso verdadeiramente informado para o tratamento de dados", sendo este contexto um enorme desafio para a tutela dos dados pessoais. Lugati e Almeida (2020) visualizam ainda que o adjetivo "*informado*" pressupõe o conhecimento adequado pelo titular acerca das ações que envolvem o tratamento dos dados para o fornecimento de uma decisão de forma adequada.

Em relação aos *cookies*, o grande problema é que para consentir "é imprescindível conhecer o significado e as implicações do uso", reconhecendo em que medida o usuário pode "ter seus dados expostos ou utilizados indevidamente. Para minorar o desconhecimento sobre o tema, os websites passaram a ter de publicar a sua política de privacidade, os tipos de cookies utilizados e como desativar o rastreamento" (FRANÇA, 2015, p. 96). Contudo, verifica-se que boa parte dos usuários não tem ideia do que será feito com os seus dados ou das consequências futuras das ações de coleta, utilização, tratamento, compartilhamento e utilização indevida de dados pessoais.

É uma constante o uso de *cookies* de forma intrusa e que, por mais que estes representem acesso a certas benesses e funcionalidades da rede, o seu emprego indiscriminado pode expor de forma abusiva informações pessoais, especialmente em relação à vigilância maciça e à criação de perfis informacionais para fins de consumo com base na experiência *online* e no conteúdo engajado pelo usuário (FRANÇA, 2015; PAULICH; CARDIN, 2020). O caso internacional paradigma acerca da necessidade de proteção de dados é o da compra de dados dos usuários da rede social *Facebook* pela empresa de consultoria *Cambridge Analytica*, contratada pelo grupo político que promoveu o *Brexit* e a campanha à presidência de Donald Trump nas eleições americanas de 2016. Estima-se que os dados pessoais de cerca de 87 milhões de usuários tenham sido atingidos com o compartilhamento indevido, sem o consentimento dos usuários para o determinado fim. Depois do ocorrido, o valor das ações do *Facebook* despencou e, se já pairavam dúvidas acerca da utilização de dados pessoais dos

indivíduos para a manipulação ideológica e política, estas preocupações se mostraram justificáveis (FORNASIER; BECK, 2020; TOBBIN; CARDIN, 2020).

Tal caso somente demonstra como os usuários de redes sociais e demais aplicativos e dispositivos de inteligência artificial disponíveis em rede ainda desconhecem como é a utilização e a possibilidade de compartilhamento de seus dados pelo mercado baseado na vigilância e na formação de perfis comportamentais e informacionais. Além disso, como visto, a efetividade do consentimento, nos moldes atuais, a um simples clique, com termos de uso extensos, dificilmente garante a tutela dos dados pessoais, pelo contrário, compele o indivíduo a aceitar os *cookies* para que consiga ter acesso a informações necessárias para sua vida cotidiana, trabalho, estudos, lazer, pesquisas sobre assuntos relacionados à saúde e essenciais para o exercício da cidadania, principalmente no contexto da pandemia da COVID-19.

4 PRIVACIDADE DO USUÁRIO E O DIREITO À AUTODETERMINAÇÃO INFORMATIVA

Nos termos da Constituição de 1988, a dignidade da pessoa humana figura, no seu art. 1º, inciso III, como um dos fundamentos da República Federativa do Brasil. Já o art. 5º, inciso X, da Constituição, considera como invioláveis "a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988). A vida privada também é mencionada como inviolável pelo art. 21 do Código Civil (BRASIL, 2002).

Pontuam Moura e Andrade (2019) que o direito à privacidade é um direito humano, fundamental e de personalidade, sendo essencial para a concretização de uma vida digna. Com a revolução tecnológica e digital, a privacidade ganhou novos delineamentos, principalmente porque, atualmente, os indivíduos são constantemente incentivados a compartilhar conteúdo pessoal no mundo virtual, de modo que abrem mão de facetas de sua privacidade em nome de reconhecimento, *status*, publicidade, seguidores e engajamento. Todavia, verifica-se que, muitas vezes, o usuário concede seus dados para entrar em uma rede social, utilizar um serviço do governo e acessar um conteúdo pago, mas não para que estes sejam compartilhados ou utilizados indevidamente no futuro. Isto é, o mercado de monetização de dados e suas consequências ainda é muito distante da percepção do usuário.

Observa Schreiber (2014, p. 137) que a tutela da privacidade hodierna amplia os tradicionais contornos do "direito a ser deixado só" para contemplar o direito a ter controle

sobre as próprias informações. Neste âmbito é que a proteção de dados passa a ser reconhecida como um direito fundamental relacionado à privacidade, alicerçando-se no direito do indivíduo de decidir como e quando dispor de suas informações, uma vez atuando em um ambiente tecnológico dinâmico e tão invasivo, como é o ciberespaço (MODESTO; ENRHARDT JUNIOR, 2020, p. 148; MOURA; ANDRADE, 2019). Para Doneda (2011, p. 103) o reconhecimento de um direito à proteção de dados, autônomo e fundamental leva em consideração os riscos advindos de tratamentos automatizados à personalidade, com base nas garantias constitucionalmente previstas de "igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada."

Já a autodeterminação informativa, segundo Sousa e Silva (2020, p. 11):

> constitui o direito do indivíduo de decidir, em princípio, sobre o uso de dados relacionados à sua pessoa. Em outras palavras, consiste no 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 no momento de definir o sentido e o alcance do fundamento da autodeterminação informativa. Isto para que, o referido termo, como instrumento de exteriorização do referido fundamento, possua aplicabilidade prática e possa cumprir seu papel com eficiência.

A autodeterminação informativa foi reconhecida inicialmente no âmbito do Tribunal Constituição Alemão, em sede de julgamento da Lei do Censo, em 1983. Na oportunidade, a Corte se manifestou no sentido de que este direito pressupõe que o indivíduo possa ter controle de suas informações diante da revolução tecnológica, escolhendo quais ações devem ser omitidas de forma livre (LUGATI; ALMEIDA, 2020). Tal direito é previsto como um dos princípios da LGPD e busca dar ao titular maior controle acerca da tutela de seus dados.

Para Sousa e Silva (2020, p. 10) o consentimento seria a "exteriorização do fundamento da autodeterminação informativa, no seu contexto prático, não constituindo assim, elemento de construção de seu sentido, mas instrumento de efetivação." Contudo, autores como Lugati e Almeida (2020), Mendes e Fonseca (2020) e Malheiro (2017) compreendem que é necessário desvincular a ideia de autodeterminação informativa baseada apenas no consentimento, uma vez que este, na realidade, representaria um instrumento utópico e ilusório, visto que facilmente perde seus efeitos, em razão da relação assimétrica da rede e da vulnerabilidade do titular de dados.

Como pontuam Moura e Andrade (2019, p. 123) o direito à autodeterminação informativa também:

> não é suficiente para evitar o fornecimento compulsório de dados para a prática dos atos mais corriqueiros de qualquer pessoa física: adquirir um telefone móvel, contratar serviços públicos essenciais, extrair documentos em órgãos públicos, prestar concursos, possuir conta bancária, etc. Logo, a "fé" no consentimento prévio como redoma protetora da privacidade do titular é puramente teórica, e baseada na extrema confiança de que os controladores e operadores de dados irão respeitar todos os ditames da LGPD. Esse ceticismo quanto à proteção do titular pelo simples fato do tratamento de dados depender de seu consentimento pode ser verificado tanto na doutrina pátria quanto na alienígena, que reconhecem a vulnerabilidade do titular e a fragilidade da proteção legal.

Para Lugati e Almeida (2020), só seria possível falar em autodeterminação se as tecnologias empoderassem o titular de dados, de forma que este tivesse uma real participação quanto ao processo de tratamento de dados. Neste âmbito, surge a proposta do consentimento granular, de modo que, segundo Bioni (2020) e Corrêa (2019), o titular poderia decidir acerca de quais dados seriam coletados, por meio de quais modalidades de tratamento, por qual período de tempo e frequência e se haveria a possibilidade de compartilhamento com terceiros. Desta forma, o consentimento granular seria o meio pelo qual o titular teria uma entrada gradual diante do fluxo de dados, mediante a fragmentação de sua autorização.

Em relação à utilização de *cookies*, é fundamental visualizar que ela aumenta a receita publicitária, especialmente de sites e jornais online, que precisam atrair o leitor e manter seus anunciantes, de modo a utilizarem *cookies* de terceiros de forma indiscriminada. Há também o problema da garantia de controle, segurança e não-compartilhamento, já que geralmente o armazenamento é feito por terceiros (empresas de tecnologia) e não pelos sites e aplicativos que o usuário acessa, havendo sempre a possibilidade de brechas para a utilização indevida. Por fim, é necessário visualizar a perspectiva possível de que, aos poucos, a privacidade deixe de ser um direito e se torne uma mercadoria, especialmente em uma sociedade pós-*cookies*, termo empregado pela *Interactive Advertising Bureau* (IAB) para designar o âmbito de relativização da privacidade e da vigilância digital (FRANÇA, 2015).

Para Schermer, Custers e Hof (2014) há atualmente uma "crise do consentimento", uma vez que a possibilidade de o usuário ser protagonista acerca do controle de seus dados é altamente questionável. As pessoas costumam não ler as políticas de privacidade e, mesmo que as leiam, dificilmente as compreendem, especialmente se há termos técnicos da informática e da tecnologia. Segundo Rodotà (2008), dificilmente o cidadão é capaz de constatar os reais riscos trazidos pelo fornecimento de seus dados no ambiente virtual, principalmente em razão da sofisticação desses sistemas. Mendes e Fonseca (2020) ressaltam que há uma limitação

cognitiva do titular acerca da utilização de seus dados no ambiente online, bem como uma assimetria na relação deste com os agentes responsáveis pelo tratamento dos dados. Neste cenário, o consentimento seria fictício, já o cidadão teria duas escolhas: consentir ou não desfrutar da gama de serviços/produtos que influenciam na sociabilidade, mercado de trabalho e acesso à informação.

Para superar esta tendência de materialização e monetização dos dados seriam soluções plausíveis responsabilizar mais a atividade de tratamento de dados:

> (i) por meio da tecnologia e do desenho dos sistemas informacionais (privacy by design), que podem auxiliar o titular no controle de seus dados; (ii) por meio de um sistema robusto de prestação de contas pelos agentes de tratamento (accountability), apto a dimensionar os riscos prévios ao tratamento de dados pessoais; e (iii) por meio do controle substantivo e contextual do consentimento (MENDES; FONSECA, 2020, p. 526

Para Moura e Andrade (2019, p. 130), diante de tal contexto, o consentimento prévio do titular para o tratamento de seus dados "é uma proteção deveras relativa e limitada, e a fiscalização estatal esboça, até o momento, uma eficiência pouco promissora, que só será possível confirmar com o decurso do tempo." Para Lessig (2006), seria necessário maior articulação entre os governos, a sociedade e as empresas de tecnologia no âmbito da discussão econômicas, políticas e humanas que envolvem as tecnologias de monitoramento. Já Hoofnagle (2012) destaca a dificuldade de transpor a visão utilitarista da monetização de dados pessoais e de suas técnicas invasivas, bem como a possibilidade de autorregulação por parte do setor tecnológico, de modo que também seria no mínimo questionável a ideia de autorregulamentação por parte das empresas de tecnologia.

Oliveira e Silva (2018) ressaltam que não há no Brasil legislação proibitiva do tratamento de dados para fins comerciais, contudo, advertem que tal prática, caso não siga parâmetros éticos, pode ofender o princípio da não-discriminação (previsto no art. 6º, IV da LGPD). Um exemplo citado por Ravindranath (2019) é a classificação de clientes com base no risco por empresas que prestam serviço médico mediante o compartilhamento de informações acerca de hábitos e saúde de pacientes, classificação visivelmente discriminatória. Também seria essencial que os desenvolvedores dos aplicativos e dispositivos de inteligência artificial criassem mecanismos mais eficazes para o controle de dados pelo indivíduo. Contudo, há que se pontuar que tecnologias como os *supercookies* e os *overcookies* conseguem contornar as preferências do usuário (OLIVEIRA; SILVA, 2018).

Ainda, ressalta-se que a coleta, o tratamento e o compartilhamento são fundamentais para o mercado de monetização de dados que sustenta tais empresas de tecnologia, de modo que também há a necessidade de maior responsabilidade por parte destas quanto aos malefícios de seus sistemas e dispositivos, uma vez que certos riscos são previsíveis, por mais que se espere que a tecnologia apresente problemas que necessitem de resolução com a evolução social. Logo, visualiza-se que há uma faceta da política de *cookies* que vulnerabiliza o usuário e o deixa mais suscetível aos interesses do capitalismo de vigilância, de igual modo, o instituto do consentimento, previsto tanto no Regulamento Geral sobre a Proteção de Dados, no âmbito da União Europeia, como na Lei de Proteção de Dados, no Brasil, ainda não se mostra, na prática, eficiente para proteger os dados dos cidadãos no ambiente virtual, demonstrando a necessidade de maior participação efetiva e debate público entre as empresas de tecnologia, o Estado, a sociedade e os usuários acerca da necessidade de proteção da privacidade e da autodeterminação informativa.

5 CONCLUSÃO

A política de *cookies* utilizada atualmente no ambiente virtual tem por objetivo analisar e formar perfis comportamentais para fins de publicidade direcionada e para a concretização de interesses dos mercados tecnológico e financeiro, podendo ser conceituados os *cookies* como pequenos arquivos de armazenamento de navegação, que funcionam com base no reconhecimento de preferências e hábitos digitais. Por mais que possam parecer benéficos e proporcionar experiência nos termos do interesse e engajamento do usuário, o seu uso de forma maciça pode acarretar a veiculação de publicidade direcionada, a inconveniência de anúncios que são mostrados ao usuário de forma excessiva, criar bolhas sociais e ambiente reacionários de manipulação ideológica, política e antidemocráticos. Isso porque, em que pese os *cookies* possam ser, em tese, geridos e bloqueados, certos tipos de *cookies* são mais difíceis de efetivamente controlar. Os tipos que representam maior repercussão nos direitos do cidadão são os *cookies* de terceiros, que colocam em dúvida quem efetivamente pode utilizar os dados coletados e os *advertising cookies*, que tem por objetivo a monetização de dados para fins de consumo.

Persiste a dúvida quanto ao que será feito com os dados coletados, uma vez que, por mais que o cidadão concorde com os termos de uso e conceda a utilização por páginas,

aplicativos e dispositivos, o armazenamento de dados geralmente é feito por empresas ligadas ao ramo da tecnologia, de modo que estas também estão suscetíveis a vazamentos e à utilização indevida. Ou sejam, não é prática ilegal, mas o seu uso indiscriminado pode repercutir na ofensa a direitos fundamentais e de personalidade dos usuários, especialmente à privacidade e à autodeterminação informativa.

O direito à privacidade na era digital ganhou contornos diversos dos tradicionais que pregavam a inviolabilidade da esfera da vida privada, de modo que atualmente pode ser compreendido como o direito de gerir e de como serão divulgadas as informações no cenário social e virtual. Já o direito à autodeterminação informativa tem por objetivo conceder maior controle e autonomia ao indivíduo para o controle da utilização e compartilhamento de seus dados, de forma a garantir que o cidadão participe ativamente do processo de tratamento, concordando acerca de como, quando, onde, por quem e para que seus dados poderão ser utilizados no futuro pelo Estado e por empresas privadas.

Tanto a tutela do direito à privacidade como a autodeterminação informativa estão previstas na Lei Geral de Proteção de Dados (LGPD), que entrou em vigor no Brasil no ano de 2020. A Lei tem por escopo garantir maior controle do indivíduo sobre seus dados, especialmente nos termos do instituto do consentimento, que deve ser uma manifestação livre, informada e inequívoca, pela qual o titular concorda com o tratamento para finalidades determinadas.

O simples consentimento, baseado em extensos termos de uso, com simples opções ao final como “Eu aceito”, “Concordo”, “Autorizo”, são pouco eficazes para garantir ao indivíduo o direito de escolha, especialmente quando a coleta de dados é o “pagamento” pelo acesso a informações importantes ao usuário, que se vê compelido a aceitar os termos de uso, a um só clique, para que não seja excluído do tráfego de circulação de informações essenciais em rede, inclusive para o próprio exercício da cidadania, principalmente em tempos de COVID-19.

Além disso, questiona-se se o usuário tem a real dimensão acerca de como seus dados podem ser utilizados tanto para fins benéficos como maléficos por diferentes atores no mundo virtual. De igual modo, o trabalho trouxe dados que demonstram que os indivíduos tendem a considerar que seus dados pouco têm utilidade para o mercado financeiro ou tecnológico, que o risco é geral e não com base na experiência individual e que as pessoas a sua volta sempre serão mais vulneráveis que eles. Isto é, grande parte da população ainda não compreende de forma abrangente qual é a real necessidade da proteção de dados, como se proteger e quais

direitos fundamentais e da personalidade poderiam ser afetados pela monetização destes, pelas práticas de vigilância digital e a criação e elaboração de perfis informacionais nos termos da experiência pessoal no ambiente virtual. De igual modo, para que o consentimento possa trazer maior autonomia e liberdade ao indivíduo, seria fundamental que as empresas de tecnologia empoderassem seus usuários, o que dificilmente ocorre, sobretudo porque a monetização de dados é o que tende a sustentar tais gigantes do ramo tecnológico, de forma que práticas como *cookies* tendem a vulnerabilizar o cidadão ainda mais e a criar maiores assimetrias entre as experiências digitais.

Outro ponto que merece destaque é a dificuldade encontrada em uma possível autorregulação deste âmbito corporativo privado, bem como que este deixe de lucrar e conceda maior proteção aos dados pessoais, principalmente tendo em vista que estes são o seu principal insumo e são capazes de, por si só, representar seu valor de mercado.

REFERÊNCIAS

ALDEIAS, Marisa. *Cookies*: uma ameaça à privacidade. 2012. Disponível em: <http://web.fe.up.pt/~jmcruz/seginf/seginf.1112/trabs-als/final/G1-T6.cookies.final.pdf>. Acesso em: fevereiro de 2015.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Brasília, DF: Presidência da República, [2002]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 5 out. 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: 10 set. 2020.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.htm1. Acesso em: 10 set. 2020.

CASTELLUCCIA, Claude. Behavioural Tracking on the Internet: A Technical Perspective. In: GUTWIRTH, Serge *et al*. (eds). *European Data Protection*: Good Health? Dordrecht: Springer, 2012.

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. Acesso em: 10 out. 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

FALEIROS JÚNIOR, José Luiz de Moura; BASAN, Arthur Pinheiro. Desafios da predição algorítmica na tutela jurídica dos contratos eletrônicos de consumo. *Revista da Faculdade de Direito da UFRGS*, Porto Alegre, n. 44, p. 131-153, dez. 2020. Disponível em: https://seer.ufrgs.br/revfacdir/article/view/95264/59892. Acesso em: 2 abr. 2021.

FACHINI, Elaine Cristina Sotelo; FERRER, Walkiria Martinez Heinrich. Biopolítica e biopoder como forma de intervenção na ordem econômica e de controle social: a Lei Geral de Proteção de Dados como inibitória da manipulação social. *Revista Direito UFMS*, Campo Grande, v. 5, n. 2, p. 226-246, jul./dez. 2019. Disponível em: https://periodicos.ufms.br/index.php/revdir/article/view/9153. Acesso em: 4 nov. 2020.

FINKELSTEIN, Carlos; 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 – RBIAD*, v. 1, n. 1, 2020. Disponível em: https://rbiad.com.br/index.php/rbiad/article/view/7. Acesso em: 10 out. 2020.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. *Revista Direito em Debate*, ano XXIX, v. 29, n. 53, p. 182-195, jan./jun. 2020. Disponível em: https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033. Acesso em: 10 out. 2020.

FRANÇA, Lilian Cristina Monteiro. Vigilância e políticas de privacidade na sociedade pós-cookie: O caso do The Guardian. *Revista Eco Pós*, v. 18, n. 2, p. 95-105, 2015. Disponível em: https://uakari.org.br/eco_pos/article/view/2229. Acesso em: 20 nov. 2020.

HOOFNAGLE, Chris Jay. Post Privacy's Paternalism. In: DIX, Alexander *et al*. (eds.). *Informationsfreiheit Und Informationsrecht:* Jahrbuch. Lexxion, 2012.

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

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. *Revista de Direito*, Viçosa, v. 12, n. 2, p. 1-33, 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 20 nov. 2020.

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

MALHEIRO, Luíza Fernandes. *O consentimento na proteção de dados pessoais na Internet*: uma análise comparada do regulamento geral de proteção de dados europeu e do projeto de lei

5.276/2016. 2017. 86 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília, 2017. Disponível em: https://bdm.unb.br/bitstream/10483/18883/1/2017_LuizaFernandesMalheiro.pdf. Acesso em: 4 abr. 2021.

MASSENO, Manuel David. Como a União Europeia procura proteger os cidadãos-consumidores em tempos de Big Data. *Revista Eletrônica do Curso de Direito da UFSM*, v. 14, n. 3, p. 1-27, 2019. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/41708. Acesso em: 20 nov. 2020.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. *Revista Estudos Institucionais*, v. 6, n. 2, p. 507-533, maio/ago. 2020. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 5 fev. 2020.

MODESTO, Jéssica Andrade; EHRHARDT JUNIOR, Marcos. Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. *REDES – Revista Eletrônica Direito e Sociedade*, v. 8. n. 2, p. 143-161, 2020. Disponível em: https://revistas.unilasalle.edu.br/index.php/redes/article/view/6770. Acesso em: 10 out. 2020.

MOURA, Plínio Rebouças; ANDRADE, Diego Calasans Melo. O direito de consentimento prévio do titular para o tratamento de dados pessoais no ciberespaço. *Revista de Direito, Governança e Novas Tecnologias*, v. 5, n.1, p. 110-133, jan./jun. 2019. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/5568. Acesso em: 20 nov. 2020.

OLIVEIRA, Jordan Vinícius de; SILVA, Lorena Abbas da. Cookies de computador e história da internet: desafios à lei brasileira de proteção de dados pessoais. *Revista de Estados Jurídicos UNESP*, ano 22, n. 36, p. 307-388, 2018. Disponível em: https://periodicos.franca.unesp.br/index.php/estudosjuridicosunesp/article/view/2767. Acesso em: 20 nov. 2020.

PAULICH, Jaqueline Silva; CARDIN, Valéria Silva Galdino. Das formas de inteligência artificial e os impactos nos padrões de consumo e a proteção dos direitos da personalidade. *Meritum*, Belo Horizonte, v. 15, n. 4, p. 228-245, 2020. Disponível em: http://revista.fumec.br/index.php/meritum/article/view/7954. Acesso em: 4 abr. 2021.

PELAU, Corina; NICULESCU, Miruna; STANESCU, Mihaela. Consumers' perception on the advantages and disadvantages of cookies and browsing history. *Proceedings of the International Conference on Business Excellence*, v. 14, n. 1, p. 829-837, 2020. Disponível em: https://content.sciendo.com/configurable/contentpage/journals$002fpicbe$002f14$002f1$002farticle-p829.xml. Acesso em: 20 nov. 2020.

PRATES, Cristina Cantú. Privacidade e intimidade na Internet: a legalidade dos cookies e spam. *FMU DIREITO*: Revista Eletrônica, v. 28, n. 42, 2014. Disponível em: https://revistaseletronicas.fmu.br/index.php/FMUD/article/view/676. Acesso em: 20 nov. 2020.

RAVINDRANATH, Mohana. How your health information is sold and turned into ‘risk scores’. *Político*, 3 de fev. 2019. Disponível em: https://www.politico.com/story/2019/02/03/health-risk-scores-opioid-abuse-1139978. Acesso em: 20 nov. 2020.

RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SANSANA, Alexandre Gomes. *Privacidade, consentimento, legítimo interesse e a nova Lei Geral de Proteção de Dados Pessoais*. Trabalho de Conclusão de Curso (Pós-Graduação) - Instituto de Ensino e Pesquisa em Direito Societário, São Paulo, 2018. Disponível em: http://dspace.insper.edu.br/xmlui/bitstream/handle/11224/2380/ALEXANDRE%20GOMES%20SANTANA_Trabalho.pdf?sequence=1. Acesso em: 4 fev. 2021.

SCHERMER, Bart Willem; CUSTERS, Bart; HOF, Simone, van der. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection. *Ethics and Information Technology*, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418#references-widget. Acesso em: 20.nov.2018.

SCHREIBER, Anderson. *Direitos da personalidade*. 3. ed. São Paulo: Atlas, 2014.

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. Acesso em: 10 out. 2020.

TOBBIN, Raíssa Arantes; CARDIN, Valéria Silva Galdino. Democracia e vigilância digital em tempos de Covid-19: uma análise do direito à autodeterminação informativa. In: *SEMINÁRIO INTERNACIONAL DE DIREITOS HUMANOS E DEMOCRACIA*: DESAFIOS JURÍDICOS EM TEMPOS DE PANDEMIA, 8., 2020, Modalidade virtual. Direitos Humanos e Democracia: desafios jurídicos em tempos de pandemia. Santa Cruz do Sul: Essere nel Mondo, 2020. v. 2. p. 360-369.

TOBBIN, Raíssa Arantes; CARDIN, Valéria Silva Galdino. Perfis informacionais e publicidade comportalmental: direito à autodeterminação informativa e a proteção de dados pessoais no ambiente virtual. *Anais do Congresso Brasileiro de Processo Coletivo e Cidadania*, v. 8, p. 1260-1276, 2020. Disponível em: https://revistas.unaerp.br/cbpcc/article/view/2193/1665. Acesso em: 4 abr. 2021.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*: the fight for a human future at the new frontier of power. Londres: Profile Books, 2019.

DADOS DA PUBLICAÇÃO

Categoria: artigo submetido ao *double-blind review*.

Recebido em: 30/04/2021.

Aceito em: 13/12/2021.