UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

LUANA MARTINS PEREIRA CAMPELO GUERRA

CONTROLE INFORMACIONAL E MONETIZAÇÃO: O CONTEÚDO VEICULADO NAS REDES SOCIAIS E A ILUSÃO DO LIVRE-ARBÍTRIO

Brasília – DF

2023

LUANA MARTINS PEREIRA CAMPELO GUERRA

CONTROLE INFORMACIONAL E MONETIZAÇÃO: O CONTEÚDO VEICULADO NAS REDES SOCIAIS E A ILUSÃO DO LIVRE-ARBÍTRIO

Trabalho de Conclusão de Curso apresentado ao Programa de Graduação em Direito da Universidade de Brasília (UnB) como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientadora: Prof.ª Dr.ª Ana Frazão

Brasília – DF

2023

LUANA MARTINS PEREIRA CAMPELO GUERRA

CONTROLE INFORMACIONAL E MONETIZAÇÃO: O CONTEÚDO VEICULADO NAS REDES SOCIAIS E A ILUSÃO DO LIVRE-ARBÍTRIO

Trabalho de Conclusão de Curso apresentado ao Programa de Graduação em Direito da Universidade de Brasília (UnB) como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientadora: Prof.ª Dr.ª Ana Frazão

BANCA EXAMINADORA

Professora Doutora Ana Frazão (Orientadora)

Universidade de Brasília

Professor Doutor Alexandre Veronese (Avaliador)

Universidade de Brasília

Professora Doutora Fernanda Lage (Avaliador)

Universidade de Brasília

Brasília, 11 de julho de 2023.

"O fim da lei não é abolir ou restringir, mas conservar e ampliar a liberdade."
John Locke

AGRADECIMENTOS

Cursar direito na UnB sempre foi o meu sonho e não poderia deixar de agradecer a todos os familiares e amigos que me acompanharam e apoiaram ao longo dessa jornada.

Em especial, gostaria de expressar minha gratidão à minha família. Adriana (mamãe) e Wagner (papai), obrigada pelo apoio incondicional ao longo de toda a minha vida. Essa monografia, assim como qualquer outra realização, se deve ao investimento e esforço de vocês. Leonardo, agradeço por estar ao meu lado nos momentos de alegria e nos percalços e, mais recentemente, por ter ingressado também no curso de direito e dividir comigo essa experiência. Às minhas avós, Ilda e Isadil, agradeço por serem símbolo de fé e força inabalável.

À ilustre Prof.ª Dr.ª Ana Frazão, por quem tenho enorme admiração, devo meus sinceros agradecimentos pelos ensinamentos e pelo suporte na escolha do tema e na elaboração deste trabalho.

Agradeço ao Pedro, cujo amor e companheirismo são refúgio nas adversidades e fonte inestimável de felicidade. Sou enormemente grata aos meus queridos amigos, Carol, Caio, Laura, Gabi e Victor, que me acompanharam durante toda a graduação (e em boa parte da minha vida). Faço menção especial à Carol, com quem compartilho desde cedo e, agora, de longe, minhas conquistas e dificuldades; e ao Grupo "Oi", integrado pela Laura e pela Gabi, que é fonte constante de alegria e apoio. Agradeço, ainda, aos amigos que fiz ao longo da graduação: Mari, Gabriel, Isadora, Malu, Duda e JL, que são fonte de inspiração e admiração e tornaram essa jornada mais divertida e leve.

Por fim, expresso minha gratidão ao Mattos Filho, que é responsável pela minha paixão pela advocacia e há mais de dois anos impulsiona o meu crescimento profissional, e à minha equipe, com a qual tenho o prazer de dividir a rotina de trabalho.

RESUMO

O presente trabalho analisa a nova realidade digital, na qual provedores de aplicação de internet classificam e gerenciam conteúdos, possibilitando que seus usuários tenham acesso a uma curadoria personalizada de informações, muitas vezes sem que sequer tenham consciência disso. Nesse compasso, pretende-se analisar se essa curadoria impacta as percepções e pensamentos dos usuários, bem como se é possível classificar tal modelo de negócios como uma violação à privacidade e à liberdade dos usuários. A partir disso, analisa-se o ordenamento jurídico brasileiro e suas limitações no que tange à proteção de dados e se é necessário regulamentar a curadoria de conteúdo realizada pelas redes sociais. Em síntese, o que se pretende é responder às seguintes perguntas: (i) o controle informacional realizado pelos provedores, muitas vezes revestido de interesses ocultos, afeta a privacidade, a liberdade e outros direitos dos indivíduos? e (ii) em que medida o ordenamento jurídico brasileiro protege os indivíduos diante da nova realidade da *data-driven economy*? Para responder à questão, foi realizada pesquisa do tipo documental e bibliográfica, baseada preponderantemente na análise a partir do arcabouço legal e da doutrina.O trabalho abordará, no primeiro capítulo, a evolução histórica da proteção de dados e do conceito da privacidade, além de demonstrar a evidente conexão entre os direitos à privacidade e à liberdade. No segundo capítulo, serão abordados os aspectos da *data-driven economy* e como podem impactar a privacidade e a liberdade dos indivíduos. Por fim, no terceiro capítulo, será abordado o ordenamento jurídico brasileiro à luz da *data-driven economy*, as limitações da legislação e, ainda, se é necessário regulamentar a curadoria personalizada da informação. Verificou-se que a atual economia movida a dados representa, além de violações à privacidade, à autodeterminação, à dignidade da pessoa humana e à liberdade dos indivíduos, ao passo em que representa um risco à própria ordem democrática. A conclusão é de que fazem-se necessárias outras iniciativas além da Lei Geral de Proteção de Dados.

Palavras-chave: dados pessoais; privacidade; tecnologia; informação pessoal; transparência; banco de dados; algoritmos; direitos fundamentais; liberdade; redes sociais; Constituição Federal.

ABSTRACT

This paper examines the new digital reality in which internet application providers classify and manage content, enabling their users to access personalized information, often without even being aware of it. In this context, the aim is to analyze whether this curation impacts users' perceptions and thoughts, as well as whether such a business model can be classified as a violation of privacy and user freedom. Based on this, the Brazilian legal framework and its limitations regarding data protection are analyzed, along with the need to regulate content curation by social networks. In summary, the intention is to answer the following questions: (i) does the informational control exercised by providers, often driven by hidden interests, affect individuals' privacy and freedom? and (ii) to what extent does the Brazilian legal framework protect individuals in the face of the new reality of the data-driven economy? To address this question, documentary and bibliographic research was conducted, primarily based on the analysis of legal frameworks and scholarly literature. The first chapter will cover the historical evolution of data protection and the concept of privacy, demonstrating the clear connection between the rights to privacy and freedom. The second chapter will address aspects of the data-driven economy and how they can impact individuals' privacy and freedom. Finally, in the third chapter, the Brazilian legal framework will be discussed in light of the data-driven economy, the limitations of legislation, and whether it is necessary to regulate personalized information curation. It has been observed that the current data-driven economy not only entails violations of privacy, but to self-determination, human dignity, and individual freedom and it also poses a risk to the democratic order. The conclusion is that additional initiatives are necessary beyond the General Data Protection Law.

Keywords: personal data; privacy; technology; personal information; transparency; database; algorithms; fundamental rights; freedom; social networks; Federal Constitution.

SUMÁRIO

INTRODUÇÃO

As redes sociais ressignificaram diversos aspectos da vida dos indivíduos e, notadamente, a forma com que esses consomem conteúdos e obtêm acesso a informações. Nesse sentido, pesquisas recentes apontam que, para 77% dos brasileiros jovens, as redes sociais representam a principal fonte de obtenção de informações (ANDRION, 2019).

Essa alteração substancial torna urgente a reflexão sobre a forma como os conteúdos são filtrados, classificados e exibidos nas redes sociais. Afinal, os reais riscos decorrentes da curadoria das informações podem passar despercebidos diante das facilidades que a conexão nas redes oferece. Há 20 anos atrás, fazia-se necessário que os indivíduos buscassem por produtos que se adequassem às suas preferências e, hoje, os usuários das redes são bombardeados por conteúdos publicitários personalizados. O acesso a conteúdo de entretenimento mostra-se também mais cômodo e prazeroso, na medida em que as plataformas elegem o que exibir aos usuários com base em suas preferências, eliminando conteúdos que podem lhes parecer desinteressantes. Ademais, as redes sociais facilitaram o acesso a informações e notícias.

No entanto, se por um lado as redes proporcionam comodidade e facilitam o acesso a determinados conteúdos, por outro lado, não possibilitam o conhecimento sobre a forma com que tais conteúdos são filtrados e impulsionadas. Ou seja, ao passo em que a tecnologia proporciona formas de se ampliar as liberdades individuais e coletivas, a partir, por exemplo, da democratização dos meios de informação, é nítido que, por outro lado, não se tem a liberdade de escolher quais conteúdos consumir nas redes sociais ou mesmo ter conhecimento sobre quais parâmetros direcionam a curadoria de conteúdo.

Nessa linha, não se pode perder de vista que, de igual modo ao açougueiro descrito por Adam Smith, as plataformas não oferecem seus serviços gratuitamente por benevolência, sem nenhuma contrapartida. Por consequência lógica, tem-se que os interesses perseguidos pelas plataformas ao filtrar conteúdos não são os de seus usuários, mas o lucro ou outros interesses de terceiros, quer sejam políticos, quer sejam econômicos.

Nesse cenário, o presente trabalho pretende discutir acerca do controle informacional nas redes sociais e de que modo a “bolha” informacional gerada pela

curadoria de conteúdos nas redes sociais pode ser utilizada para moldar consciências e influenciar comportamentos a fim de atingir interesses dos detentores de poder. Pretende-se, assim, explanar tal problemática a fim de responder a hipótese principal: o livre-arbítrio resta ameaçado diante dessa nova realidade?

A hipótese seguinte desenvolve-se a partir da análise dos contornos da *data-driven economy*, em que a violação da privacidade se tornou um negócio, por meio de um paralelo traçado entre a exploração dos dados pessoais e as potenciais violações ao livre-arbítrio. Isso porque, conforme será demonstrado, as redes sociais possibilitam um monitoramento próximo e contínuo dos seus usuários. Assim, pretende-se analisar se tal monitoramento pode ser utilizado para moldar consciências, além de simplesmente prever comportamentos. Portanto, será investigado quais fatores e mecanismos podem facilitar a potencial manipulação dos indivíduos a partir da coleta de dados pessoais.

O presente trabalho volta-se, ainda, a analisar o ordenamento jurídico brasileiro à luz dos aspectos da *data-driven economy*, visando a abordar em que medida as regras atualmente vigentes mostram-se adequadas e eficazes para responder à problemática abordada e evitar (ou não) as potenciais violações ao livre-arbítrio. Por fim, como decorrência, busca-se responder acerca da necessidade de uma legislação mais robusta, bem como abordar as iniciativas existentes que visam a coibir tais violações, além dos possíveis caminhos para um tratamento adequado da problemática.

No primeiro capítulo, pretende-se explorar o contorno histórico da proteção de dados pessoais (1.1 e 1.2), para que se possa, adiante, questionar se é necessária uma legislação mais robusta. Ademais, o primeiro capítulo (1.3 e 1.4) volta-se a estabelecer premissas acerca da relação entre liberdade e privacidade.

No capítulo seguinte, serão expostas as características intrínsecas à economia movida a dados, evidenciando que o tratamento de dados constitui um mecanismo de poder cuja capacidade de extração e processamento é ampliada em larga escala por meio de bancos de dados e algoritmos. Posteriormente, ainda no segundo capítulo, pretende-se tratar acerca da suposta gratuidade dos serviços prestados por plataformas e, por fim, tratar sobre a questão do livre-arbítrio diante do controle informacional, respondendo se, de fato, o livre-arbítrio representaria apenas uma ilusão.

No terceiro capítulo, será examinado o ordenamento jurídico brasileiro e suas limitações, analisando-se as disposições do Marco Civil da Internet, do Código Civil e da Lei Geral de Proteção de Dados, procurando, ao fim, responder se é necessária uma legislação mais robusta para coibir a violação ora tratada, qual seja, ao livre-arbítrio.

Portanto, o presente trabalho irá discutir em suma: (i) de que forma a tecnologia impactou a evolução histórica da proteção de dados e qual a relação entre a privacidade e a liberdade; (ii) se é possível que haja violações ao livre-arbítrio em decorrência do controle informacional nas redes sociais, de que forma tais violações ocorrem e como são facilitadas a partir da coleta de dados pessoais; e (iii) quais os limites impostos pelo ordenamento jurídico brasileiro e se são necessárias outras iniciativas além das atuais regras vigentes para se garantir a liberdade.

1. A PROTEÇÃO DE DADOS PESSOAIS: EVOLUÇÃO HISTÓRICA E CONCEITOS

O presente capítulo se destina a apresentar os contornos históricos da proteção de dados pessoais, especialmente à luz do desenvolvimento tecnológico (1.1. e 1.2.) para, em seguida, analisar de que forma se dá a atual tutela da privacidade, bem como qual a relação entre a proteção de dados e a liberdade (1.3. e 1.4). A partir disso, o segmento inicial deste trabalho tem a função de nortear as discussões dos capítulos seguintes, na medida em que são fixadas as premissas o contexto sob a qual se deve analisar o atual problemática envolvendo a potencial manipulação dos indivíduos perante o conteúdo veiculado nas redes sociais.

1.1. Panorama histórico internacional

Em 1890, foi publicado na Harvard Law Review o que se conhece como o primeiro marco histórico relacionado ao direito à privacidade: o artigo "*The Right to Privacy*", escrito por Samuel Warren e Louis Brandeis (FRAZÃO et al., 2022, p. 18). Nesse artigo, os autores consolidaram a jurisprudência sobre o direito à privacidade e deduziram, a partir da análise jurisprudencial inglesa e norte americana, o *"right to be let alone*", isto é, o direito de ser deixado só, que garantiria ao indivíduo proteção contra intromissões não desejadas em sua vida privada (MILANEZ, 2022, p. 9, apud ZANINI, 2015). Os autores indicaram na obra, ainda, acentuada preocupação com o vínculo entre o processo tecnológico e a tutela da privacidade (MILANEZ, 2022, p. 9).

O advento de novos meios para a obtenção de informações e dados pessoais é possibilitado e catalisado por meio do progresso tecnológico, de modo que, à medida em que a tecnologia progredia, recrudescia também uma demanda para a elaboração de um direito à privacidade (DONEDA, 2019, p. 6).

Em 1928, o caso Olmstead vs. United States, apreciado pela justiça americana, chamou atenção para a necessidade de se analisar as disposições legais, no caso, a Quarta Emenda, à luz da evolução tecnológica (DONEDA, 2019, p. 6).

Na década de 1950, o direito à privacidade individual e familiar passou a ser resguardado como um direito humano pela Declaração Universal de Direitos Humanos e pela Convenção Europeia de Direitos Humanos, da Organização das Nações Unidas (ONU) (FRAZÃO et al., 2022, p. 19).

Na década de 1960, com o advento da informática, os limites do direito à privacidade foram ressignificados a partir da concentração crescente do objeto da matéria nos dados pessoais em si e não mais no caráter subjetivo das considerações quanto à violação da privacidade (DONEDA, 2019, p. 6).

A preocupação descrita anteriormente por Samuel Warren e Louis Brandeis diante do progresso tecnológico, aliada ao crescimento exponencial dos bancos de dados e processos automatizados de tratamento de dados pessoais à época, fez com que, em 1960, o Congresso dos Estados Unidos deixasse de aprovar um projeto que previa a construção do *National Data Center*, que seria uma base de dados centralizada (MILANEZ, 2022, p. 9). A partir de audiências realizadas perante o Congresso americano para a análise do projeto, foram constatados riscos para a privacidade e liberdade, os quais não poderiam ser mitigados em virtude da ausência de medidas regulatórias capazes de proporcionar e salvaguardar esses direitos à época. Nesses debates, destacou-se o discurso do sociólogo Vance Packard, que se mostrou atento quanto ao uso de informações pessoais para controle social, bem como a fala do relator das audiências, Deputado Cornelius Gallagher, que asseverou que, embora a proposta tivesse o condão de recrudescer a eficiência da burocracia estatal, sobressaiam as ameaças à privacidade (DONEDA, 2019, p. 7).

Em 1973, outro marco para a proteção de dados foi o relatório compilado pelo Departamento de Saúde, Educação e Bem-Estar dos Estados Unidos (*U.S. Department of Health, Education and Welfare*), por meio do qual foi proposta a observância dos Fair Information Principles (FIPPs ou princípios para o tratamento leal da informação). Esses princípios, na atualidade, ainda são classificados como o núcleo principal das leis de proteção de dados ao redor do mundo e foram sintetizados por meio da análise do impacto do desenvolvimento tecnológico e da informação massiva de dados pessoais por agências governamentais, potencialmente para vigilância (MILANEZ, 2022, p. 10-11). Conforme leciona FRAZÃO *et al*. (2022, p. 20), os FIPPs se concretizaram a partir:

> "da previsão de institutos relacionados à publicidade dos bancos de dados, à exatidão e qualidade dos dados pessoais armazenados, ao livre acesso aos bancos de dados pelos titulares, à utilização dos dados conforme a finalidade informada no momento da sua coleta e à segurança no armazenamento e utilização desses dados pessoais."

Também na década de 1970, adveio o primeiro diploma normativo acerca da proteção de dados pessoais: a Lei de Proteção de Dados do Land alemão de Hesse. A referida Lei foi pioneira tanto ao se estabelecer como um modelo normativo autônomo como também na utilização do termo *Datenschutz*, que significa "proteção de dados", e não dos termos *Datensicherung* ou *Datensicherheit*, já consagrados na legislação alemã, que se referiam à segurança da informação (DONEDA, 2019, p. 8). Suas disposições, à época, mostravam-se únicas também porque foram responsáveis por elevar as cláusulas de confidencialidade ao nível da lei, fazendo com que tais cláusulas estivessem em pé de equidade com outras cláusulas que versavam sobre outros conflitos de poder (DONEDA, 2019, p. 8, apud. ENGEL; KELLER, 2000. p. 46).

A partir da Lei de Proteção de Dados do Land alemão de Hesse, surgiram algumas legislações na Europa na década de 1970, como a Lei sueca de proteção de dados - *Datalagen*, a lei francesa de proteção de dados pessoais de 1978, a *Informatique et Libertées* e outras (DONEDA, 2019, p. 9).

O Tribunal Constitucional alemão, em 1983, proferiu decisão essencial para o desenvolvimento do direito à proteção de dados pessoais. Ao analisar uma lei federal que regia o censo alemão de 1982, se concluiu que o avanço da tecnologia viabiliza o processamento de dados em maiores proporções, e, portanto, possibilita que a atividade estatística promova riscos não apenas à privacidade, mas a diversas liberdades e garantias fundamentais. A Corte, então, decidiu ser necessário promover uma revisão da interpretação de alguns direitos fundamentais e assentou a existência do direito à autodeterminação informacional, por meio do qual os indivíduos teriam o domínio sobre as suas informações a fim de proteger a personalidade em meio às circunstâncias tecnológicas e ao tratamento automatizado de dados (DONEDA, 2019, p. 9).

No contexto da União Europeia, a Convenção 108 do Conselho da Europa, editada em 1981, teve importância singular e pioneira ao vincular os Estados da Comunidade Europeia a internalizar normas a fim de proteger os dados pessoais. (FRAZÃO et al., 2022, p. 19). Anos depois, em 1995, houve a adoção da Diretiva 95/46/CE em todo o espaço europeu, (DONEDA, 2019, p. 10) que preceitua a adoção de diversas obrigações que visavam à proteção de direitos de privacidade (FRAZÃO et al., 2022, p. 19). Foi a Diretiva 95/46/CE, conhecida como a Diretiva Europeia de Proteção de Dados, que sintetizou "*as bases do direito fundamental à proteção de*

dados pessoais e do modelo ex ante de proteção de dados" (FRAZÃO et al., 2022, p. 19).

Nesse sentido, FRAZÃO et al. (2022, p. 19) assim conceituam o modelo *ex ante*:

> O modelo ex ante caracteriza-se essencialmente pela previsão de que o controlador (ou o responsável pelo tratamento, conforme o RGPD) somente poderá realizar atividades de tratamento de dados pessoais quanto estiver amparado em uma base legal, restringindo assim as hipóteses de utilização dos dados, de forma a proteger preventivamente os direitos e as liberdades dos seus titulares.

Em 14/4/2016, foi adotado o Regulamento Geral de Proteção de Dados europeu (RGPD), o qual estabelece diretrizes a fim de proteger as pessoas singulares no que tange ao tratamento de dados pessoais. Sua aplicação se deu a partir de 25/5/2018, momento em que suas disposições passaram a vincular os Estados-membros da União Europeia, com a possibilidade de ajuste de alguns aspectos por meio da legislação nacional pelos Estados-membros (FRAZÃO et al., 2022, p. 19). FRAZÃO *et al*. (2022, p. 20) afirmam que o propósito da RGPD é:

> (...) eliminar inconsistências em leis nacionais, ampliar o escopo de proteção da privacidade e proteção de dados e modernizar a legislação para desafios tecnológicos, econômicos e políticos atuais, a exemplo daqueles advindos do uso intensificado da internet.

Hoje, a disciplina de proteção de dados pessoais está presente em mais de 140 países, de acordo com estimativas (DONEDA, 2019, p. 3). Embora o perfil da proteção de dados esteja fortemente ligado aos marcos regulatórios europeus, é possível verificar que se trata de uma disciplina global. Prova disso é que alguns de seus institutos mais característicos foram consagrados nos Estados Unidos, e não na Europa. Foi em virtude de mútuas influências entre vários sistemas jurídicos, principalmente da Europa e dos Estados Unidos, que ganhou forma o "núcleo duro" da proteção de dados (DONEDA, 2019, p. 5).

1.2. A proteção de dados pessoais no Brasil

Em 1995, enquanto na União Europeia vigorava a Diretiva 95/46/CE, regra unificada em matéria de proteção de dados, no Brasil, a proteção de dados pessoais se dava de forma esparsa em institutos desconexos (MILANEZ, 2022, p. 16).

A “proteção de dados pessoais” é uma expressão cuja incorporação se deu de forma tardia no ordenamento jurídico brasileiro. Como aponta DONEDA (2019, p. 10):

> (...) o fato é que é muito recente no Brasil o elemento indutor que, finalmente, organizou em torno da proteção de dados toda uma verdadeira ‘fenomenologia’ jurídica comportada por situações jurídicas nas quais o elemento principal ou determinante diz respeito a um tratamento de dados pessoais.

Durante um longo período de tempo, o que atualmente se conhece como questões associadas à proteção de dados, antes se associava a outras matérias, como ao direito do consumidor (DONEDA, 2019, p. 10). Essa proximidade entre a proteção de dados e outros campos pode ser vista ainda na atualidade, pois alguns autores utilizam os conceitos de privacidade e proteção de dados com certa ambivalência. Tal aspecto traduz a evolução do direito à privacidade, já que esse foi regulado ao ponto de se chegar a um marco regulatório específico (DONEDA, 2019, p. 10-11).

Não obstante a ausência de uma legislação específica sobre a proteção de dados no contexto brasileiro, na década de 1980 surgiram leis estaduais que tratavam sobre os direitos de acesso e de retificação de dados pessoais. Esses dispositivos antecederam o *habeas data*, remédio constitucional consagrado com o advento da Constituição Federal de 1988 (FRAZÃO et al., 2022, p. 21) e que teve influência do conceito de Vittorino Frisoni, a “liberdade informática”, uma extensão da liberdade pessoal e resultado necessário da evolução da tecnologia (DONEDA, 2019, p. 12).

Ademais, na Constituição de 1988, foram consagrados direitos associados à privacidade: o direito à vida privada e intimidade (art. 5º, X), o direito ao segredo das comunicações telefônicas, telegráficas e de dados (art. 5º, XII). No entanto, não foi consagrado expressamente um direito à proteção de dados pessoais (DONEDA, 2019, p. 13).

Nos anos que se seguiram à Constituinte, foram editadas leis federais que tratam sobre institutos relacionados à utilização de dados pessoais (FRAZÃO et al., 2022, p. 23), as quais estimularam discussões sobre a demanda de uma legislação única (MILANEZ, 2022, p. 19). Pode-se citar, entre elas, o Código de Defesa do Consumidor, que ainda em 1990 impôs a obrigação consistente em notificar o consumidor nas hipóteses de coleta de seus dados pessoais, bem como lhe assegurar

o acesso para eventuais retificações nas informações coletadas (FRAZÃO et al., 2022, p. 23).

Em 2011, sobreveio a Lei do Cadastro Positivo (Lei nº 12.414), que objetivava facilitar crédito aos "bons pagadores", (FRAZÃO et al., 2022, p. 23) disciplinando "*a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito*". A Lei do Cadastro Positivo foi pioneira eis que elaborada à luz de uma sistemática comum à tradição de proteção de dados, já enraizada em diversos outros países. Nela, foram empregados diversos conceitos importantes para a matéria, como o de dados sensíveis, transparência e finalidade (DONEDA, 2019, p. 15).

Também sancionada em 2011, podemos destacar a Lei de Acesso à Informação (Lei 12.527/2011), que objetiva regulamentar o princípio da transparência, consagrado no artigo 5º, XXXIII, da Constituição Federal, e, ainda trouxe a definição de informação pessoal, que posteriormente foi referendada pela LGPD (DONEDA, 2019, p. 15).

Por fim, destaca-se também o Marco Civil da Internet (Lei nº 12.965), que busca nortear o uso da Internet e instituiu direitos aos seus usuários e, em seu artigo 3º, disciplina que como princípio a "proteção dos dados pessoais, na forma da lei" (DONEDA, 2019, p. 15).

Ou seja, antes do advento da Lei Geral de Proteção de Dados (LGPD), já existia no ordenamento jurídico brasileiro previsões que objetivavam a proteção da privacidade e restringiam a utilização dos dados pessoais. Todavia, careciam as normas existentes de clareza e as suas disposições não eram aplicadas de forma suficiente para garantir os direitos os quais visava proteger, o fazendo de forma esparsa (MILANEZ, 2022, p. 15).

O contexto para se estabelecer uma regulamentação geral e uniforme para a proteção de dados parecia cada vez mais concreta à medida que em diferentes cenários, seja na proteção ao consumidor ou no acesso facilitado ao crédito, já havia a previsão de dispositivos sobre a utilização de dados pessoais (DONEDA, 2019, p. 15).

O processo que deu origem à LGPD se originou a partir de negociações no Mercosul no Subgrupo de Trabalho de número 13 acerca de um dispositivo que regulamentasse de forma única a matéria de proteção de dados para os países que integravam o bloco, cuja proposta havia sido encaminhada pela República Argentina

(DONEDA, 2019, p. 15-16). Os debates levaram à aprovação das "Medidas para a proteção de dados pessoais e sua livre circulação", um documento que, no entanto, não foi analisado e deliberado para se tornar uma norma efetiva no âmbito do Mercosul (DONEDA, 2019, p. 16).

Paralelamente, tais debates no Mercosul culminaram em um crescente debate em âmbito nacional pelo governo brasileiro acerca da proteção de dados, o que pode ser exemplificado pela realização do “I Seminário Internacional sobre Proteção de Dados Pessoais”, que contou com juristas e autoridades. Ou seja, embora não tenha sido adotado um regulamento comum pelo Mercosul no que tange à proteção de dados, os debates ocorridos incentivaram discussões do Poder Executivo Brasileiro sobre a regulamentação da matéria (DONEDA, 2019, p. 16).

Os órgãos do Poder Executivo assumiram a liderança de iniciativas voltadas para a internalização da disciplina de proteção de dados pessoais. Nesse contexto, em 30 de novembro de 2010, o Ministério da Justiça divulgou o texto que é o precursor direto da atual Lei Geral de Proteção de Dados e que serviu como base para o debate público promovido pelo referido Ministério e conduzido pela Internet, com a colaboração da Fundação Getúlio Vargas - Direito Rio e do Observatório da Internet, do Comitê Gestor da Internet do Brasil (DONEDA, 2019, p. 16).

Após a conclusão desse debate, o Ministério da Justiça, por meio do Departamento de Proteção e Defesa do Consumidor (DPDC), procedeu à consolidação de um novo texto-base do Anteprojeto de Lei de Proteção de Dados (DONEDA, 2019, p. 16).

Entre 2011 e 2015, o texto-base do Anteprojeto passou por diversas revisões, embora não tenham sido divulgadas as novas versões. Nesse período, o debate sobre o Anteprojeto se deu no governo federal, liderado pelo Ministério da Justiça, contando com a participação de diversos órgãos e ministérios interessados no tema, e, em âmbito externo, contando com um público amplo e atores diversos, impulsionado pela intensificação do debate internacional sobre o assunto (DONEDA, 2019, p.16-17).

No ano de 2015, uma nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais foi divulgada publicamente pela Senacon, órgão do Ministério da Justiça, que conduziu um novo debate público sobre o tema através da Internet, por meio do qual foram recebidas mais de 1.100 contribuições (DONEDA, 2019, p. 17).

Após o debate, o Ministério da Justiça, em conjunto com o Ministério do Planejamento, Orçamento e Gestão, consolidou uma nova versão do Anteprojeto.

Esse texto foi enviado à Casa Civil da Presidência da República, que, em 13 de maio de 2016, encaminhou-o ao Congresso Nacional. O Anteprojeto foi protocolado na Câmara dos Deputados como PL nº 5.276/2016 (DONEDA, 2019, p. 17).

Em 14 de agosto de 2019, foi aprovada a versão final da LGPD (Lei nº 13.709), após extenso período de debates sobre o texto. Essa norma tem o objetivo de salvaguardar os direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade das pessoas naturais, por meio de conceitos, institutos, princípios, direitos do titular, regras de prestação de contas (*accountability*), elementos de análise de riscos, entre outros aspectos, os quais já são reconhecidos e consolidados internacionalmente no campo da proteção de dados e que foram introduzidos pela LGPD, de forma inaugural, no ordenamento jurídico brasileiro (MILANEZ, 2022, p. 19).

O texto final da LGPD representou diversas vitórias para a proteção de dados pessoais, na medida em que o seu texto se amolda ao ordenamento jurídico brasileiro, apesar de ter sido fortemente inspirada no Regulamento Europeu de Proteção de Dados, e, ainda, porque a lei logrou êxito em dar início à essencial discussão acerca da necessidade de atualizar os conceitos relacionados à regulação da privacidade e, em especial, à proteção de dados no país (MILANEZ, 2022, p. 19-20).

As legislações supracitadas, não obstante não tenham alterado formalmente a Constituição Federal de 1988, instituíram novas categorias de direitos, possibilitando o reconhecimento de um direito fundamental à proteção de dados. Nesse sentido, o STF, em 2020, reconheceu ser um direito autônomo o direito fundamental à proteção de dados (MILANEZ, 2022, p. 21).

1.3. A concepção de privacidade

Há certa indefinição no que tange ao conceito de privacidade, aspecto esse que pode ser considerado como uma característica intrínseca à matéria, e não um defeito ou óbice à sua utilização e estudo. Afinal, a indeterminação terminológica é comum a outras matérias e termos estudados pelo direito (DONEDA, 2009, p. 4), como os princípios (SUNDFELD, 2017, p. 63).

Do ponto de vista terminológico, há, no direito americano, as expressões "*right to privacy*" e "*right to be let alone*" (MENDES, 2008, p. 18). Sobre o termo "*privacy*", a jurista americana BEVIER (1995, p. 458) ensina que:

> Privacidade é uma palavra camaleônica, usada denotativamente para designar uma ampla gama de interesses diferentes - desde a confidencialidade de informações pessoais até a autonomia reprodutiva - e conotativamente para gerar confiança em favor do interesse que está sendo defendido. (tradução nossa)

No direito francês, há as expressões "*droit a la vie privée*" e "*droit a la intimité*" e no direito italiano, por sua vez, são utilizados os termos "*diritto alla riservatezza*", "*diritto alla segretezza*" e "*diritto alla rispetto della vita privatta*". Na Alemanha vê-se a expressão "*Recht auf informatiolelle Sebstbestimmung*" (direito à autodeterminação informacional) sendo utilizada de forma predominante e, por fim, na Espanha utiliza-se o termo "*derecho a la intimidad*" (MENDES, 2008, pp. 18-19).

Além dos diversos termos, em diferentes países, utilizados para designar o que se conhece como privacidade, o conteúdo de tal direito também varia conforme o *modus vivendi* de cada indivíduo e aos costumes e valores socioculturais da sociedade em que se insere. Eis, portanto, que não é possível formular uma definição universal do que seria a privacidade e o direito à intimidade e à vida privada, consagrados na Constituição Federal (CARVALHO, 2003).

No Brasil, a Constituição Federal de 1988 abre espaço para discussões acerca do termo privacidade, na medida em que o artigo 5º, inciso X, consagra que "*são 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*". O legislador constituinte, ao explicitar que tanto a "vida privada" como a "intimidade" seriam invioláveis, é possível questionar se esses seriam bens jurídicos distintos (MENDES, 2008, p. 19).

Acerca dessa discussão, MENDES (2008, p. 19) pontua que:

> O embasamento da distinção do Constituinte brasileiro pode ser encontrado na teoria das esferas de Heinrich Hubmann, segundo a qual o sentimento de privacidade do indivíduo pode ser compreendido a partir de um esquema de círculos concêntricos, que representam diferentes graus de manifestação da privacidade: no núcleo estaria a esfera da intimidade ou do segredo (Geheimsphäre); em torno dela, viria a esfera privada (Privatsphäre); e em torno de ambas, em um círculo de maior amplitude, encontrar-se-ia a esfera pessoal (Öffentlichkentsbereich), que abrangeria a vida pública do indivíduo.

No entanto, embora a Constituição Federal tenha diferenciado os termos "vida privada" e "intimidade", não se deve conferir efeitos jurídicos à proteção da privacidade pelo direito brasileiro, uma vez que o escopo de proteção, as limitações e os seus efeitos independem de tal distinção. Assim, é possível concluir ser mais adequada a

expressão “privacidade”, seja pela eventual dificuldade de se distinguir “vida privada” e “intimidade”, seja porque a expressão refere-se à existência de um único direito que engloba os casos relacionados à proteção do indivíduo em sua esfera privada, sendo uma “noção guarda-chuva” (MENDES, 2008, p. 20).

Apesar da divergência doutrinária sobre o termo privacidade (MENDES, 2008, p. 20), destaca-se o conceito de privacidade empregado por RODOTÁ (2008, p. 15): “*o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular*”.

No mesmo sentido, Alan Westin conceitua a privacidade como “*a reivindicação de indivíduos, grupos ou instituições para determinar, quando, como e em que extensão, informações sobre si próprios devem ser comunicadas a outros*” (MENDES, 2008, p. 21, apud WESTIN, 1970, p. 7).

Na atualidade, a concepção clássica da privacidade como sendo o “direito a ser deixado só” ou o “direito a estar só” foi abandonada, sendo entendido, agora, como a possibilidade de cada indivíduo controlar o uso das informações que lhe dizem respeito (MARTINS, 2020). Nesse sentido, MARTINS (2020, apud RODOTÁ, 1995, p. 19-20) assevera que:

> Na sociedade da informação, tendem a prevalecer definições funcionais da privacidade, que se referem à possibilidade de um sujeito conhecer, controlar, endereçar ou interromper o fluxo das informações que lhe dizem respeito.

Um novo eixo da tutela da privacidade emergiu a partir da necessidade de controle das informações pessoais em circulação: o direito à autodeterminação informacional, que abarca a prerrogativa do indivíduo de dispor e revelar dados concernentes à sua vida privada, em todas as etapas do processamento e uso desses dados, tais como sua coleta, transmissão, modificação e exclusão (MARTINS, 2020, apud LORENZETTI, 2004, p. 90).

Tal eixo adveio em virtude dos riscos acarretados pelo crescimento exponencial da capacidade de processamento dos computadores, bem como sua interconexão em redes que possibilitam o acesso a localidades distantes geograficamente, exercendo um efeito multiplicador na coleta, manipulação e armazenamento de dados em formato digital (MARTINS, 2020).

1.4. A privacidade e a liberdade

É cediço que os seres humanos estão sempre observando e ouvindo o que se encontra à sua volta e, tal fato, por si só, não é problemático. Todavia, quando há observação contínua, como um monitoramento de vigilância, é possível que haja efeitos problemáticos, não apenas pelo desconforto da vigilância, mas pela possibilidade de que o indivíduo altere o seu comportamento. A vigilância pode levar à autocensura e inibição, sendo até mesmo uma ferramenta de controle social, aumentando o poder das normas sociais, que funcionam de maneira mais eficaz quando as pessoas estão sendo observadas por outros na comunidade. Esse controle social não é intrinsecamente prejudicial, mas, quando em excesso, pode afetar negativamente a liberdade, a criatividade e o autodesenvolvimento (SOLOVE, 2006, p. 491).

De acordo com COHEN (2000, p. 1426), "*o monitoramento pervasivo de cada primeiro movimento ou falso começo inclinará, na margem, as escolhas em direção ao tedioso e ao convencional*", na medida em que resulta em "*uma mudança sutil, mas fundamental, no conteúdo de nosso caráter, um embotamento e uma confusão de arestas e linhas afiadas*" (tradução nossa).

A vigilância, portanto, ameaça a individualidade e inibe a liberdade de escolha, afetando a autodeterminação, além de ser equivocado por si só, eis que demonstra uma falta de respeito pelo sujeito como pessoa autônoma (SOLOVE, 2006, p. 494).

Sob esse panorama, é importante ressaltar que é absolutamente incorreta a premissa de que somente indivíduos que praticam atos ilícitos ou querem ocultar atos teriam interesse na proteção de seus dados (FRAZÃO et al., 2022, p. 6). Na realidade, conforme leciona Neil Richardson, a proteção da privacidade e dos dados pessoais tem o fim de impedir que agentes de tratamento usem o grande poder obtido a partir dos dados contra os seus próprios titulares (FRAZÃO et al., 2022, p. 6, apud RICHARDSON, 2021). Esse poder, que decorre dos dados e informações dos indivíduos, é plástico e dinâmico e está intrinsecamente ligado ao poder econômico, ao poder político e ao poder social (FRAZÃO et al., 2022, p. 6).

Desse modo, a tutela de dados pessoais não visa a esconder aspectos privados das vidas dos indivíduos, mas, de acordo com FRAZÃO et al. (2022, p. 6), visa a "a estabelecer o controle das informações a seu respeito e delimitar o poder que os agentes de tratamentos têm a partir dessas informações, inclusive para o fim de impedir que exerçam tal poder contra a população".

Além disso, em uma era em que a informação se tornou a primordial fonte de poder, a influência dos dados está intrinsecamente ligada a modalidades de *soft power* que, embora fundamentadas na persuasão, e não na violência física, podem produzir resultados igualmente ou até mais eficazes do que formas de coerção material. Tais meios têm a capacidade de moldar as opiniões e crenças das pessoas, a fim de que estas ajam em detrimento de seus próprios interesses, direcionando-se mais aos interesses dos detentores do poder (FRAZÃO et al., 2022, p. 6).

O poder que emana do tratamento dos dados, a partir disso, demanda até mesmo uma redefinição da própria concepção de *hard power*, eis que, como conclui Carissa Véliz, quando grandes corporações coletam dados de seus usuários mesmo contra a vontade destes ou em situações nas quais os mesmos resistem, estão empregando igualmente uma forma de *hard power*, cujo desfecho final é a subjugação do indivíduo (FRAZÃO et al., 2022, p. 6, apud VÉLIZ, 2020. p. 27).

Nesse sentido, se a tutela da proteção de dados tem como fim proteger os indivíduos para que não tenham suas opiniões e crenças moldadas por meio dos agentes que tratam os seus dados e informações, é nítido que a privacidade está inerentemente ligada à liberdade.

No tocante a isso, FRAZÃO *et al*. (2022, p. 7) apontam que:

> Nem as tecnologias são necessariamente boas - tudo depende da finalidade que lhes é atribuída - nem são necessariamente neutras. No atual contexto, muitas das tecnologias de tratamento de dados têm sido escolhidas unilateralmente por poderosos agentes econômicos, em relação aos quais são consideráveis os incentivos para a priorização do interesse próprio sobre os interesses dos usuários.

Sob esse prisma, o direito à privacidade manifesta-se, primordialmente, como uma projeção dos axiomas supremos da liberdade e da dignidade humana (CARVALHO, 2003). Nesse passo, acerca desses direitos, CARVALHO (2003, p. 78) afirma que:

> Para ser livre e digno, o homem precisa dispor, no âmbito de sua esfera individual, de um espaço em que possa permanecer só, sem intromissões e ingerências alheias, em que se possa isolar e resguardar seus pensamentos, sentimentos e fatos de sua vida familiar e doméstica, em que possa conter a curiosidade e o conhecimento alheio.

O problema do poder que emana dos dados apresenta dimensão coletiva, na medida em que os dados de um determinado indivíduo geralmente contêm

informações de outros indivíduos, como informações concernentes à familiares próximos do titular. Eis, portanto, que a proteção de dados é um valor social sob diversos aspectos (FRAZÃO et al., 2022, p. 6-7).

Além disso, outro aspecto que conecta a privacidade e a liberdade é o efeito Panóptico, baseado no projeto arquitetônico de Jeremy Bentham para uma prisão de 1791. A prisão foi projetada de modo que os guardas podiam observar cada prisioneiro da torre, mas os prisioneiros não podiam ver os guardas. A partir desse projeto, concluiu-se que a consciência de que poderiam estar sendo vigiados pode ser tão inibidora quanto a vigilância real (SOLOVE, 2006, p. 491).

Isso porque a consciência de estar sendo observado afeta a liberdade dos indivíduos, pois inibe comportamentos, o se amplifica quando as pessoas estão cientes da possibilidade de vigilância, ainda que não tenham certeza se estão sendo observadas em um determinado momento. A vigilância, portanto, é uma forma abrangente de poder investigatório: registra o comportamento, a interação social e potencialmente tudo o que uma pessoa diz e faz. Em vez de direcionar informações específicas, a vigilância pode capturar uma quantidade significativa de dados além do que foi originalmente buscado (SOLOVE, 2006, p. 491).

A prisão projetada por Jeremy Bentham muito se assemelha ao atual contexto decorrente do tratamento de dados pessoais.

PASQUALE (2015) descreve a realidade da *data-driven economy* como um "*one way mirror*", em que importantes agentes detentores de poder têm conhecimento pormenorizado de indivíduos, ao passo em que esses não sabem sobre como esse conhecimento será utilizado ou para qual finalidade.

Para além disso, sob a perspectiva da psicanálise social, Raymond Barglow pontua que, não obstante as novas tecnologias possam representar um meio de aprimoramento da capacidade humana de organização e interação, os sistemas de informação e a formação de redes deformam a concepção de um sujeito independente. Ou seja, as noções de soberania e autossuficiência são subvertidas pela tecnologia, dando origem a um sentimento de solidão generalizada que acarreta a busca de conectividade em redes e gera uma identidade partilhada, reconstruída (CASTELLS, 1999a, apud BARGLOW, 1994).

CASTELLS afirma que, com as sociedades civis desarticuladas, as identidades passaram a ser reconstruídas de forma coletiva, em torno de princípios comunais, tese que se comprova com base na ascensão de identidades coletivas como o

fundamentalismo religioso, a identidade étnica e o nacionalismo (AZEVEDO, 2008, apud CASTELLS, 1999b).

2. A ERA DIGITAL: *DATA-DRIVEN ECONOMY*

O presente capítulo volta-se a apresentar os contornos da *data-driven economy*, expondo (2.1) que o tratamento de dados é um mecanismo de poder, cuja capacidade de extração de dados e tratamento é facilitada em grande escala por meio de (2.1.1.) banco de dados e (2.1.2.) algoritmos. Adiante, pretende-se discutir (2.2.) acerca da suposta gratuidade dos serviços prestados por plataformas, já que há remuneração indireta e a busca por interesses que não os dos usuários, e (2.3) sobre o livre-arbítrio diante do controle informacional.

2.1. O tratamento de dados como mecanismo de poder

É reconfortante para os indivíduos acreditar que seus registros e dados pessoais estão seguros, de igual modo que estão os segredos de um grande banco. No entanto, o cenário em que vivemos muito se assemelha a um espelho unidirecional, um "*one way mirror*". Nele, importantes atores corporativos têm conhecimento das minúcias das vidas dos indivíduos, enquanto estes pouco ou nada sabem sobre o destino desse conhecimento e como ele pode influenciar decisões tomadas pelas companhias (PASQUALE, 2015, p. 2).

A verdade é que, desde os anos 2000, a questão da privacidade tem se tornado mais complicada diante de diversos fatores: a ascensão do *Big Data* e dos centros de fusão, o tsunami de violações à proteção de dados, o crescimento do marketing comportamental e a proliferação de tecnologias de rastreamento (SOLOVE, 2013).

Nesse contexto, GÜNTHER *et al.* (2017) assim definem *Big Data*:

> Big Data pode ser definido com base em grandes volumes de dados amplamente variados que são gerados, capturados e processados em alta velocidade. Como tal, esses dados são difíceis de processar usando as tecnologias existentes. Ao adotar tecnologias analíticas avançadas, as organizações podem usar Big Data para desenvolver insights, produtos e serviços inovadores.

Por sua vez, *Big Analytics* é "*a implementação de soluções técnicas de análise em massa desses grandes conjuntos de informações*" (FRAZÃO et al., 2022, p. 12).

A evolução tecnológica, por meio da coleta e registro de dados, possibilitada em grandes proporções pelo *Big Data* e *Big Analytics*, viabilizou que os dados pessoais sejam atribuídos a usos que outrora seriam inimagináveis. Essas práticas, desprovidas de uma regulamentação adequada, passaram a ser realizadas de forma indiscriminada, com potenciais consequências que podem ecoar perpetuamente (FRAZÃO et al., 2019).

Não por outro motivo se utiliza a expressão *data-driven economy*, em português, "economia movida a dados", para designar a centralidade da extração e do uso de dados pessoais no capitalismo do século XXI, na qual a violação da privacidade tornou-se um negócio (FRAZÃO et al., 2022, p. 2, apud. FRAZÃO, 2019c, p.25-63).

No âmbito da *data-driven economy*, à medida que a privacidade é violada, é aumentada a coleta de dados e informações, acarretando um aumento substancial do poderio econômico, político e social dos agentes de tratamento. É nessa perspectiva que a vigilância sobre os indivíduos se intensifica, visando a obter uma quantidade máxima de informações. Concomitantemente, à medida que o poder dos agentes de tratamento se amplia, são maiores os incentivos e meios para perpetuar e amplificar o processo de extração de dados, em um ciclo de retroalimentação constante (FRAZÃO et al., 2022, p. 2, apud. FRAZÃO, 2019c, p.25-63).

A ampla exploração de dados pessoais dos usuários na *data-driven economy* é abordada no documentário Dilema das Redes, da Netflix (2020), por meio de relatos de diversos ex-funcionários de Big Techs. Jeff Seibert, ex-funcionário do Twitter, revelou que "*cada ação que você realiza é cuidadosamente monitorada e registrada… exatamente qual imagem você parou e olhou e por quanto tempo a observou*" (tradução nossa). No mesmo sentido, Tristan Harris, ex-funcionário do Google, afirmou que:

> (...) em muitas dessas empresas de tecnologia, existem três objetivos principais. Há o objetivo de engajamento para aumentar o uso, mantendo você rolando. Há o objetivo de crescimento, para fazer você voltar e convidar o máximo de amigos possível, e fazer com que eles convidem mais amigos. E então há o objetivo de publicidade: garantir que, enquanto tudo isso acontece, estejamos ganhando o máximo de dinheiro possível com publicidade. Cada um desses objetivos é impulsionado por algoritmos cujo trabalho é descobrir o que mostrar para você para manter esses números em alta. (tradução nossa)

O intuito central dos denominados *data brokers* e de agentes como as plataformas digitais de grande porte, consiste em adquirir a maior quantidade de informações possível acerca dos cidadãos (FRAZÃO et al., 2022, p. 3). A partir dessa

perspectiva, Tim Wu afirma que a real empreitada desses agentes é empregar as informações adquiridas para exercer influência sobre as mentes dos usuários, uma vez que aqueles que possuem conhecimento íntimo das pessoas podem utilizar esse precioso acervo para manipulá-las em prol de uma ampla gama de objetivos (FRAZÃO et al., 2022, p. 3 apud WU, 2016).

A coleta de dados para manipular e moldar consciências não se restringe à seara econômica apenas. Esse fenômeno apresenta inúmeras repercussões nas esferas individuais dos cidadãos, levando à reestruturação de relações sociais e políticas (FRAZÃO et al., 2022, pp. 3-4).

Um exemplo de como os dados pessoais são sinônimo de poder na *data-driven economy* é a atividade desenvolvida por companhias conhecidas como *data brokers*. Em 2014, a *Federal Trade Comission* norte-americana realizou um mapeamento da indústria de dados e do papel dos *data brokers*, em um relatório denominado "*A Call for Transparency and Accountability*", por meio do qual se concluiu que os *data brokers* coletam informações pessoais dos indivíduos e as revendem ou compartilham e geralmente nunca interagem com os consumidores, que muitas vezes sequer têm conhecimento da sua existência e das práticas adotadas por elas (FRAZÃO, 2019a).

Conforme aponta Ana Frazão (2019a), as principais conclusões obtidas por meio do estudo desenvolvido pela *Federal Trade Comission* são:

> (i) os *data brokers* coletam informações sobre os consumidores de diversas e numerosas fontes comerciais, governamentais e públicas (incluindo nesta última mídias sociais, blogs e internet);
> (ii) os *data brokers* não usam apenas os dados crus (raw data) mas também os chamados dados derivados, que são as inferências já realizadas a partir de dados crus;
> (iii) os *data brokers* combinam dados obtidos on-line e off-line para atingirem os consumidores on-line;
> (iv) as principais utilizações comerciais dos dados são marketing, serviços de mitigação de riscos e serviços de busca de pessoas;
> (v) parte expressiva da coleta de dados ocorre sem o conhecimento dos consumidores.
> (vi) a indústria dos dados é complexa, com muitas camadas de *data brokers* que oferecem e trocam dados uns com os outros, sendo frequente o intercâmbio e a compra e venda de informações entre eles;
> (vii) os *data brokers* coletam e armazenam bilhões de dados que, na época da pesquisa, já cobriam praticamente todos os consumidores norte-americanos;
> (viii) qualquer que seja a metodologia utilizada, os data brokers coletam mais informações do que usam;
> (ix) uma das maiores aplicações dos dados é o desenvolvimento de modelos complexos para predizer o comportamento dos consumidores e para extrair inferências potencialmente sensíveis a respeito deles;

> (x) apesar dos benefícios da atividade de tratamento de dados, muitos dos propósitos pelos quais os *data brokers* coletam e usam dados apresentam riscos para os consumidores;
> (xi) as escolhas que os *data brokers* oferecem aos consumidores sobre os seus dados são amplamente invisíveis e incompletas, com grande ausência de transparência.

Apesar de a pesquisa sobre os *data brokers* ter sido realizada em 2014, FRAZÃO (2019a) indica que há evidências atuais de que as práticas por eles adotadas se intensificaram, de modo que os dados pessoais seguem sendo utilizados sem qualquer transparência ou *accountability*, e, agora, estão sendo utilizados em maiores proporções.

Ademais, por meio de estudos empíricos realizados entre 2009 e 2011 pela UC Berkeley e descritos por HOOFNAGLE *et al.* (2012), se constatou que anunciantes estavam se utilizando de tecnologias de rastreamento persistente que eram relativamente desconhecidas pelos consumidores, os quais se mantiveram ativos mesmo com as configurações de privacidade mais avançadas ligadas. O estudo demonstrou, ainda, que o número de *cookies* de rastreamento havia aumentado de forma drástica (HOOFNAGLE et al., 2012).

Assim, as observações empíricas do estudo evidenciaram que (i) os anunciantes utilizam tecnologias novas e relativamente desconhecidas para rastrear as pessoas, especificamente porque os consumidores não têm conhecimento dessas técnicas; (ii) essas tecnologias anulam os mecanismos de escolha que os consumidores exercem; e (iii) os anunciantes estão tornando impossível evitar o rastreamento online por meio da ideia de uma web personalizada e não acreditam que os consumidores sejam competentes para decidir rejeitá-la (HOOLNAGLE et al., 2012).

Essas observações são especialmente valiosas para o debate sobre a privacidade *online*, pois informam acerca da efetividade e sobre eventuais falhas relacionadas à legislação de privacidade. No debate político, aqueles que se voltam contra as regras que protegem a privacidade dos usuários alegam que são normas "paternalistas" mas, por meio do estudo realizado pela UC Berkeley, HOOLNAGLE et al. (2012) afirmam que foi possível inverter a suposição de que as intervenções para garantir a privacidade são “paternalistas”, enquanto abordagens de mercado supostamente promoveriam a liberdade

Além disso, por meio de um estudo realizado por VENTURINI *et al.* (2016), foi constatado que as plataformas podem permitir que terceiros instalem tecnologias de monitoramento em suas páginas, uma prática conhecida como "*third-party tracking*" ou, em português, rastreamento de terceiros. Essas tecnologias incluem *cookies* e *beacons*, assim como "*social buttons*" e ferramentas de análise. Nesse estudo, a conclusão obtida a partir das plataformas analisadas foi de que 80% destas permitem esse tipo de atividade.

Essa prática, isto é, a coleta de dados por terceiros, é permitida, de forma padrão, por termos de inúmeros sites, o que possibilita que empresas rastreiem a forma com que os usuários visualizam ou interagem com seus anúncios e, assim, veiculem anúncios direcionados e avaliem a sua eficácia. Pode-se exemplificar o site de compartilhamentos de vídeos Vimeo, que permite que terceiros instalem tecnologias de rastreamento em seu site para coletar informações sobre os seus usuários e a plataforma 4shared, que permite a utilização de "botões sociais" (VENTURINI et al., 2016).

Como se vê, os dados ganharam uma importância transversal, tornando-se elementos centrais para a compreensão das vidas e das liberdades individuais, assim como da sociedade e da própria democracia. A *data-driven economy* está, nesse sentido, inerentemente ligada a uma sociedade e uma política impulsionada por dados, com todas essas esferas envolvidas em interação contínua (FRAZÃO et al., 2022, pp. 3-4).

E, como é cediço, as informações podem ser lucrativas. Não por outro motivo, os governantes, há milênios, utilizam de censos populacionais, que possuem grande utilidade (DONEDA, 2011, p. 92). De igual modo, PASQUALE (2015, p. 13) afirma que "*decisões baseadas em Big Data podem levar a lucros sem precedentes*" (tradução nossa).

Assim, no seio da sociedade de consumo, os dados dos indivíduos ostentam um valor econômico substancial, posto que são empregados para, por exemplo, subsidiar as campanhas publicitárias de fornecedores, possibilitando a adoção de táticas comerciais direcionadas, aptas a obter resultados de considerável eficácia (CARVALHO, 2003).

2.1.1. Banco de dados

Em essência, os bancos de dados configuram conjuntos estruturados de informações baseados em uma lógica específica, que é sempre utilitarista, buscando, ao máximo, extrair benefícios a partir das informações sistematizadas (DONEDA, 2011, p. 92).

Com o surgimento da informática, os bancos de dados, embora não fossem novidade para a humanidade, adquiriram um novo sentido (CARVALHO, 2003) diante da facilidade de manipulação das informações, desde a coleta e processamento até a comunicação da informação, o que possibilitou a análise de volumes gigantescos de dados (DONEDA, 2011, p. 92).

Mas não é só. Ao passo em que a capacidade de armazenamento e comunicação de informações aumenta, recrudesce, na mesma medida, a variedade de maneiras pelas quais as informações podem ser aproveitadas ou utilizadas. Com o potencial de maleabilidade e utilidade aumentado, a informação se torna continuamente um elemento fundamental em um número crescente de relações e, com isso, tem o condão de influenciar o cotidiano dos indivíduos. Isso ocorre em consonância com o avanço tecnológico e, particularmente, com o uso de computadores para o processamento de dados pessoais (DONEDA, 2011, pp. 92-93).

A preocupação em torno dos bancos de dados foi externada pelo Superior Tribunal de Justiça, já em 1995, no julgamento do Recurso Especial nº 22.337/RS, da Quarta Turma do Superior Tribunal de Justiça, o que pode ser observado do trecho do voto do Ministro Ruy Rosado de Aguiar:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador.

Nesse sentido, o Ministro Ruy Rosado de Aguiar reconheceu a importância do Serviço de Proteção ao Crédito (SPC), mas alertou que “o registro não deve ser

perpétuo", justamente para se evitar que o dano social seja maior do que o bem visado com a instituição do SPC. Veja-se:

> O Serviço de Proteção ao Crédito (SPC), instituído em diversas cidades pelas entidades de classe de comerciantes e lojistas, tem a finalidade de informar seus associados sobre a existência de débitos pendentes por comprador que pretenda obter novo financiamento. É evidente o benefício que dele decorre em favor da agilidade e da segurança das operações comerciais, assim como não se pode negar ao vendedor o direito de informar-se sobre o crédito do seu cliente na praça, e de repartir com os demais os dados que sobre ele dispõe. Essa atividade, porém, em razão da sua própria importância social e dos graves efeitos dela decorrentes – pois até para inscrição em concurso público tem sido exigida certidão negativa no SPC – deve ser exercida dentro dos limites que, permitindo a realização da sua finalidade, não se transforme em causa e ocasião de dano social maior do que o bem visado.

Semelhantemente ao julgado supracitado, PASQUALE (2015) alerta que em uma sociedade dominada pelos algoritmos e bancos de dados, que são guardados em clima de sigilo, as más informações têm tanta probabilidade de perdurar quanto as boas e, assim, resultar em previsões injustas e até desastrosas. Por esse motivo, o uso indiscriminado dessas tecnologias, por mais lucrativo que seja para quem a administra, é perigoso para a sociedade como um todo.

Esse perigo, na atualidade, resta aumentado na medida em que os bancos de dados permitem a diversos entes o acesso a um conjunto de informações cada vez mais detalhados e precisos acerca dos indivíduos cujos dados pessoais são sintetizados (DONEDA, 2011, p. 93).

Nesse passo, DONEDA (2011, p. 93) assevera que os bancos de dados acarretam uma redefinição dos poderes e direitos das informações pessoais:

> 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, consequentemente, sobre a própria pessoa. Aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o 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.

Ademais, o montante crescente de informações sobre os indivíduos é problemático na medida em que recrudesce a assimetria informacional entre empresas e consumidores, colocando em xeque muitas das teorias econômicas que se baseiam na escolha racional ou soberania dos consumidores (FRAZÃO, 2018a).

2.1.2. Algoritmos

MANZANO *et al*. (2000, p. 9), definem algoritmo como:

> (...) regras formais, sequenciais e bem definidas a partir do entendimento lógico de um problema a ser resolvido por um programador com o objetivo de transformá-lo em um programa que seja possível de ser tratado e executado por um computador, em que dados de entrada são transformados em dados de saída.

A utilização dos algoritmos no comércio *on-line*, mesmo que aparente conceder aos consumidores uma sensação de liberdade de escolha devido à concorrência entre diferentes agentes econômicos, é controlada e manipulada pelas grandes corporações, que possuem um amplo domínio sobre a informação e a dinâmica do mercado (MARTINS, 2020). Esses intermediários da rede desempenham o papel de guardiões da Internet, exercendo uma forma de soberania sobre redes e plataformas, por meio de sua arquitetura lógica (códigos ou algoritmos) e regras que são estabelecidas e controladas exclusivamente por eles (VENTURINI et al., 2016).

Quando se trata de filtrar unilateralmente o conteúdo disponibilizado na internet, os algoritmos estão se tornando cada vez mais complexos, a fim de distribuir e personalizar o conteúdo de acordo com as preferências do usuário, ou mesmo excluí-lo a depender de tais preferências. Todo o conjunto de recursos técnicos empregados pelos fornecedores desempenha um papel importante na publicidade dos produtos e serviços oferecidos, fazendo uso de sinais audiovisuais cuja sofisticação crescente coloca o consumidor em uma situação de hiper vulnerabilidade (MARTINS, 2020).

Assim, por meio da avaliação de parâmetros como qualidade e preço, os consumidores são discriminados para aproveitar falhas de informação e comportamentos equivocados, para então, alcançar o objetivo de agentes econômicos. O objetivo dos algoritmos, portanto, é classificar os clientes a partir de uma classificação instantânea e automática, coletando informações, analisando registros, tomando decisões distintas a cada chamada e assumindo a responsabilidade pelas consequências resultantes (MARTINS, 2020).

Diante dessa discriminação promovida pelos algoritmos, somos levados a refletir se esses impactam as decisões dos indivíduos. RODRIGUES (2020, p. 116) assim questiona:

> Se os algoritmos por meio de reconhecimento geral dos padrões identificam preferências e a partir disso disparam sugestões, seria possível, tão logo, com a extração dos dados comportamentais, identificar manifestações inconscientes, vontades e tabus, proibições e desejos, preconceitos e imperativos, e então, intervir para evitá-los ou transformá-los através da modelagem probabilística?

De acordo com a pesquisa desenvolvida pelo *Share Lab*, da Sérvia, denominada "*Facebook Algorithmic Factory*", que visava investigar minuciosamente o funcionamento do Facebook, a resposta para o questionamento supracitado é positiva. O *Share Lab* adverte que sob as camadas de máquinas algorítmicas podem estar escondidas novas formas de potencial violação dos direitos humanos e novas formas de manipulação em grande escala, que permitem a influência de bilhões de pessoas a cada dia (SILVEIRA, 2019).

A pesquisa do *Share Lab* aponta que o Facebook emergiu como um agente central no cenário democrático, eis que mais da metade dos eleitores em um país democrático recorre à plataforma diariamente para obter informações, interagir e expressar apoio ou críticas às forças políticas. Com base em documentos divulgados pelo próprio Facebook, o *Share Lab* analisou o fluxo de informação na rede social e as interfaces de programação e mapeou parte da dinâmica oculta presente na plataforma. O desafio principal da investigação residia em descobrir técnicas de pesquisa e metodologias que viabilizassem a compreensão de como os dados são mantidos e de que forma operam os algoritmos fechados e obscuros. Para avançar na pesquisa, o *Share Lab* optou por examinar centenas de patentes registradas pelo Facebook, a partir das quais foi possível sintetizar interpretações do que ocorre nos bastidores da "caixa preta" da plataforma (SILVEIRA, 2019).

Nesse contexto, se identificou o *social graph* (grafo social), que é uma ferramenta que conecta todos os dados da plataforma, e, de acordo com o *Share Lab*, representa a "*história de dominação e ambição para governar o Mundo dos Metadados, interligando cada pedaço de informação dentro e fora do Império do Facebook num único gráfico*" (SILVEIRA, 2019, apud SHARE LAB, 2017).

O próprio Mark Zuckerberg, em 2007, revelou que o *social graph* é a razão pela qual o Facebook funciona. A partir dele, o Facebook cria um código identificador para cada evento, objeto, usuário, entre outros elementos da plataforma e esse código serve para interligar todos esses elementos de forma eficiente. Assim, cada conexão realizada entre esses elementos como, por exemplo, um *like*, é registrada, permitindo que os gestores da plataforma tenham um "mapa" das ligações entre os elementos da

plataforma. Nesse sentido, como demonstração, o <like> vincula o usuário <userID> e a foto curtida <photoID> (SILVEIRA, 2019, apud SHARE LAB, 2017).

Desse modo, o *social graph* possibilita que seja realizada uma análise estatística dos dados contidos nos bancos de dados da plataforma, fazendo cruzamentos entre todas as ligações. Esses cruzamentos, como demonstra o *Share Lab*, são essenciais para que o Facebook produza um público para o marketing, agrupando perfis de usuários para cada finalidade, por meio de algoritmos de aprendizado e de bancos de dados com informações cada vez mais ricas sobre os usuários (SILVEIRA, 2019, apud SHARE LAB, 2017).

SILVEIRA (2019, p. 72) elucida que há três categorias principais de segmentação para organizar os perfis de usuários, conforme concluiu o *Share Lab*:

> Os pesquisadores do Share Lab consideram que existem três categorias principais de segmentação, segundo organizam os perfis de usuário conforme informações básicas (localização, idade, sexo e língua), segmentação detalhada (correlacionando dados demográficos, interesses e comportamentos) e conexões (visualização e ligação com páginas e demais objetos presentes no Facebook).

Vê-se, nesse sentido, que os produtos são criados pelos humanos e apresentados pelo Facebook a outros humanos, mas o trabalho de apresentação desses produtos é realizado por algoritmos (SILVEIRA, 2019).

O grande problema reside no fato de que a escolha dos indivíduos sobre qual produto consumir, em quais ideais acreditar, e escolhas sobre tantos outros aspectos, pode ser influenciada por interesses econômicos.

A coleta de informações pode ser danosa, ainda que nenhuma informação seja revelada publicamente, uma vez que os dados pessoais extraídos são parcialmente destinados para o aprimoramento de produtos e serviços, mas, a parte que resta é destinada para avançadas tecnologias denominadas “inteligência de máquina”, que tem como finalidade a predição das ações dos indivíduos. Tais predições são, então, comercializadas com companhias que estão dispostas a apostar em um comportamento futuro para lucrar (ZUBOFF, 2021).

Nesse sentido, é o que alerta FRAZÃO (2018b, p. 19):

> (...) a tecnologia pode ser perigoso instrumento de dominação, uma vez que a sua escolha não é neutra e, no atual contexto, acaba sendo feita, em grande parte, por grandes agentes empresariais, sem transparência, accountability ou qualquer filtro democrático, podendo estar a serviço exclusivo dos interesses econômicos daqueles que a detêm.

Desse modo, é necessário buscar conhecer quem são os agentes responsáveis por empregar a tecnologia, bem como refletir acerca de quais são os interesses ou valores os quais essa tecnologia serve (FRAZÃO, 2018b, p. 20).

2.2. A Falácia da Gratuidade

A expressão "*There ain't no such thing as a free lunch*" reflete a ideia de que a todo serviço ou atividade prestada, há um custo, ainda que esse não seja visível de imediato (DOLAN, 1971). Eis, portanto, que essa frase é capaz de ilustrar a relação entre usuários e gigantes da tecnologia (*Big Techs*). Isso porque, enquanto empresa, cuja própria razão de existência é justamente gerar lucro, não faz sentido que uma plataforma desempenhe uma atividade para beneficiar e enriquecer, sem qualquer contrapartida, os próprios clientes. É mais crível, nesse sentido, que o sacrifício do operador econômico em prestar o serviço se deva a um interesse patrimonial (MARTINS, 2020, apud MOTRONI, 2002, p. 200).

É o que expõem ex-funcionários de *Big Techs* no documentário Dilema das Redes, da Netflix (2020). Roger McNamee, um dos primeiros investidores do Facebook, afirmou que:

> Nos primeiros 50 anos do Vale do Silício, a indústria criava produtos... Hardware, software... e os vendia aos clientes. Um negócio simples e agradável. Nos últimos 10 anos, as maiores empresas do Vale do Silício estão no negócio de vender seus usuários. (tradução nossa)

Aza Raskin, inventor do sistema de rolagem utilizada por diversas plataformas, afirmou também ao documentário Dilema das Redes (2020) que:

> (...) porque não pagamos pelos produtos que usamos, os anunciantes pagam pelos produtos que usamos. Os anunciantes são os clientes, nós somos o objeto que está sendo vendido". (tradução nossa)

Por fim, Tristan Harris, ex-funcionário do Google, asseverou que "o ditado clássico é: se você não está pagando pelo produto, então você é o produto. (tradução nossa)

Portanto, se há remuneração, ainda que indireta, evidencia-se que a gratuidade dos provedores não passa de uma miragem. Nesse sentido, MARQUES (2004, p. 253) aponta que:

> A ‘gratuidade’ no mercado de consumo é muitas vezes ilusória, pois há remuneração indireta (e por vezes direta e conexa) do fornecedor pela prestação daquele ‘serviço’ na sociedade de informação. É justamente o movimento da análise econômica nos Estados Unidos que nos alerta para a falácia ‘econômica’ dos chamados ‘serviços’, ‘utilidades’ ou promessas ‘gratuitas’, o que não passaria de uma superada ficção jurídica. O que parece juridicamente gratuito, alertam-nos mesmo os conservadores e radicais autores desse movimento de Chicago, é economicamente baseado na certeza da remuneração indireta, na interdependência de prestares futuros e atuais (sinalagma escondido), no estado de catividade e de dependência a que um dos parceiros fica reduzido e no lucro direto e indireto do outro (...)

A depender do modelo comercial adotado, o valor comercial de um *site* depende diretamente da quantidade de usuários que possui, já que quanto maior o público para uma eventual publicidade, mais valorizado será o espaço publicitário e, consequentemente, maior será o lucro destinado ao titular do *site* (MARTINS, 2020, apud TOSI, 1999, pp. 270-271). Assim, toda nova conexão de usuários agregará valor ao *site* (MARTINS, 2020, apud MOTRONI, 2002, p. 195).

Além disso, os operadores econômicos podem também coletar informações sobre as características e os gostos dos usuários, a baixos custos de obtenção e gestão. Nesse modelo, um site pode memorizar na respectiva *database* diversos dados e preferências do usuário (MARTINS, 2020, apud MOTRONI, 2002, p. 200).

Mas, por vezes, agentes econômicos e políticos justificam que o preço a se pagar pela utilização de novos serviços, especialmente aqueles supostamente gratuitos, seria a perda da privacidade ou a violação aos dados pessoais. Nesses serviços “gratuitos”, os usuários não pagam pela sua utilização em valores monetários, mas por meio da obtenção de seus dados pessoais, configurando um simples *trade-off*, em que os titulares dos dados pessoais escolheriam por uma opção, isto é, utilizar o serviço, em detrimento de outra, que seria ter os seus dados salvaguardados (FRAZÃO et al., 2022, p. 4).

FRAZÃO *et al*. (2022, p. 4), a partir desse contexto, classificam essa análise como simplista, na medida em que o titular de dados é colocado em situação de fragilidade diante da utilização dos seus dados como a contraprestação necessária para usufruir de serviços.

No mesmo sentido, HOOFNAGLE (2012) defende que aqueles que argumentam que os consumidores podem negociar as nuances da privacidade e do rastreamento *on-line* assumem que o mundo online é semelhante ao mundo *offline*, o que é uma visão equivocada. No mundo *offline*, os consumidores podem votar com os pés e, na maioria das circunstâncias, deixar um negócio que não desejam

frequentar sem que ele colete dados sobre a experiência. Todavia, no mundo *online*, as eficiências na identificação e agregação alteram o equilíbrio de poder na relação entre o consumidor e o negócio.

Embora, por um lado, a evolução tecnológica tenha sido benéfica para consumidores na medida em que possibilita a comparação de preços e aspectos de produtos de forma mais fácil, por outro lado, aspectos da privacidade restam prejudicados, pois possibilita que os proprietários de sites se organizaram para rastrear os indivíduos enquanto navegam na web, e poucos sites populares abrem mão desse rastreamento (HOOFNAHLE, 2012).

MOTRONI (2002, p. 210), no mesmo sentido, afirma que:

> Seguramente em análoga posição se encontra o usuário, tendo em vista o seu baixo nível informativo médio e considerado o caráter potencialmente ilimitado das informações que lhe dizem respeito e que podem ser comunicadas a um número praticamente infinito de operadores, prescindindo (e sem conhecer) o uso a ser feito por estes últimos.

De igual modo, MARTINS (2020, apud LORENZETTI, 2004) afirma que há nítida assimetria de informações na internet diante da existência de acordos entre os servidores e os provedores, os quais o usuário desconhece, de modo que a internet se divide em uma rede visível e uma rede invisível ao usuário.

Desse modo, constata-se que o usuário usufrui dos serviços prestados pelas plataformas, especialmente das redes sociais, acreditando que se trata de um serviço gratuito e muitas vezes sequer imagina que aquele serviço está sendo remunerado de forma indireta. Ademais, em virtude da assimetria da informação, sequer possui as condições necessárias para negociar os termos em que se dá a extração de seus dados.

Uma das consequências jurídicas de se constatar que há uma contraprestação por parte do usuário pelo serviço prestado pela plataforma, é a possibilidade de se classificar a relação entre o usuário e a plataforma como consumerista, nos termos do art. 3º do Código de Defesa do Consumidor (Lei 8.078/1990). Ademais, não havendo atividade desinteressada ou mera cortesia, há de se afastar a incidência do art. 392 do Código Civil, o que significa, portanto, que a plataforma deve responder pelos danos causados pelas suas atividades, seja por dolo, seja por culpa (MARTINS, 2020).

Por fim, a conclusão lógica que se extrai a partir da inexistência de gratuidade por parte dos serviços prestados pelas plataformas, é que deve-se ter atenção aos conteúdos impulsionados, sejam publicitários, jornalísticos ou mero conteúdo de terceiro, haja vista que as plataformas estão a perseguir lucro e outros interesses – que não os dos usuários – sendo necessário refletir quais seriam esses interesses e questionar se não iriam de encontro ao interesse dos usuários.

2.3. O livre-arbítrio corre perigo no Capitalismo de Vigilância?

A professora emérita da Harvard Business School, Shoshana Zuboff, emprega a expressão “capitalismo de vigilância” para explicar a nova ordem econômica, na qual se reivindica a “*experiência humana como matéria prima gratuita para a tradução em dados comportamentais*" (ZUBOFF, 2021, p. 15).

No capitalismo de vigilância, os consumidores são atraídos para operações extrativas, configurando-se objetos dos mercados de comportamentos, nos quais os clientes são as companhias que negociam, não havendo reciprocidade na relação com o consumidor. De acordo com Zuboff, a plataforma Google inventou e aperfeiçoou o capitalismo de vigilância, que logo foi disseminado para o Facebook e para a Microsoft. Esse modelo de negócios foi estabelecido como o modelo-padrão de grande parte dos negócios realizados on-line (ZUBOFF, 2021, p. 24).

De acordo com MARTINS (2020), é possível elencar cinco principais elementos como impulsionadores dos perigos intrínsecos à coleta eletrônica de dados: “*A maior quantidade de informações disponíveis, a enorme facilidade e a maior escala de intercâmbio de informações, os efeitos potencializados das informações errôneas e a duração perpétua dos registros*”.

Afinal, ao contrário das informações armazenadas no papel, como se fazia no passado, por meio da computação é possível na atualidade coletar, armazenar, manipular, trocar e retar uma infinidade de dados, que podem ser facilmente copiados e trocados por diversas companhias (MARTINS, 2020).

A partir da dinâmica competitiva do mercado, as companhias dos “mercados de comportamentos futuros” foram levadas a, cada vez mais, adquirirem fontes de dados ainda mais preditivas. Assim, se descobriu que mais preditivo do que apenas coletar dados seria intervir no jogo: induzindo e imbuindo o comportamento para atingir

maior lucratividade. Passou-se a orientar e tentar automatizar o comportamento dos indivíduos – e não mais conhecê-lo (ZUBOFF, 2021, p. 25).

As empresas na sociedade capitalista usam cada vez mais processos automatizados para avaliar riscos e alocar oportunidades, de modo que esses processos configuram uma das partes mais dinâmicas, lucrativas e importantes da economia da informação. Esses serviços fazem uso de algoritmos, geralmente secretos, para colocar alguma ordem em vastas quantidades de informação. O fascínio da tecnologia é claro – a antiga aspiração de prever o futuro, temperada com um toque moderno de sobriedade estatística (PASQUALE, 2015).

O capitalismo de vigilância impulsinou uma forma de poder que molda o comportamento humano para atingir finalidades de terceiros: o lucro. Não há poder por meio de violência, mas sim, por meio de automatização de uma arquitetura computacional quase que onipresente, formada por dispositivos, coisas e espaços inteligentes conectados (ZUBOFF, 2021, p. 25).

A tecnologia, a partir de métodos de manipulação antes inimaginável, empregada por meio da internet, submete os seus usuários a novos riscos de atentado à privacidade: por meio de rastreamento digital das informações acessadas, inclusive cookies, o envio de mensagens não solicitadas, entre outros (MARTINS, 2020).

Ademais, a pressão competitiva entre companhias fez com que o capitalismo de vigilância não mais estivesse restrito às curtidas e à navegação online, chegando ao mundo real: o cotidiano, as conversas do dia a dia, as atividades físicas, os locais frequentados. Mais do que anúncios online, as predições futuras são negociadas para atingir outros setores: o de seguros, lojas de varejo, o ramo das finanças e um conjunto cada vez maior de empresas de bens e serviços (ZUBOFF, 2021, p. 25).

Assim, como pontua FRAZÃO et al. (2022, p. 9), a possibilidade de exercer influência sobre os indivíduos e manipulá-los sempre existiu; contudo, o que se destaca nos tempos atuais é a capacidade de efetuar tal influência a partir de um conhecimento praticamente pleno sobre o sujeito a ser manipulado, aliado a técnicas altamente personalizadas que visam explorar suas fragilidades e suscetibilidades. É possível dizer, a partir dessas nuances, que a manipulação na atualidade é muito mais eficaz (FRAZÃO et al., 2022).

Um exemplo da tentativa de moldar comportamentos a partir da extração de dados é o jogo "*Pokemon Go*", um jogo de realidade aumentada, em que os jogadores deveriam sair de casa para jogar em áreas de cidades, estruturado como uma "caça

ao tesouro" (ZUBOFF, 2021, p. 375). Conforme informou John Hanke, CEO da Niantic Inc, desenvolvedora do jogo, além de oferecer compras no aplicativo, esse tinha como modelo de negócios "locais patrocinados", ou seja, lojas ou comércios seriam locais dentro do jogo virtual e, em troca, pagariam a Niantic (ZUBOFF, 2021, p. 379).

O objetivo das companhias — as verdadeiras clientes do jogo — era receber a visita de jogadores do *Pokemon Go*, atraídos a partir do jogo, para que pudessem consumir produtos e serviços. Conforme pontua ZUBOFF (2021, p. 380 apud COHEN, 2017), a estratégia dessas companhias foi bem sucedida:

> Por algum tempo, parecia que todo mundo estava lucrando. A Niantic fechou um acordo com o McDonald's para levar os usuários do jogo aos trinta mil restaurantes da cadeia no Japão. O dono de uma rede britânica de shopping centers providenciou "equipes de recarga" para perambular os shoppings com carregadores portáteis para os jogadores. A Starbucks anunciou que "participaria da brincadeira" com doze mil lojas nos Estados Unidos se tornando "Pokéstops" ou "gyms" oficiais, além de criar um "Pokémon Go Frappuccino [...] a iguaria perfeita para qualquer praticante de Pokémon em ação". Outro acordo, dessa vez com a cadeia de celulares Sprint, converteria 10.500 lojas e pontos da empresa em Pokémon hub. A empresa de streaming de música Spotify anunciou que as músicas relacionadas com Pokémon tiveram a venda triplicada. Uma seguradora do Reino Unido ofereceu cobertura especial para telefones celulares, com o seguinte aviso: "Não deixe que um dano acidental atrapalhe você de capturar todos eles.

Outrossim, os algoritmos se tornaram mediadores da comunicação e das interações nas plataformas (SILVEIRA, 2019), conforme demonstrado no tópico 2.1.2.

Como aponta SILVEIRA, os algoritmos "*praticam a seleção dos públicos e pretendem obter a modulação das opiniões e dos comportamentos*" (2019, p. 76). FRAZÃO (2021b, apud ACEMOGLU, 2021), de igual modo, afirma, com relação à manipulação comportamental, que:

> (...) dados e técnicas sofisticadas de machine learning possibilitam que empresas identifiquem e explorem vieses e vulnerabilidades que os próprios consumidores não reconhecem, empurrando-os para níveis menores de utilidade, transferindo *surplus* dos consumidores para as plataformas, distorcendo a composição do próprio consumo e criando ineficiências.

É possível citar como um exemplo de modulação de comportamentos o vício causado pelo aplicativo TikTok, um aplicativo de mídia social que permite aos usuários criar vídeos e compartilhá-los com amigos, e tem se tornado um dos aplicativos de vídeo mais baixados, com jovens representando metade dos 500 milhões de usuários mensais. Somente no ano de 2019, 16,3 milhões de pessoas baixaram o aplicativo (ZAHRA et al., 2022).

O TikTok oferece conteúdos personalizados com base na análise das preferências dos usuários, recurso que faz desse entretenimento um vício para usuários jovens (ZHANG et al., 2019). Pesquisas demonstram que a utilização de algoritmos leva ao desenvolvimento de uma dependência, na medida em que essa ferramenta proporciona conteúdo personalizado sem a necessidade de procurá-lo (MIRANDA et al., 2023 apud Yang, 2020).

Esse vício, conforme demonstrado por uma pesquisa realizada em Lahore, no Paquistão, tem comprometido a saúde mental de jovens estudantes, pois resulta em diferentes problemas de saúde física e mental, como problemas de visão, sensação de solidão, dores de cabeça, estresse, depressão e ansiedade, além de comprometer o desempenho acadêmico (ZAHRA et al., 2022 apud MUSSARAT et al., 2022).

Matthew Brennan, autor da obra *Attention Factory,* explica que o sucesso do aplicativo TikTok decorre diretamente da experiência de renomados engenheiros, eis que, é por meio de algoritmos que o aplicativo "aprende" os gostos do usuário e passa a exibir conteúdos compatíveis com essa preferência, tornando-o um aplicativo mais atrativo que outros e viciante. Matthew Brennan afirma, ainda, que essa tecnologia está em seu início e deve prevalecer, tornando-se ainda mais viciante (ORGAZ, 2020). Mas características que causam vício não se restringem ao TikTok, sendo comuns a diversas outras redes sociais.

No Facebook, há ferramentas interativas específicas, como likes, que permitem a satisfação de várias necessidades, levando ao uso intensivo das redes sociais e ao desejo constante de buscar as mesmas gratificações (MIRANDA, 2023, apud MASUR et al., 2014).

Ademais, no que tange ao conteúdo consumido nas redes sociais, mostra-se problemática a predição dos algoritmos pois, com a precisão do Big Data, os algoritmos podem conhecer os indivíduos e de forma mais profunda e melhor traçar seus gostos e opiniões do que eles próprios (SILVEIRA 2019, p. 78). Esse poder preditivo, de acordo com SILVEIRA (2019, p. 78), pode empobrecer a criatividade e representar uma servidão maquínica:

> Essa transferência automatizada da nossa capacidade de escolha para um sistema algorítmico se baseia na fé cega no processamento veloz de uma grande e variada quantidade de dados. Retira do inusitado a possibilidade de nos sensibilizar, pois mesmo que uma pessoa nunca tenha gostado de certo estilo musical não significa que ela não será atraída por uma

> música desse estilo. A filtragem algorítmica e a produção de bolhas, ou melhor, de públicos calculados, é empobrecedora da realidade, principalmente da criatividade. Trata-se de uma manifestação da servidão maquínica (SILVEIRA, 2019, p. 78).

Para além de moldar consciências para consumir determinados produtos ou conteúdos nas redes sociais, é necessário abordar a intensa preocupação com a própria democracia diante do advento da *data-driven economy*.

Ao passo em que se verificou um processo de inclusão no meio político baseado na persuasão, e não mais na violência, com o advento de meios de comunicação como a televisão e o rádio, se observou o potencial dos meios de comunicação em massa para o controle da informação. Não por outro motivo as elites econômicas e políticas logo assumiram a propriedade dos grandes meios de comunicação em massa. Com a internet e as mídias digitais, houve uma mudança nesse ambiente, que passou a propiciar novas formas de poder persuasivo (FRANCOSKI; TASSO, 2021).

Pôde-se observar diversos movimentos, como a Primavera Árabe, que demonstraram o poder dos novos meios de comunicação com o advento da informática e das redes sociais para articular eventos em prol da democracia. Todavia, deve-se ter em mente que as redes sociais não se prestam apenas às forças democráticas, mas também à organização de discursos antidemocráticos (SILVEIRA, 2019, p. 32).

Em 2016, nas eleições que se deram nos Estados Unidos da América e nas eleições de 2018, no Brasil, a utilização de técnicas avançadas de segmentação na propaganda eleitoral, especialmente por meio da agregação de grandes volumes de dados provenientes de diversas fontes, com o propósito de delinear microssegmentos do eleitorado, suscita questionamentos acerca da capacidade da democracia de resistir à destruição dos parâmetros da realidade, que anulam o debate e o substituem por um confronto de pós-verdades. No contexto brasileiro, sistemas algorítmicos sofisticados foram empregados para identificar indivíduos ou grupos de WhatsApp que poderiam ser suscetíveis a determinadas informações, mesmo que falsas, exageradas ou completamente fabricadas (SILVEIRA, 2019, p. 32-33).

Afinal, como é possível que o debate democrático seja realmente democrático na realidade de manipulação informacional, em que cada cidadão recebe uma versão dos fatos, muitas vezes sem qualquer correspondência com o que realmente está

ocorrendo e com o que é comprovado cientificamente. Para além disso, é possível que haja um debate consciente, em um contexto em que há técnicas que influenciam e trabalham o subconsciente dos indivíduos e em que esses podem ser facilmente direcionados e ludibriados a atingir o interesse de outros agentes em detrimento dos seus próprios? (FRAZÃO et al., 2022, p. 8).

Mostra-se desafiador para os indivíduos manter sua soberania em um contexto no qual companhias detêm conhecimentos acerca deles que, muitas vezes, eles próprios não possuem e uma vez que esses dados podem ser utilizados não somente para conhecer suas preferências, mas, por um processo inverso, moldar, modificar ou mesmo manipular suas opiniões e crenças (FRAZÃO, p. 21, 2018a).

Se a liberdade de expressão é importante para a democracia, igualmente relevante é a liberdade de visualização. Por meio da liberdade de visualização, os indivíduos têm o direito de ver, ouvir e ver conteúdos políticos sem que estes sejam fruto de um filtro, por algoritmos de plataformas, cujos critérios e parâmetros são obscuros (SILVEIRA, 2019).

Todavia, pesquisas mostram que plataformas têm ativamente impulsionado conteúdos que favorecem candidatos e ideologias. O Twitter constatou que os seus algoritmos favorecem conteúdos de direita em detrimento dos conteúdos de esquerda (ALGORITMOS, 2023) e o Youtube privilegia vídeos da Jovem Pan a favor da campanha do ex-presidente e então candidato à época, Jair Bolsonaro, conforme aponta pesquisa do NetLab da Universidade Federal do Rio de Janeiro (YOUTUBE, 2022).

Esses episódios mostram-se mais preocupantes ao se analisar à luz do efeito da verdade, descrito por FRAZÃO (2023, apud WOLTERS et al., 2021), como uma condição por meio da qual uma informação é mostrada em diversas oportunidades a um indivíduo, fazendo com que se torne mais familiar, aumentando, assim, a probabilidade de o indivíduo considerá-la como uma verdade.

Nas democracias industriais a liberdade de imprensa mostra-se essencial para supervisionar o poder estatal e a própria democracia por meio da difusão de pontos de vista divergentes e de críticas ao governo, mas, nas sociedades controladas por tecnologias de Big Data, há uma dicotomia: os indivíduos são livres para acessar conteúdos, mas esses conteúdos são restringidos por algoritmos (SILVEIRA, 2019).

As empresas que comandam a internet e dirigem o fluxo de capital estão influenciando o nosso pensamento e cultura e fazem isso nas sombras (PASQUALE,

2015). As plataformas, que se apresentam como meras ferramentas técnicas, neutras e imparciais, colocam, na verdade, o lucro acima do interesse público (SILVEIRA, 2019). Assim, é possível concluir de forma inequívoca que o progresso tecnológico representa perigos inéditos à salvaguarda dos cidadãos, notadamente no que tange ao âmbito do direito fundamental à privacidade (consagrado no artigo 5º, inciso X, da Constituição Federal de 1988), por meio da obtenção de acesso a informações relativas ao indivíduo e do emprego que delas se faz (MARTINS, 2020).

Martins (2020) leciona, acerca desses novos perigos, que:

> A tecnologia empregada na Internet propicia novos riscos, em situações em que há atentado à privacidade dos indivíduos por meios antes inimagináveis, a partir de eventos como o rastreamento digital das informações acessadas, inclusive por meio dos cookies, o envio de mensagens não solicitadas (Spam), entre outros.

Podemos salientar, ainda, a violação à dignidade da pessoa humana perante o controle informacional das plataformas, uma vez que prejudicado o direito à autodeterminação.

Alexandre de Moraes (2003, p. 41) traça um paralelo entre a dignidade e a autodeterminação, *in verbis*:

> A dignidade é um valor espiritual e moral inerente à pessoa, que se manifesta singularmente na autodeterminação consciente e responsável da própria vida e que traz consigo a pretensão ao respeito por parte das demais pessoas, constituindo-se um mínimo invulnerável que todo estatuto jurídico deve assegurar, de modo que, somente excepcionalmente, possam ser feitas limitações ao exercício dos direitos fundamentais, mas sempre sem menosprezar a necessária estima que merecem todas as pessoas enquanto seres humanos.

Conforme ressalta FRAZÃO (2018b), são numerosas as preocupações que surgem em relação aos direitos dos usuários decorrentes da *data-driven economy*, já que as informações pessoais, frequentemente recolhidas de maneira ilegal, sem o conhecimento e consentimento informado dos titulares, estão se tornando, cada vez mais, elementos essenciais da economia atual.

Desse modo, conclui-se que resta comprometida não somente a privacidade dos usuários, mas também a sua identidade individual, a capacidade de controlar as suas próprias informações, a liberdade, as oportunidades e as perspectivas presentes e futuras das pessoas, e até mesmo a democracia em si (FRAZÃO, 2018b), na medida em que não há nada de democrático na operação oculta dos algoritmos no controle

de conteúdos nas redes sociais online — a modulação algorítmica da opinião pública, na verdade, representa um grande perigo para a democracia (SILVEIRA, 2019).

3. O ORDENAMENTO JURÍDICO BRASILEIRO

O presente capítulo busca discutir acerca do ordenamento jurídico brasileiro e suas limitações, abordando (3.1.) as disposições do Marco Civil da Internet no que tange à privacidade e à responsabilidade civil das plataformas; (3.2) as regras do Código Civil no tocante à responsabilidade civil; e (3.3.) as regras da Lei Geral de Proteção de Dados. Por fim, a partir dessas reflexões, será respondida a questão (3.4.) faz-se necessária uma regulação mais robusta?

3.1. O Marco Civil da Intenet

O Marco Civil da Internet prevê, em seu artigo 3º, incisos II e III, "a proteção da privacidade" e "a proteção de dados pessoais, na forma da lei", como princípios que disciplinam o uso da internet no Brasil.

Em seu artigo 7º, inciso VI, a lei assegura ao usuário "informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade". No inciso VII do mesmo artigo, a lei ainda garante o "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei". O inciso IX prevê ser necessário o "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais" e, por fim, o inciso X assegura a "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais".

Embora sejam importantes as disposições do Marco Civil da Internet no que tange à privacidade, a ausência de precisão de tais normas confere pouca segurança jurídica e fragiliza a tutela dos dados pessoais (FRAZÃO, 2021a). Ou seja, o Marco

Civil da Internet mostra-se insuficiente na proteção de dados pessoais, característica essa que é inerente ao objeto da lei, já que não foi editada com o propósito de conferir essa proteção (OLIVEIRA; COTS, 2021), sendo relevantes para tanto as disposições da LGPD (FRAZÃO, 2021a).

Nessa linha, se a violação à privacidade proporciona aos detentores de poder informações sobre usuários e, consequentemente, meios para influenciar consciências, conforme demonstrado no capítulo 2, evidencia-se que o Marco Civil da Internet não é capaz de dar uma resposta adequada à problemática da manipulação e das violações ao livre-arbítrio, justamente por ser insuficiente para conferir adequada proteção aos dados pessoais.

Para além disso, no que tange à responsabilidade civil, deve-se salientar que o Marco Civil da Internet teve suas disposições sintetizadas com base em uma estrutura principiológica e com intensa preocupação com a liberdade de expressão, de modo que preconiza "*a necessidade de se garantir um discurso livre e plural na rede que não sofra uma indevida interferência externa ou uma eventual censura prévia"* (TEFFÉ, 2015, p. 5).

Nos artigos 19, 20 e 21, há previsões sobre o regime de responsabilidade civil dos provedores de aplicações de internet em relação aos danos decorrentes do conteúdo inserido por terceiros (TEFFÉ, 2015). Ao provedor de acesso foi conferida a exonerabilidade civil em relação aos danos ocasionados pelos usuários, por meio do artigo 18. O artigo 19, por sua vez, estabelece minuciosamente a regulação da responsabilidade civil dos provedores de conteúdo, como, por exemplo, páginas da internet que armazenam arquivos fotográficos e musicais e blogs (TOMASEVICIUS, 2016).

Essas regras emergiram da necessidade de regular os conflitos suscitados pelas redes sociais virtuais, como o Orkut e o Facebook, quando terceiros disseminavam conteúdos prejudiciais ou criavam perfis falsos causando danos a terceiros. Nesse caso, o autor do conteúdo ofensivo, se devidamente identificado, será responsabilizado de forma direta e pessoal, nos termos dos artigos 186, 187 e 927 do Código Civil (TEFFÉ, 2015).

O artigo 21 estabeleceu ser subsidiária a responsabilidade entre o usuário da internet que praticou o ato ilícito civil e o provedor de conteúdo. Assim, a responsabilidade primordial recai sobre o usuário da internet, de modo que o provedor de conteúdo responde de forma conjunta ao causador do dano tão somente quando

descumprir uma ordem judicial para tornar indisponível o conteúdo ofensivo (TOMASEVICIUS, 2016).

Ou seja, as normas do MCI não se ocupam da responsabilidade pelos próprios conteúdos dos provedores, mas sim dos conteúdos produzidos por terceiros (TEFFÉ, 2015). É nítido, pois, que essas regras não visam a tratar sobre os danos decorrentes da própria atuação das plataformas ao gerir os conteúdos exibidos aos seus usuários e, tampouco, a coibir eventuais violações ao livre arbítrio.

Na verdade, como se vê, as disposições do MCI partem do pressuposto de que as plataformas digitais desempenham uma função passiva no fluxo informacional. Isso, todavia, é uma premissa equivocada, uma vez que as plataformas regulam discurso emanado por seus usuários e impõem a eles políticas e termos de serviço, bem como exercem papel moderador de conteúdos ilícitos automaticamente, antes ou depois da publicação (FRAZÃO, 2021a).

Os danos e as consequentes violações à privacidade, à autonomia e à liberdade, decorrentes da atuação das próprias plataformas digitais, e não de terceiros, explicitadas no capítulo anterior, não estão sujeitas ao regime de responsabilidade do MCI (FRAZÃO, 2021a).

O regime de responsabilidade das plataformas pela gerência de seus conteúdos, portanto, deve ser interpretado à luz das disposições do Código Civil, Código de Defesa do Consumidor, Estatuto da Criança e do Adolescente, e da Lei Geral de Proteção de Dados (FRAZÃO, 2021).

3.2. O Código Civil de 2002

Conforme elucidado no tópico anterior, as disposições do Marco Civil da Internet apenas exoneram as plataformas de responsabilidade nas hipóteses de conteúdo veiculado por terceiros. Desse modo, tratando-se de dano acarretado por uma ação da própria plataforma, incidem, as disposições do Código Civil de 2002 – em tese.

A Lei nº 10.406/2002 (Código Civil) dispõe, em seu artigo 927, que "*aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo*". Por sua vez, os atos ilícitos são conceituados por meio dos artigos 186 e 187, *in verbis*:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
>
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

Todavia, para que haja o dever de reparar o dano causado, "*segundo a doutrina e jurisprudência pacíficas, não basta o ato ilícito. Dele deve decorrer um dano, seja de ordem material, como moral*" (STOCO, 2015).

Portanto, os elementos formadores da obrigação de reparar são: "*um comportamento (ação ou omissão) do agente, o elemento subjetivo (dolo ou culpa), o nexo de causalidade entre a conduta e o resultado e a ocorrência de um dano efetivo, seja de ordem patrimonial ou extrapatrimonial (moral)*" (STOCO, 2015).

Conforme demonstrado no Capítulo 2, as plataformas, ao exercerem uma curadoria personalizada da informação, acarretam em uma violação genérica à liberdade ou ao livre-arbítrio, que pode ser interpretada pormenorizadamente como violações à liberdade, à privacidade e à dignidade da pessoa humana.

Desse modo, resta evidente a existência de um ato ilícito que decorre do uso da tecnologia e, em especial, das redes sociais, para extrair dados e tentar moldar comportamentos, de modo que é inequívoco que há o primeiro requisito para ensejar a obrigação de reparar o dano, qual seja, o ato ilícito. No entanto, a eventual responsabilização de plataformas por tal ato ilícito esbarra na comprovação do dano, na impossibilidade de se aferir as suas reais proporções e, ainda, em demonstrar o nexo de causalidade. Explica-se.

Afigura-se praticamente impossível estimar as reais proporções do dano para que se possa repará-lo nessa medida, uma vez que os danos são causados a todos aqueles que utilizam dos serviços das plataformas digitais e são impactados pela extração e utilização de seus dados para fins de alteração comportamental.

Outro desafio para que o Código Civil seja suficiente e possa dar adequado tratamento à problemática da manipulação é a exigência de demonstração do nexo de causalidade, que é a interligação de um evento ocorrido anteriormente, qualificado como causa, e outro evento subsequente, qualificado como efeito, isto é, o dano. Isso porque a relação entre esses dois eventos não é uma mera associação entre os fenômenos: trata-se de uma relação na qual um evento específico (a causa) determina a sucessão de outro fenômeno específico (o efeito) (MARINONI et al., 2016).

Entre a causa e o feito se dá uma relação denominada nexo causal, nexo de causalidade ou nexo etiológico. Essa relação não é um evento empírico observável ou perceptível e, por esse motivo, é considerada pela doutrina como o elemento mais complexo da responsabilidade civil (MARINONI et al., 2016). Ou seja, o nexo de causalidade é um "*vínculo obrigatório entre o fato (causa) e o dano (efeito)*" (SANSEVERINO, 2010, p. 153) e, sem ele, não é possível se reconhecer a obrigação de indenizar (MARINONI et al., 2016).

Não obstante haja diversos critérios para se aferir o nexo de causalidade (MARINONI et al., 2016), é particularmente desafiador demonstrar o nexo de causalidade entre a ação das plataformas de exercer controle sobre o conteúdo exibido aos usuários, e um eventual efeito, qual seja, a manipulação abordada no Capítulo 2.

Veja-se como exemplo o impulsionamento de conteúdos de direita por algoritmos do Twitter. Mesmo que tenha sido comprovado que houve um controle informacional por algoritmos visando a favorecer uma determinada ideologia, não é possível demonstrar efetivamente o alcance do conteúdo de direita aos indivíduos, isto é, quantos foram os indivíduos que visualizaram aquele conteúdo, quais deles foram efetivamente influenciados por ele, em que medida se deu essa influência e, consequentemente, qual foi o real impacto desse conteúdo sobre o pleito e a democracia.

Nesse passo, é improvável demonstrar um nexo causal, na medida em que não se pode ligar a causa (o impulsionamento de conteúdos de direita pelo Twitter) diretamente o efeito (usuários influenciados), até mesmo porque há diversos outros aspectos da vida que poderiam acarretar a mudança de opinião ideológica de um determinado indivíduo.

Mas, mesmo que se comprovasse o nexo causal, a responsabilização das plataformas pelas violações pelos atos ilícitos consistentes na exploração de dados para moldar comportamentos vai de encontro ao próprio propósito da responsabilidade civil. Senão vejamos.

CRETELLA JR. (1980, p. 8) afirma que a pessoa que infringe a norma deve reparar o dano causado e essa reparação consiste "*na volta ao status quo ante da produção do dano*".

Por conseguinte, se a reparação consiste no retorno ao *status quo ante*, não é possível reparar uma manipulação de consciências gerada pelo controle

informacional. Ora, não há que se falar no retorno ao *status quo ante* em tratando-se da problemática ora exposta, uma vez que é inviável e ilógico que as consciências sejam "desmoldadas" ou que as ações dos indivíduos, tomadas em decorrência de uma manipulação, sejam desfeitas.

Naqueles casos em que não é possível o retorno ao *status quo ante*, STOCO (2015) leciona que "*se indeniza pelo equivalente em dinheiro*". No entanto, a possibilidade de se indenizar monetariamente, quando analisada à luz da problemática da manipulação e das consequentes violações ao livre arbítrio, também não se mostra viável e adequada já que sequer é possível aferir as proporções do dano causado, sendo, portanto, inviável estimar uma quantia capaz de indenizá-lo.

Conclui-se, portanto, que as disposições do Código Civil são limitadas no que tange à reparação dos danos causados pelas plataformas ao gerenciarem conteúdos e direcionar os indivíduos de modo a atingir determinados interesses.

3.3. A Lei Geral de Proteção de Dados

3.3.1 Princípios

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), por meio de seu artigo 1º, dispõe como objetivo "*proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural*". Em seguida, em seu artigo 2º, a Lei elenca diversos fundamentos além do respeito à privacidade, quais sejam, a autodeterminação informativa (inciso II); a liberdade de expressão, de informação, de comunicação e de opinião (inciso III); a inviolabilidade de intimidade, da honra e da imagem (inciso IV); o desenvolvimento econômico e tecnológico e a inovação (inciso V); a livre iniciativa, a livre concorrência e a defesa do consumidor (inciso VI); e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (inciso VII).

Ao fazer menção explícita ao livre desenvolvimento da personalidade, à cidadania e à dignidade, a legislação busca inibir categoricamente as atuais designações atribuídas aos dados pessoais, uma vez que esses, ao serem submetidos ao processamento por algoritmos, possuem a capacidade de efetuar diagnósticos e classificar usuários, o que, por conseguinte, pode levar à uma certa

restrição de suas perspectivas de vida. Para além disso, a partir desses dados, empresas podem discriminar usuários ou mesmo ensaiar manipulações de suas opiniões, crenças ou valores em diversos âmbitos, inclusive no campo político (FRAZÃO, 2018b).

Assim, a LGPD visa a resguardar integralmente o usuário-cidadão em todos os âmbitos de sua autonomia pública e privada, ao valorizar e salvaguardar sua autodeterminação informacional e seu poder de tomada de decisões. Consequentemente, esse princípio torna-se um ponto nodal, em torno do qual todas as demais disposições previstas na legislação devem ser interpretadas (FRAZÃO, 2018b).

No que tange aos conceitos-chave utilizados pela Lei, ressalta-se o conceito de dado pessoal, classificado como "*informação atinente a pessoa natural identificada ou identificável*" (art. 5º, I) e dado pessoal sensível, definido como dado que versa acerca de "*origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a pessoa natura*l" (art. 5º, II) (FRAZÃO, 2018b).

Outrossim, a LGPD instituiu a figura do titular dos dados que é, de acordo com o art. 5º, V: "*pessoa natural a quem se referem os dados pessoais que são objeto de tratamento*". A titularidade dos dados, prevista pela LGPD, é acompanhada por um conjunto de direitos concebidos para permitir ao titular o seu exercício perante aqueles que possuírem seus dados (OLIVEIRA; COTS, 2021).

Ademais, podemos elencar como conceito-chave o termo tratamento (FRAZÃO, 2018b), que, nos termos do art. 5º, X, é "*toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração*".

O tratamento de dados enquanto conceito empregado pela LGPD é extremamente amplo, proporcionando a compreensão de que a Lei, em conformidade com o seu artigo 3º, é aplicável a qualquer atividade referente ao processamento de dados, seja conduzida por pessoa natural ou por pessoas jurídicas de direito público ou privado, independentemente do meio empregado, da localização em que se dá a manipulação dos dados, e outros aspectos (FRAZÃO, 2018b).

Os princípios instituídos pela LGPD são de grande importância pois regulam de forma ampla uma matéria que antes apenas existia no ordenamento jurídico brasileiro de forma lateral (OLIVEIRA; COTS, 2021), além de servirem de apoio para a interpretação das demais regras contidas na Lei (FRAZÃO, 2018b).

Antes de adentrar nos princípios da LGPD propriamente ditos, cumpre explicitar o que são princípios:

> princípios, no plural, significam as normas elementares ou os requisitos primordiais instituídos como base, como alicerce de alguma coisa [...] revelam o conjunto de regras ou preceitos, que se fixam para servir de norma a toda espécie e ação jurídica, traçando, assim, a conduta a ser tida em qualquer operação jurídica [...] exprimem sentido mais relevante que o da própria norma ou regra jurídica [...] mostram-se a própria razão fundamental de ser das coisas jurídicas, convertendo-as em perfeitos axiomas [...] significam os pontos básicos, que servem de ponto de partida ou de elementos vitais do próprio Direito. (DE PLACIDO E SILVA, 2001, p. 639)

FRAZÃO (2018b), elenca os seguintes princípios no tratamento de dados no Brasil, além da boa-fé objetiva, a partir da interpretação do art. 6º da LGPD:

> (i) princípio da finalidade, descrito como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (inciso I);
> (ii) princípio da adequação, descrito como a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (inciso II);
> (iii) princípio da necessidade, descrito como a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (inciso III);
> (iv) princípio do livre acesso, descrito como a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais" (inciso IV);
> (v) princípio da qualidade dos dados, descrito como a "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento" (inciso V);
> (vi) princípio da transparência, descrito como a "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial" (inciso VI);
> (vii) princípio da segurança, que exige "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (inciso VII);
> (viii) princípio da prevenção, traduzido na "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (inciso VIII);
> (ix) princípio da não discriminação, que consiste na "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (inciso IX);

> (x) princípio da responsabilização e prestação de contas, que exige "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

Analisando os princípios da LGPD à luz da problemática ora trabalhada, temos que apesar da inexistência de qualquer disposição expressa acerca da utilização de algoritmos por empresas, os princípios previstos na LGPD indicam ser imprescindível um tratamento transparente e a prestação de contas sobre o meio utilizado para o tratamento dos dados (FRAZÃO, 2018b). No entanto, embora a LGPD preveja ser necessária transparência no controle informacional realizado pelas redes sociais, pode-se concluir, a partir do exposto no Capítulo 2, que não é o que se vê.

Há exceções ao princípio da transparência: os segredos de negócios, o que pode gerar dúvidas acerca da compatibilização dos princípios em jogo (FRAZÃO, 2018b). Afinal, podemos classificar os algoritmos utilizados pelas redes sociais como um segredo de negócios e, nessa medida, não informar aos consumidores o modo com que os conteúdos estão sendo filtrados e exibidos, bem como para qual finalidade os seus dados pessoais estão sendo empregados?

O problema da compatibilização surge do fato de que a análise dos princípios previstos pela LGPD em seu art. 6º deve se dar à luz dos fundamentos do art. 2º (FRAZÃO, 2018b). Ao mesmo tempo em que a LGPD prevê como princípio para o tratamento de dados pessoais a transparência (art. 6º, VI), há também a proteção ao desenvolvimento econômico e tecnológico e a inovação (art. 2º, V). Nessa linha, sendo os algoritmos que classificam conteúdos nas redes sociais com base em informações pessoais uma inovação tecnológica, poderia ser priorizado o desenvolvimento tecnológico em detrimento da transparência?

Eis, portanto, que é improvável que os objetivos de livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania (art. 2º VII) possam ser facilmente alcançados diante da nova realidade na qual o tratamento de dados se dá via algoritmos (FRAZÃO, 2018b). FRAZÃO (2018b), afirma, nesse sentido que:

> (...) sem maior transparência e accountability sobre os algoritmos, não se tem como assegurar a eficácia de vários dos princípios elencados pela lei, incluindo os que exigem que o meio utilizado para o tratamento de dados atenda aos requisitos da necessidade, adequação e proporcionalidade, assim como o que veda discriminações ilícitas ou abusivas.

Assim, sem que haja transparência sobre como os dados são utilizados e tratados por algoritmos, os riscos decorrentes desse tratamento não podem ser suficientemente identificados e quanto menos podem ser mitigados (FRAZÃO, 2018b).

3.3.2. Bases legais de tratamento de dados pessoais

Para que seja possível tratar dados pessoais, é necessário que o tratamento esteja embasado em uma das hipóteses legais da LGPD, referenciadas como bases legais ou jurídicas. Excetuando-se as hipóteses previstas no art. 4º da LGPD, o tratamento de dados pessoais só pode ser feito havendo o enquadramento em uma das bases legais do art. 7º. No caso do tratamento de dados sensíveis, há oito bases legais e, para o tratamento de dados pessoais não sensíveis ou comuns, há dez bases legais. O rol do art. 7º é exaustivo, de modo que não há outras bases além das citadas. (OLIVEIRA; COTS, 2021).

Uma das bases legais para o tratamento de dados é o consentimento, isto é, a manifestação de vontade do titular no sentido de permitir o tratamento de seus dados, conceituada no art. 5º e eleita como base legal no art. 7º, I. A manifestação do titular deve ser por meio escrito ou por uma forma que possibilite a preservação de seus dados básicos, como o que está sendo consentido e o prazo do tratamento. As outras bases previstas pela LGPD independem da autorização do titular para o seu tratamento, podendo ocorrer mesmo sem a anuência do titular (OLIVEIRA; COTS, 2021).

O consentimento deve ser altamente qualificado, uma vez que a manifestação de vontade deve ser necessariamente livre e inequívoca; formada mediante o conhecimento de todas as informações necessárias para tal, o que inclui a finalidade do tratamento; e, por fim, restrita às finalidades específicas e determinadas. Se houver qualquer alteração nas circunstâncias que justifiquem o consentimento do titular, como a finalidade específica do tratamento e a forma, deve haver novo consentimento, nos termos do art. 8º, §6º. Ou seja, excetuando-se aquelas informações consideradas como segredo comercial ou industrial, as outras informações devem ser repassadas ao titular para que haja o consentimento informado (FRAZÃO, 2018c).

Todavia, no tocante ao consentimento, SOLOVE (2013), afirma que por mais que a autogestão da privacidade seja um componente necessário em um regime

regulatório, ela não é capaz de fornecer às pessoas controle significativo sobre seus dados, eis que, muitas vezes, os indivíduos não são capazes de tomar decisões informadas e racionais sobre os custos e benefícios de consentir na coleta, uso e divulgação de seus dados pessoais.

Conforme ressalta CASTRO (2020), as plataformas que porventura se utilizarem de termos de uso genéricos, de acordo com as novas disposições da LGPD, se sujeitarão à anulação de tais termos:

> O primeiro impacto da nova legislação já é perceptível no momento em que o usuário autoriza a utilização de seus dados. Os termos de uso pouco claros ou genéricos serão considerados nulos. Assim, os aspectos relativos à utilização de dados deverão ter consentimento específico, destacado dos demais termos de utilização da plataforma.

Mas mesmo que os termos de uso das plataformas não sejam genéricos, conforme assevera SOLOVE (2013), há problemas estruturais que fazem com que indivíduos, mesmo bem informados, não sejam capazes de autogerenciar adequadamente sua privacidade, como o fato de os termos de serviço das plataformas conterem linguagem jurídica e muitos termos técnicos. Desse modo, na maior parte das vezes, não há uma explicação clara aos usuários sobre o impacto que o uso de certas tecnologias, como *cookies*, por exemplo, pode ter nos direitos dos usuários (SOLOVE, 2013).

No mesmo sentido, SUZOR (2018, p. 3) afirma, sobre o consentimento que:

> (...) os usuários têm pouquíssimos meios legais para reclamar sobre como as plataformas são governadas. Os usuários são considerados consumidores que voluntariamente aceitaram os termos de participação em redes privadas. Ao aceitarem e adotarem esses termos, os usuários estão legalmente vinculados por eles. A resposta legal para as preocupações que os usuários têm sobre a governança das plataformas é, em grande parte: se você não gosta, saia.

Assim, podemos concluir, à luz do problema da manipulação e do controle informacional que ocorre de forma personalizada a partir da coleta de dados, que o consentimento se mostra uma base de tratamento incapaz de coibir o real problema pois os indivíduos não são bem informados dos riscos decorrentes desse tratamento, podendo anuir com sua própria manipulação por não possuir informações suficientes.

Além do consentimento, são bases para o tratamento de dados pessoais: o cumprimento de obrigação legal ou regulatória (art. 7º, II); políticas públicas (art. 7º, III); órgão de pesquisas (art. 7º, IV); execução de contratos (art. 7º, V); exercício

regular de direitos (art. 7º, VI); proteção da vida (art. 7º, VII); tutela da saúde (art. 7º, VIII); legítimo interesse (art. 7º, IX); e proteção ao crédito (art. 7º, X).

O legítimo interesse é previsto como base jurídica de tratamento de dados pessoais no art. 7º, inciso IX, da LGPD. Quando baseado no legítimo interesse, cabe aos controladores e operadores registrarem as operações de tratamento de dados pessoais que realizarem (art. 37), uma vez que, por ser a base mais subjetiva, inevitavelmente tem maior potencial de gerar riscos aos titulares dos dados (OLIVEIRA; COTS, 2021).

Todavia, ainda que maior o potencial de riscos, a criação do legítimo interesse enquanto base legal de tratamento representou medida essencial para que o empreendedorismo e a inovação não sofressem ainda mais o abalo do advento da LGPD, eis que há, por exemplo, banco de dados amplos que não se encaixavam em nenhuma outra base legal de tratamento e, embora férteis, poderiam se tornar inúteis com a nova Lei (OLIVEIRA; COTS, 2021).

O legítimo interesse não resta definido expressamente pela LGPD, de modo que deve-se entendê-lo em seu sentido literal, ou seja, interpretar a partir de “interesse”, como sendo algo importante para alguém, e “legítimo”, como um interesse justificado ou amparado pelo bom senso, costumes, ou pelo ordenamento jurídico (OLIVEIRA; COTS, 2021).

Os requisitos para o tratamento de dados com base no legítimo interesse estão previstos no art. 10º, e outros requisitos foram identificados a partir da legislação europeia, sendo eles: Interesse do Controlador ou de Terceiros, Finalidades Legítimas, Situações Concretas, Proteção dos Direitos do Titular ou Benefício ao Titular, observando-se a Legítima Expectativa dele, o Princípio da Necessidade e o Princípio da Transparência (OLIVEIRA; COTS, 2021).

Nesse sentido, não é possível que a finalidade do tratamento de dados baseado no legítimo interesse seja alterada, de modo que, por exemplo, não é possível que o legítimo interesse demonstrado inicialmente para o armazenamento de dados, após, seja utilizado para justificar o encaminhamento de promoções ou mensagens aos titulares (OLIVEIRA; COTS, 2021).

Ademais, também não é possível que o Operador utilize a base jurídica do legítimo interesse, já que o legítimo interesse só pode ser exercido se atender a um ou mais Interesses do Controlador, que é o ente que decide sobre o tratamento, não

do Operador, que é o ente que cumpre as determinações do primeiro (OLIVEIRA; COTS, 2021).

No entanto, apesar das disposições da LGPD que visam a fornecer maior proteção aos usuários, já que a base jurídica do legítimo interesse mostra-se extremamente subjetiva, é importante não perder de vista que, a partir do art. 2º da LGPD, são assegurados o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência.

Desse modo, o lucro pode ser utilizado como aspecto a justificar o tratamento de dados pessoais com base no legítimo interesse, sem que seja necessário o consentimento do titular dos dados (OLIVEIRA; COTS, 2021).

A partir disso, é necessário refletir sobre a desnecessidade do consentimento do titular em se tratando do tratamento dos dados pessoais com base no legítimo interesse justificado, na hipótese tal interesse configurar a perseguição do lucro. Afinal, seria o lucro uma importância crucial a ponto de se afastar a necessidade de consentimento?

É necessário questionar em que medida é possível haver um tratamento de dados pessoais realmente transparente, já que, quando baseado no consentimento, há a problemática atinente à falta de transparência e conhecimentos necessários para que os usuários possam anuir livremente, eis que, os riscos permanecem ocultos. Por outro lado, quando o tratamento se baseia no legítimo interesse, sendo dispensado o consentimento, é possível que tal interesse baseie-se no lucro.

3.4. Faz-se necessária uma regulação mais robusta?

A regulação é, por vezes, falha, conforme pontua OLIVEIRA (2021, p. 1), ao afirmar que o Estado regulador pode substituir “falhas de mercado” por “falhas de governo”, o que, ao seu entendimento, “*pode ser hábil a causar um estrago ainda maior: a diferença entre eles é que a falha de governo é promovida por um agente monopolista e com poder de coerção*”.

No entanto, é nítido que, na atualidade, os pensamentos e emoções dos indivíduos não estão a salvo e podem ser utilizados para manipular e criar consciências e mercados (FRANCOSKI; TASSO, 2021), conforme demonstrado no Capítulo 2. A problemática da manipulação digital pode ainda se intensificar com a evolução constante da neurotecnologia e do desenvolvimento de técnicas de

mapeamento de dados cerebrais (FRANCOSKI; TASSO, 2021), sendo, assim, arriscada a falta de regulação adequada (FRAZÃO, 2023). Nesse sentido, FRANCOSKI e TASSO (2021), ressaltam que:

> (...) na era do "neurocapitalismo", em que nossos pensamentos, desejos e emoções são submetidos a precisos escrutínios e mapeamentos, nossos cérebros precisam, inclusive, de novos direitos. Afinal, no atual contexto, tornou-se desatualizada a ideia defendida por George Orwell em seu famoso livro "1984", de que, no contexto de vigilância, a única coisa que continuava pertencendo verdadeiramente aos cidadãos eram poucos centímetros cúbicos dentro de seus crânios. A ironia dos tempos presentes é que estamos correndo o risco de perder o controle até mesmo sobre esses centímetros cúbicos.

Diante desse cenário, é inequívoco que há limitações inerentes à Lei Geral de Proteção de Dados (FRAZÃO, 2018b), o que faz com que, na atualidade, e, mais ainda no futuro, as suas disposições não sejam suficientes para resolver todos os problemas da *data-driven economy*, muito embora seja uma importantíssima Lei e represente um importante passo para a proteção de dados (FRAZÃO et al., 2022, p. 9). Isso porque, como visto, os problemas que decorrem da exploração de dados pessoais são mais amplos do que a mera violação da privacidade em sentido clássico, trazendo também inúmeros riscos aos indivíduos, como riscos à identidade pessoal, à autodeterminação informativa, à liberdade e às oportunidades (FRAZÃO, 2021a).

Ademais, conforme demonstrado nos tópicos 3.1 e 3.2, o Marco Civil da Internet e o Código Civil também não são se mostram suficientes para oferecer proteção diante da possibilidade de manipulação dos indivíduos e das consequentes violações à liberdade e à autodeterminação.

A partir disso, se conclui ser necessário defender os "direitos da mente", que são assim classificados por FRANCOSCKI e TASSO (2021):

> I) Direito à liberdade cognitiva, que envolve o direito de optar pelo uso ou não da neurotecnologia;
> II) Direito à privacidade mental, que requer a preservação da intimidade da mente, com importantes desdobramentos sobre garantias constitucionais centrais, tais como o direito ao silêncio e o direito de não se autoincriminar;
> III) Direito à integridade mental, segundo o qual ninguém pode ser prejudicado física ou psicologicamente pela neurotecnologia, de modo que se deve evitar qualquer forma de manipulação da mente e, com maior razão, novas modalidades de lavagem cerebral, o que seria extremamente perigoso se utilizado por interessados em propagar doutrinas religiosas, políticas e terroristas, bem como para casos de neuromarketing. O direito à integridade mental também tem importante desdobramento sobre a segurança dos dados cerebrais, a fim de evitar que sejam hackeados ou sequestrados;
> IV) Direito à continuidade psicológica, que diz respeito ao direito de ser protegido contra alterações do seu senso de identidade, como a que ocorreria

> caso a empresa que implantou determinado aparelho no cérebro de alguém, que com ele desenvolveu verdadeira relação de simbiose, falisse e tivesse que remover o equipamento, caso em que haveria uma perda de identidade por parte do usuário.

Eis, portanto, que outras iniciativas se fazem necessárias para além de apenas uma legislação de proteção de dados (FRAZÃO, 2021b). Como aponta PASQUALE (2015), uma vez que usamos a computação não apenas para exercer poder sobre as coisas, mas também sobre as pessoas, precisamos desenvolver uma estrutura ética muito mais robusta, e não é isso o que se vê na atualidade.

Assim, a transparência é necessária para dar inteligibilidade não apenas ao mercado, mas ao mundo como um todo (FRAZÃO, 2019b, apud PASQUALE, 2015). Deste modo, para avançar na regulação jurídica dos mercados, é fundamental a criação de mecanismos de transparência e *accountability*, na medida em que é impossível regular o que não se conhece (FRAZÃO, 2019b). Sendo nítida a necessidade de uma regulação mais robusta, são intensas as discussões sobre o modo com o qual essa regulação deve se dar.

Um método de regulação que se propõe resolver os problemas inerentes ao uso de algoritmos baseia-se na imposição do que se denomina "responsabilidade algorítmica" às entidades responsáveis pelo processamento de dados, a qual se divide em duas fases (FERREIRA, 2018 apud BALKIN; ZITTRAIN, 2016). Essas duas fases são assim descritas por FERREIRA (2018, p. 43 apud BALKIN; ZITTRAIN, 2016):

> Em primeiro lugar, durante a execução dos algoritmos, a sua supervisão seria garantida por entidades independentes, que avaliariam a sua imparcialidade e eficácia, utilizando os métodos técnicos disponíveis. Esta supervisão seria acompanhada de uma transparência para com esta entidade reguladora, que garantiria uma continuação da concorrência face aos rivais do criador do algoritmo. Numa segunda fase, seria permitida a responsabilidade extracontratual nas situações em que o processamento dos dados seja parcial ou incorreto, garantindo-se assim a existência de incentivos à manutenção da imparcialidade e eficácia dos algoritmos.

Outros autores, como AMATO (2021) defendem que para que a regulação de tecnologias digitais seja mais efetiva, o Estado não deve regular diretamente os comportamentos, mas sim, priorizar regular a autorregulação privada das redes sociais. Esse tipo de regulação é chamada de "metarregulação", já que se estaria regulando a autoregulação e, a partir dela, seria possível cobrar as plataformas digitais para que desenvolvessem os mecanismos de responsabilização e os parâmetros de sancionamento devidos em relação a seus usuários (AMATO, 2021).

Seja qual for o modo, qualquer regulação das plataformas digitais que lide com os sistemas e processos de moderação e curadoria de conteúdo deve ter um propósito legítimo e deve, ainda, garantir a liberdade de expressão, o direito ao acesso à informação e outros direitos humanos reconhecidos em tratados e instrumentos internacionais relevantes de direitos humanos, conforme aponta o Guia da Unesco (UNESCO, 2023).

A regulamentação, nesse sentido, deve focar nos sistemas e processos usados pelas plataformas para moderar e curar o conteúdo, em vez de buscar julgar a adequação ou legalidade de peças individuais de conteúdo, para que se possa garantir que as plataformas digitais sejam transparentes sobre os sistemas e processos utilizados para moderar e curar conteúdo em suas plataformas (UNESCO, 2023). Ou seja, não visando a eliminar conteúdos específicos, não há que se falar em risco à liberdade de expressão decorrente da regulação das plataformas digitais.

Ora, não se pode compreender a regulação sobre a forma com que uma *fake news* se propaga como uma forma de censura, mas sim como uma forma de proteger a própria liberdade de expressão e dar transparência ao conteúdo inserido por terceiros (BORGES et al., 2021).

De igual modo, conforme leciona FRAZÃO (2023), "*a preocupação com a liberdade de expressão não se justifica em relação à parte considerável do fluxo informacional nas grandes plataformas, especialmente no tocante às interações que envolvem bots, contas inautênticas, propagandas, conteúdos impulsionados ou pagos, negócios escusos e manipulações*".

Isso porque, conforme já elucidado no capítulo 2 deste trabalho, as operações algorítmicas representam um risco significativo à ordem democrática e à liberdade de expressão e a falta de regulação adequada pode agravar ainda mais esse risco.

Nesse contexto, se são imensos os riscos reais que a falta de regulação apropriada representa para a liberdade de expressão, para o acesso à informação e para a própria democracia, ainda mais grave e arriscado é invocar a liberdade de expressão para ignorar esses riscos (FRAZÃO, 2023).

Sendo assim, é necessário, no tocante à divulgação de *fake news*, que o Direito não só defina os direitos, poderes e responsabilidades, mas que busque definir os próprios canais pelos quais podem ser construídos os programas e órgãos decisórios capazes de lidar com esse fenômeno emergente e com a tipificação dos instrumentos

preventivos e repressivos ao abuso da comunicação digital (AMATO, 2021). O mesmo pode ser aplicado no que tange ao controle informacional pelas redes sociais.

Nesse sentido, conforme aponta o Guia da UNESCO (2023), é essencial que a agência reguladora responsável pelo controle e fiscalização das plataformas digitais seja dotada de *expertise* para que tenha capacidade e conhecimentos técnicos a fim de tomar decisões informadas com base nas diretrizes estabelecidas. Recentemente, o Projeto de Lei 2.768/22, que tramita na Câmara dos Deputados, do deputado João Maia (PL-RN), atribui à Agência Nacional de Telecomunicações (Anatel) o poder de regular o funcionamento e a operação das plataformas digitais que operam no Brasil. O texto cria ainda uma taxa a ser paga pelas grandes empresas do setor (MACEDO, 2023).

A Coalizão Direitos na Rede, que reúne mais de 50 entidades de direitos digitais, se posiciona em sentido contrário à atribuição da regulação das plataformas digitais à Anatel, eis que considera que a Anatel "*não possui competência para regular aplicações de internet e é reconhecida sua falta de expertise no assunto*", que "*falhou em manter o controle do inventário do patrimônio público de bens reversíveis, gerando um prejuízo que pode chegar a R$ 100 bilhões ao tesouro público*", e, ainda, que "*a atuação da sociedade civil na Agência é extremamente dificultada e reduzida*" (COALIZÃO DIREITOS NA REDE, 2023). Portanto, é necessário discutir sobre o ente responsável por fiscalizar as plataformas.

Ademais, os "direitos da mente", descritos por FRANCOSCKI e TASSO (2021), têm sido alvo de iniciativas de proteção por alguns países, como o Chile. O Chile foi o primeiro país a aprovar uma lei de proteção de dados (RAMIRO, 2020) e, em 2021, por meio da Lei nº 21.383, tornou-se o primeiro país a instituir proteção legal aos neurodireitos, isto é, direitos do cérebro ou da mente (SILVA, 2022).

Por sua vez, na Europa, há um projeto que discute a regulação de inteligência artificial e busca proibir o uso de tecnologias associadas a técnicas subliminares que possibilitem a manipulação de indivíduos e, ainda, a exploração de vulnerabilidades de indivíduos, como crianças e pessoas com deficiência (FRAZÃO, 2021b). Por meio desse projeto, a Comissão Europeia propõe que os sistemas de inteligência artificial sejam divididos por categorias, de acordo com o risco que representam para os usuários. Caso aprovada a proposta, a lei será aplicável a indivíduos que desenvolvam e utilizem sistemas de inteligência artificial na União Europeia, mesmo que estejam as companhias desenvolvedoras localizadas fora do bloco (ZIADY, 2023).

No Brasil, o Projeto de Lei nº 2.630/20, conhecido como “PL das Fake News”, mostra a preocupação do legislador de proteger a liberdade de expressão e promover transparência (BORGES et al., 2021).

No que tange à publicidade, é possível notar que, caso aprovado, o PL das Fake News conferirá maior proteção aos usuários das redes sociais. Isso porque, como elucidado no Capítulo 2 do presente trabalho, por vezes, a publicidade pode ser velada, concretizando-se a partir de meios psicológicos complexos, que, conforme ressalta FRAZÃO (2021a), “*fogem à tendência crítica da esfera cognitiva*”. Como exemplo, podemos citar o jogo “Pokemon Go”, que direcionava seus usuários a comércios com o intuito de que consumissem produtos, ao passo em que muitos desses usuários, especialmente os mais novos, poderiam acreditar que somente estavam lá para capturar os Pokémons do jogo.

Em seu artigo 19, o PL das Fake News dispõe que “*é direito do usuário o acesso fácil e direito a informações claras (...) sobre os motivos pelos quais está sendo destinatário de publicidade ou impulsionamento*”. Ainda, no §1º do mesmo artigo, impõe-se às plataformas digitais que ofereçam publicidade o fornecimento aos usuários das “*informações do histórico dos conteúdos impulsionados e publicitários com os quais a conta teve contato nos últimos 6 (seis) meses*”. No que tange à publicidade eleitoral, o PL das Fake News, em seu artigo 25, assegura aos indivíduos o acesso de *“todo o conjunto de anúncios impulsionados*”.

O PL das Fake News visa, ainda, ao “*combate a contas automatizadas não identificadas*”, determinando às plataformas a adoção de medidas técnicas que viabilizem a identificação de contas que apresentem movimentação incompatível com a capacidade humana.

A iniciativa do PL das Fake News é de extrema importância e visa a garantir maior transparência e, em certa medida, coibir a manipulação e as violações ao livre arbítrio ora tratadas. Há um lapso, no entanto, com relação aos conteúdos que não se configuram publicidade, já que as obrigações impostas às plataformas digitais no sentido de dar transparência aos usuários com relação ao conteúdo exibido se restringem a conteúdos publicitários.

Por exemplo, caso um usuário faça um comentário em favor de determinado candidato em uma rede social, essa publicação não configuraria uma propaganda, mas apenas uma opinião. Seria possível, nesse exemplo, que os algoritmos dessa rede social exibissem esse conteúdo a diversos outros usuários, sem qualquer tipo de

transparência, e visando a satisfazer um interesse oculto? Analisando-se as disposições do PL das Fake News, é possível dizer que sim.

Outra iniciativa legislativa no Brasil é o Projeto de Lei nº 21/2020, que visa a estabelecer "*fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil*". Todavia, suas disposições são vagas, de modo que é questionável em que medida tais princípios, como a liberdade e o respeito aos valores democráticos, seriam efetivamente garantidos caso aprovado o projeto.

Outrossim, outros percalços que coloca em risco a efetividade do projeto é a falta de transparência com relação aos algoritmos e inteligências artificiais. Afinal, o modo como os algoritmos funcionam é conhecido como uma *black box* justamente porque nem o próprio programador do algoritmo pode perceber a razão pela qual o algoritmo ter chegado a um resultado específico, em virtude de questões de programação e de interface do utilizador (FERREIRA, 2018). Desse modo, a eventual supervisão do funcionamento dos algoritmos pode não ser suficientemente eficaz.

Assim, o que coloca em risco o sucesso de uma eventual regulação é o fato de que os algoritmos têm direcionado o fluxo informacional muitas vezes sem que nem mesmo as plataformas responsáveis por eles entendam o que está acontecendo (FRAZÃO, 2018a).

Nesse passo, é também questionável se uma regulação de proteção de dados pode ser realmente eficiente se em grande parte das situações não se tem consciência de como é feita a extração dos dados e para quais finalidades (FRAZÃO et al., 2022 p. 9). Sem transparência quanto ao tratamento dos dados pessoais e critérios utilizados para tanto, é difícil que haja efetivo controle sobre a aplicação dos algoritmos por parte do direito (FRAZÃO, 2018a, p. 22).

Outro desafio para se regular tal matéria é encontrar soluções que protejam os usuários, mas ao mesmo tempo, estimulem a inovação. Há, ainda, o risco de se deixar ser seduzido por uma lógica ardilosa por meio do qual se mantém um determinismo tecnológico, o qual frequentemente apenas mascara o determinismo econômico (FRAZÃO, 2018a, p. 22).

Apesar dos desafios, faz-se necessária uma legislação mais robusta a fim de se definir aqueles aspectos desconhecidos, mas que podem e devem ser conhecidos, como a forma de coleta e de tratamento de dados, bem como a de classificação e filtragem conteúdos por meio das redes sociais, o que deve ser feito pelo Estado. Somente assim será possível superar a assimetria do *one way mirror* e equilibrar de

forma mais justa o jogo de forças atualmente existente, preservando os direitos individuais e a própria democracia (FRAZÃO, 2019b).

CONSIDERAÇÕES FINAIS

A modernidade trouxe consigo uma revolução tecnológica que ressignificou a forma com que vivem os indivíduos, desde o campo do entretenimento, até o do trabalho, do estudo e dos relacionamentos. Esse fenômeno trouxe consigo uma maior facilidade de obtenção de dados. Não por outro motivo, legislações específicas foram desenvolvidas visando a garantir o direito à privacidade e, na atualidade, a proteção de dados configura-se como uma disciplina global. No Brasil, a transição para um marco regulatório específico iniciou-se de forma tímida, ainda na década de 1980, com leis estaduais que versavam sobre o direito de acesso e retificação de dados pessoais e culminou, em 2019, com a aprovação da LGPD, que representou uma grande conquista para a proteção de dados pessoais.

Não obstante a evolução dos diplomas legais que visam à proteção dos dados pessoais, a sociedade na atualidade, cercada por redes sociais que utilizam de bancos de dados e algoritmos para coletar e processar cada vez mais informações de seus usuários, na maior parte das vezes sem qualquer transparência, é uma realidade alvo de preocupações, cujos arranjos de poder podem acarretar irreversíveis violações.

Isso porque, conforme abordado, na *data-driven economy,* a violação da privacidade tornou-se um negócio: ao passo em que se aumenta a coleta de dados dos usuários, o poder econômico, político e social dos agentes de tratamento de dados resta também aumentado. Nessa linha, é essencial que se compreenda o poderio econômico que emana dos dados pessoais para a compreensão do presente trabalho, que busca alertar sobretudo sobre a finalidade para a qual tais dados são empregados.

Assim, como exposto no presente trabalho, as redes sociais monitoram os seus usuários para extrair o máximo de informações possíveis, que, então, são empregadas para influenciar as mentes dos usuários valendo-se do conhecimento detalhado que possuem para manipulá-los em benefício de uma ampla variedade de interesses, sejam econômicos, políticos ou sociais.

Buscou-se, desse modo, exemplificar situações nas quais é possível constatar que a manipulação, possibilitada muitas vezes pela invasão constante da privacidade,

proporciona oportunidades lucrativas aos agentes econômicos. Os dados dos indivíduos podem ser empregados em campanhas publicitárias ou mesmo para influenciar as eleições em favor de determinados candidatos.

Assim, os indivíduos têm acesso a um conteúdo selecionado e muitas vezes personalizado a partir de seus dados, o que permite às companhias e aos agentes econômicos a adoção de estratégias cada vez mais persuasivas para moldar consciências e atingir seus interesses ocultos. O resultado desse controle informacional é uma "bolha" de conteúdo, que compromete o pensamento crítico, a criatividade e representa riscos à autonomia, à liberdade e à própria ordem democrática.

É possível concluir, a partir disso, que o principal objetivo do estudo foi alcançado ao passo em que restou confirmada a hipótese de que, de fato, o livre-arbítrio, em uma sociedade na qual os indivíduos recorrem às redes sociais de forma cotidiana, é, por vezes, uma mera ilusão.

Ou seja, embora o tema abordado envolva e tenha como ponto de partida violação da privacidade, a principal problemática a qual buscou-se trazer à luz é como e por que o livre arbítrio resta comprometido diante do contexto da *data-driven economy*.

O presente trabalho buscou, ainda, analisar o ordenamento jurídico brasileiro à luz das violações abordadas e aferir de que forma as normas vigentes dialogam com essa problemática. A conclusão obtida foi de que as normas vigentes mostram-se insuficientes para se evitar tanto a violação à privacidade, decorrente da coleta de dados dos usuários de forma indevida, quanto a violação à liberdade, que resulta do controle informacional destinado a satisfazer interesses econômicos ou políticos.

Ao analisar o Marco Civil da Internet, o presente trabalho constatou que essa lei carece de precisão nas disposições sobre a privacidade e não se presta a responsabilizar as plataformas digitais pela forma de impulsionamento de conteúdos, mas tão somente por conteúdos veiculados por terceiros na hipótese de descumprimento de ordem judicial para retirá-las.

O Código Civil, por sua vez, não se mostra adequado para que, a partir de suas previsões, se estipule uma forma de reparação para as violações de direitos ora tratados, na medida em que: (i) é imprescindível a demonstração de nexo causal, e, tratando-se de manipulações de consciências, é complicado – para não dizer impossível – demonstrar que houve uma mudança de percepção ocasionada por

determinados conteúdos exibidos; e (ii) o intuito da reparação é justamente o retorno ao *status quo ante*, sendo incompatível com danos causados às consciências.

Por fim, quanto às previsões da LGPD, o presente trabalho constatou que: (i) há dificuldade de compatibilização entre os princípios previstos e a atuação dos algoritmos, eis que desprovida de qualquer transparência; (ii) excetua-se da necessidade de transparência as informações consideradas como segredo comercial ou industrial, podendo servir de amparo para que os algoritmos não se submetam à regra; (iii) quanto às bases de tratamento de dados pessoais, o legítimo interesse pode ser justificado pelo lucro, que é justamente um dos interesses ocultos que move os algoritmos e as violações exploradas pelo presente trabalho; e (iv) o livre consentimento prescinde que o indivíduo esteja informado sobre a forma e a finalidade do tratamento de seus dados, mas, por meio dos algoritmos, isso não é possível.

Nota-se que, diante das conclusões obtidas, faz-se necessário o alerta a respeito da possibilidade de manipulação dos usuários, daí a importância do presente trabalho. Tal alerta deve servir como incentivo à reflexão crítica acerca dos conteúdos veiculados nas redes sociais, para o fim de buscar ampliar a autonomia dos cidadãos e não fazê-los subjugados, bem como de se aferir quais são os agentes responsáveis por empregar tecnologias capazes de manipular e entender os interesses ou valores ocultos aos quais essa tecnologia serve.

O Tópico 3.4 do presente trabalho abordar as iniciativas legislativas ora existentes. Foram analisadas as disposições do “PL das Fake News”, constatando-se que suas disposições não impedem integralmente a ocorrência de violações ao livre-arbítrio, mas revelam-se extremamente relevantes ao passo em que conferem maior transparência ao impulsionamento de conteúdos publicitários. Foi analisado também o Projeto de Lei nº 21/2020, que visa a regular o uso da inteligência artificial, constatando-se que suas disposições mostram-se vagas.

Por fim, se alertou sobre a necessidade de uma legislação mais robusta para coibir as violações ora abordadas, notadamente, a violação ao livre-arbítrio.

Referências Bibliográficas

ACEMOGLU, Daron. Harms of AI. Working Paper 29247, Cambridge, set. 2021. Disponível em: http://www.nber.org/papers/w29247.Acesso em: 15 jun. 2023.

ALGORIMOS do Twitter favorecem conteúdos políticos de direita. Tecnomundo, 22 out. 2021. Disponível em: https://www.tecmundo.com.br/redes-sociais/227437-algoritmos-twitter-favorecem-conteudos-politicos-direita.htm. Acesso em: 14 de junho de 2023.

AMATO, Lucas Fucci. Fake news: regulação ou metarregulação? Revista de Informação Legislativa: RIL, Brasília, DF, v. 58, n. 230, p. 29-53, abr./jun. 2021. Disponível em: https://www12.senado.leg.br/ril/edicoes/58/230/ril_v58_n230_p29. Acesso em: 29 jun. 2023.

ANDRION, Rosell. Pesquisa aponta: sete em cada dez brasileiros se informam pelas redes sociais. Olhar Digital. Disponível em: https://olhardigital.com.br/2019/02/01/noticias/pesquisa-aponta-sete-em-cada-dez-brasileiros-se-informam-pelas-redes-sociais/. Acesso em: 31 jun. 2023.

AZEVEDO, Rodrigo Ghiringhelli. Resenha: A Era da Informação: Economia, Sociedade e Cultura. Vol. 2 - O Poder da Identidade. Sociologias, Porto Alegre, v. 1, n. 2, p. 304-313, jul./dez. 2008. Disponível em: https://seer.ufrgs.br/index.php/sociologias/article/view/6936. Acesso em: 6 maio. 2023.

BALKIN, Jack; ZITTRAIN, Jonathan. A Grand Bargain to Make Tech Companies Trustworthy, The Atlantic, out. 2016. Disponível em: https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/. Acesso em: 15 jun. 2023.

BARGLOW, Raymond. **The Crisis of the Self in the Age of Information: Computers, Dolphins and Dreams.** New York: Routledge, 1994.

BEVIER, Lillian R. Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection. **William & Mary Bill of Rights Journal**, Williamsburg, v. 4, n. 2, p. 455-506, fev. 1995. Disponível em: https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1489&context=wmborj. Acesso em: 10 jun. 2023.

BRASIL. Constituição da República Federativa do Brasil de 1988. Planalto. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 14 jun. 2023.

BRASIL. Lei nº 8.078. 11 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 14 jun. 2023.

BRASIL. Lei nº 10.406. 10 de janeiro de 2002. Disponível em https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 14 jun. 2023.

BRASIL. Lei nº 12.965. 23 de abril de 2014. Planalto. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 jun. 2023.

BRASIL. Lei nº 13.709. 14 de agosto de 2018. Planalto. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2023.

BRASIL. Projeto de Lei n° 2.630/20. Câmara Legislativa. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2263075&filename=PL%202120/2023. Acesso em: 21 jun. 2023.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 22.337/RS. SERVIÇO DE PROTEÇÃO AO CRÉDITO. Cancelamento do registro. Prazo (cinco anos). O registro de dados pessoais no SPC deve ser cancelado após cinco anos. Art. 43, §1º, do Código de Defesa do Consumidor (Lei 8.078/90). Quarta Turma. Relator: Ministro Ruy Rosado de Aguiar. Julgado em 13 de fevereiro de 1995. *Diário de Justiça Eletrônico*. Brasília, 20 mar. 1995.

BORGES, Gabriel Oliveira de Aguiar; LONGHI, João Victor Rozatti; MARTINS, Guilherme Magalhães. Comentários acerca de alguns pontos do projeto da lei das fake news sob a ótica da responsabilidade civil. **Revista IBERC**, v. 4, n. 1, p. 35-51, jan./abr. 2021. Disponível em: https://revistaiberc.emnuvens.com.br/iberc/article/view/141/120. Acesso em: 27 jun. 2023.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. **Revista de Direito do Consumidor**, São Paulo, v. 46, p. 77–119, abr./jun., 2003.

CASTELLS, Manuel. **A era da informação: economia, sociedade e cultura, Vol 1: A sociedade em rede.** Trad: Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999a. 6ª edição, p. 58-59. Disponível em: http://www.fafich.ufmg.br/ppgs/wp-content/uploads/2020/09/1-CASTELLS-Manuel.-Pr%C3%B3logo_-a-rede-e-o-ser...-pp-39-a-66_compressed.pdf. Acesso em: 16 jun. 2023.

CASTELLS, Manuel. **A Era da Informação: Economia, Sociedade e Cultura Vol. 2: O Poder da Identidade.** São Paulo: Ed. Paz e Terra, 1999.

CASTRO, Bruno Martins Thorpe. Redes sociais e LGPD: a influência no modelo de negócio. Consultor Jurídico, out. 2020. Disponível em: https://www.conjur.com.br/2020-out-02/bruno-castro-redes-sociais-lgpd. Acesso em: 15 jun. 2023.

COALIZÃO DIREITOS NA REDE. Órgão independente de supervisão das plataformas é essencial, mas não pode ser Anatel: A agência deve priorizar sua competência no

setor de telecomunicações, que necessita de aprimoramentos e não se confunde com a regulação das plataformas. 28 de abril de 2023. Disponível em: https://www.telesintese.com.br/wp-content/uploads/2023/04/CDR-Nota-sobre-Anatel-como-orgao-regulador.pdf. Acesso em: 15 jun. 2023.

COHEN, David. Mark Zuckerberg Seeks Forgiveness in Yom Kippur Facebook Post. Adweek, 2 de outubro de 2017. Disponível em: https://www.adweek.com/performance-marketing/mark-zuckerberg-yom-kippur-facebook-post/#:~:text=Zuckerberg%20indirectly%20referenced%20Facebook%20in,will%20try%20to%20be%20better. Acesso em: 14 de junho de 2023.

COHEN, Julie E. Examined Lives: Informational Privacy and the Subject as Object. **Stanford Law Review**, v. 52, 2000, p. 1373-1438. Disponível em: https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub. Acesso em: 13 de junho de 2022.

CRETELLA JR., José. **O Estado e a Obrigação de Indenizar.** São Paulo: Saraiva, 1980.

DE PLACIDO E SILVA, Oscar Joseph. **Vocabulário Jurídico**. 18. ed. Rio de Janeiro: Forense, 2001, p. 639.

DOLAN, Edwin G. **TANSTAAFL: The Economic Strategy for Environmental Crisis.** New York: Holt, Rinehart, and Winston, 1971.

DOMO, Data Never Sleeps 10.0. Disponível em: https://www.domo.com/data-never-sleeps. Acesso em: 16 jun. 2023.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo. A Tutela da Privacidade no Código Civil de 2002. **Anima Revista Eletrônica**, 1ª ed. Vol I., 2009, p. 89-100.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coords). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Editora Forense, 2021. p. 3-20.

ENGEL, Christoph; KELLER, Keller H. **Governance of Global Networks in the Light of Differing Local Values.** Baden-Beden: Nomos, 2000.

FERREIRA, Afonso José. Profiling e algoritmos autónomos: um verdadeiro direito de não sujeição? In: PEREIRA COUTINHO, Francisco; MONIZ, Graça Canto (coord). Anuário da Proteção de Dados 2018. Lisboa: CEDIS, 2018, p. 35-43. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/Anuario_da_Protecao_de_Dados_2018-1-1.pdf. Acesso em: 15 jun. 2023.

FRAZÃO, Ana. A indústria dos dados pessoais e os data brokers. Reflexões sobre os riscos da atuação de tais agentes no mercado de dados pessoais. Jota, mar. 2019a. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/a-industria-dos-dados-pessoais-e-os-data-brokers-20032019. Acesso em: 27 maio 2023.

FRAZÃO, Ana. A falácia da soberania do consumidor: Economia digital pode tornar o consumidor ainda mais vulnerável, dez. 2021b. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/falacia-soberania-do-consumidor-08122021#_ftn12. Acesso em: 15 jun. 2023.

FRAZÃO, Ana; CARVALHO, Angelo Prata; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais: Fundamentos da LGPD**. Rio de Janeiro: Editora Forense, 2022.

FRAZÃO, Ana. Capitalismo de vigilância e black box society. Jota, fev. 2019b. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/capitalismo-de-vigilancia-e-black-box-society-28022019. Acesso em: 15 jun. 2023.

FRAZÃO, Ana. Dever geral de cuidado das plataformas diante de crianças e adolescentes. Publicação encomendada pelo programa Criança e Consumo, do Instituto Alana. São Paulo, nov. 2021a. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2021/11/dever-geral-de-cuidado-das-plataformas.pdf. Acesso em: 26 maio 2023.

FRAZÃO, Ana. Fundamentos dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords). **Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro** [edição eletrônica]. São Paulo: Revista dos Tribunais, 2019c, p. 25-63.

FRAZÃO, Ana. Nova LGPD: a importância do consentimento para o tratamento dos dados pessoais. Jota, set. 2018c. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018. Acesso em: 3 jun. 2023.

FRAZÃO, Ana. Nova LGPD: principais repercussões para a atividade empresarial, Jota, ago. 2018b. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018. Acesso em: 11 jun. 2023.

FRAZÃO, Ana. Prefácio. In: FERNANDES, Ricardo Vieira de Carvalho; COSTA, Henrique Araújo; CARVALHO, Angelo Gamba Prata (coords). **Tecnologia Jurídica e Direito Digital.** Belo Horizonte: Fórum, 2018a.

FRAZÃO, Ana. Regulação de conteúdos em plataformas digitais. Jota, mar. 2023. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-

e-mercado/regulacao-de-conteudos-em-plataformas-digitais-22032023. Acesso em: 15 jun. 2023.

FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio. **A Lei Geral de Proteção de Dados Pessoais: Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado.** São Paulo: Thomson Reuters, 2021.

GÜNTHER, Wendy Arianne; MEHRIZI, Mohammad H.; FELDBERG, Marleen Huyman Frans.Debating big data: A literature review on realizing value from big data. **Sciencedirect**. Volume 26, Issue 3, September 2017, Pages 191-209. Disponível em: https://www.sciencedirect.com/science/article/pii/S0963868717302615. Acesso em: 27 maio 2023.

HOOFNAGLE, Chris Jay; SOLTANI, Ashkan; GOOD, Nathaniel; WANBACH, Dietrich J. Behavioral advertising: the offer you can`t refuse. Harvard Law & Policy Review, v. 6, p. 273-296, 2012. Disponível em https://harvardlpr.com/wp-content/uploads/sites/20/2013/06/Behavioral-Advertising-Hoofnagle-et-al.pdf . Acesso em: 30 maio 2022.

LORENZETTI, Ricardo L. **Comércio Eletrônico**. São Paulo: Revista dos Tribunais, 2004, p. 90.

MACEDO, Luis. Projeto atribui à Anatel regulação das plataformas digitais em operação no Brasil. Agência Câmara de Notícias. Brasília, jan. 2023. Disponível em: https://www.camara.leg.br/noticias/927967-PROJETO-ATRIBUI-A-ANATEL-REGULACAO-DAS-PLATAFORMAS-DIGITAIS-EM-OPERACAO-NO-BRASIL. Acesso em: 15 jun. 2023.

MANZANO, José Augusto NG; OLIVEIRA, Jayr Figueiredo. **Algoritmos: lógica para desenvolvimento de programação de computadores.** São Paulo: Saraiva Educação, 2000.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. **A prova do nexo de causalidade na responsabilidade civil.** 1ª ed. em e-book. São Paulo: Editora Revista dos Tribunais Ltda, 2016.

MARQUES, Claudia Lima. **Confiança no comércio eletrônico e a proteção do consumidor.** São Paulo: Revista dos Tribunais, 2004.

MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na internet.** 3ª edição. São Paulo: Revista dos Tribunais, 2020.

MASUR, Philipp; REINICKE, Leonard; ZIEGELE, Marc. The interplay of intrinsic need satisfaction and Facebook specific motives in explaining addictive behavior on Facebook. ScienceDirect, v. 39, out. 2014, pp. 376-386. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0747563214003343. Acesso em: 14 jun. 2023.

MENDES, Laura Schertel. Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo. Brasília: Universidade de Brasília,

2008. Disponível em: https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf Acesso em: 15 jun. 2023.

MILANEZ, Giovanna. **O tratamento de dados pessoais disponíveis publicamente e os limites impostos pela LGPD**. Rio de Janeiro: Editora Processo, 2022.

MORAES, Alexandre de. **Direito Constitucional.** São Paulo: Editora Atlas S.A., 2003. 13ª ed.

MIRANDA, Sandra; TRIGO, Inês; RODRIGUES, Ricardo; DUARTE, Margarida. Addiction to social networking sites: Motivations, flow, and sense of belonging at the root of addiction. ScienceDirect, v. 188, mar. 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S0040162522008010 Acesso em: 14 jun. 2023.

MOTRONI, Raimondo. Gli scambi "a titolo gratuito" nelle reti telematiche. In: Ricciuto, Vincenzo; Zorzi , Nadia. Il contratto telemático. Padova: Cedam, 2002.

MUSSARAT, R., Ahmed, S., Munir, F., Riaz, S., Hayat, N. Digital narcissism, self-esteem and self-objectification among Snapchat vs Facebook users. Journal of Positive School Psychology. v. 6. n. 9, 2022, pp. 3128-3141 Disponível em: https://journalppw.com/index.php/jpsp/article/view/12814/8305. Acesso em: 14 jun. 2023.

O Dilema das Redes. Direção: Jeff Orlowski. Produção: Netflix. Estados Unidos: Netflix, 2020 (94 min).

OLIVEIRA, Amanda Flávio de. O mito do regulador infalível. Brasília: Editora WebAdvocacy, 2021, n.3, p. 1. Disponível em: <https://webadvocacy.com.br/wp-content/uploads/2021/05/O-mito-do-regulador-infalivel.pdf> Acesso em: 26 maio 2023.

OLIVEIRA, Ricardo; COTS, Márcio. **O Legítimo Interesse e a LGPDP**. São Paulo: Thomson Reuters, 2021.

ORGAZ, Cristina J. 'TikTok foi feito para ser viciante': o homem que investigou as entranhas do aplicativo. BBC News Brasil, 3 dez. 2020. Disponível em: https://www.bbc.com/portuguese/geral-55173900. Acesso em: 14 jun. 2023.

PASQUALE, Frank. **The black box society. The secret algorithms that control money and information.** Cambridge: Harvard University Press, 2015. Disponível em: https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf. Acesso em: 20 maio 2022.

RAMIRO, André. A proteção de dados pessoais no Brasil e no Chile: uma análise comparativa sob a perspectiva da decisão de adequação da comissão europeia. . Observatório LGPD, 2020. Disponível em: https://observatoriolgpd.com/wp-content/uploads/2020/02/Protecao-de-dados-pessoais-no-Brasil-e-no-Chile.pdf. Acesso em: 27 jun. 2023.

RICHARDSON, Neil. **Why privacy matters**. Oxford: Oxford University Press, 2021.

RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008. p.15.

RODOTÀ, Stefano. **Tecnologie e diritti**. Bologna: Il Mulino, 1995. p. 19-20

RODRIGUES, Marlo Gonçalves. Algoritmos de Mal-Estar: Ciberpandemia e Privacidade Hackeada. **Revista de Filosofia Moderna e Contemporânea**, Brasília, v. 8, n. 3, p. 105-136, dez. 2020. Disponível em: https://periodicos.unb.br/index.php/fmc/issue/view/2176/545. Acesso em: 15 jun. 2023.

SANSEVERINO, Paulo de Tarso Vieira. **Princípio da reparação integral.** São Paulo: Saraiva, 2010.

SILVA, Evelyn Melo. Pela proteção dos neurodireitos no Brasil. Consultor Jurídico, agosto, 2022. Disponível em: https://www.conjur.com.br/2022-ago-29/evelyn-silva-protecao-neurodireitos. Acesso em: 29 jun. 2023.

SILVEIRA, Sérgio Amadeu . **Democracia e os códigos invisíveis: como os algoritmos estão modulando comportamentos e escolhas políticas.** 1. ed. São Paulo: Edições SESC-SP, 2019. v. 1. e-book.

SHARE LAB. The Human Fabric of the Facebook Pyramid. Maio, 2017. Disponível em: https://labs.rs/en/the-human-fabric-of-the-facebook-pyramid/. Acesso em: 15 jun. 2023.

SOLOVE, Daniel J. Introduction: privacy self-management and the consent dilemma. **Harvard Law Review**, Cambridge, v. 126, p. 1.880-1.903, 2013.

SOLOVE, Daniel J. A taxonomy of privacy. **University of Pennsylvania Law Review**, Philadelphia, v. 154, n. 3, p. 477-564, jan. 2006.

SUNDFELD, Carlos Ari. **Direito Administrativo para Céticos.** 2 ed. São Paulo: Malheiros Editores, p. 60-84, 2017.

SUZOR, Nicolas. Digital constitutionalism: Using the rule of law to evaluate the legitimacy of governance by platforms. **Social Media+Society**, v. 4, n. 3, jul/set 2018. Disponível em: https://journals.sagepub.com/doi/10.1177/2056305118787812. Acesso em: 15 jun. 2023.

STOCO, Rui. **Tratado de Responsabilidade Civil.** 2 ed. em e-book. São Paulo: Revista dos Tribunais, 2015.

TEFFÉ, Chiara Antonia Spadaccini. A responsabilidade civil do provedor de aplicação de internet pelos danos decorrentes do conteúdo gerado por terceiros, de acordo com o Marco Civil da Internet. **Revista Fórum de Direito Civil** - RFDC, Belo Horizonte, v.

4, n. 10, set./dez. 2015. Disponível em https://www.editoraforum.com.br/wp-content/uploads/2015/12/A-responsabilidade-civil-do-provedor-de-aplicacoes-de-internet.pdf. Acesso em: 13 jun. 2023.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados (Online)** , v. 30, p. 269-285, 2016. Disponível em https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/. Acesso em: 10 jun. 2023.

TOSI, Emilio. Le responsabilità civili. In: **I problemi giuridici di Internet**. Milano: Giuffrè, 1999. p. 270-271.

UNESCO. Guidelines for regulating digital platforms: a multistakeholder approach to safeguarding freedom of expression and access to information. Internet for Trust - Towards Guidelines for Regulating Digital Platforms for Information as a Public Good, Paris, [2023]. Disponível em: https://bityli.com/JQV14. Acesso em: 4 maio 2023.

VÉLIZ, Carissa. **Privacy is power: why and how you should take back control of your data.** Londres: Bantam Press, 2020.

VENTURINI, Julia; LOUZADA, Luiza; MACIEL, Marília; ZINGALES, Nicolo; STYLIANOU, Konstantinos; BELLI, Luca. **Terms of service and human rights: An analysis of online platform contracts**. Rio de Janeiro: Editora Revan, 2016. Disponível em https://internet-governance.fgv.br/sites/internet-governance.fgv.br/files/publicacoes/terms_of_services_06_12_2016.pdf. Acesso em: 17 maio 2023.

WOLTERS, Heather ; STRICKLIN, Kasey; CAREY, Neil; MCBRIDE, Megan. The Psychology of (Dis)information: A Primer on Key Psychological Mechanisms. CNA, set. 2021. Disponível em: https://www.cna.org/reports/2021/10/The%20Psychology-of-%28Dis%29information-A-Primer-on-Key-Psychological-Mechanisms.pdf. Acesso em: 10 jun. 2023.

WESTIN, Alan. **Privacy and Freedom.** Nova York: Atheneum, 1970.

WU, Tim. **The attention merchants: the epic scramble to get inside our heads.** New York: Knopf, 2016.

YANG, Yuxin. Understanding Young Adults' TikTok Usage: Real People, Creative Videos That Make Your Day Understanding. University of California, 2020. Disponível em: https://communication.ucsd.edu/_files/undergrad/yang-yuxin-understanding-young-adults-tiktok-usage.pdf. Acesso em: 14 jun. 2023.

YOUTUBE recomenda mais vídeos pró-Bolsonaro, diz estudo. Folha de São Paulo, set. 2022. Disponível em: https://www1.folha.uol.com.br/poder/2022/09/youtube-privilegia-videos-pro-bolsonaro-em-recomendacoes-a-usuarios-diz-estudo.shtml. Acesso em: 28 maio 2023.

ZAHRA, Muniba Fatima; QAZI, Tehmina Ashfaq; ALI, Ashbeelah Shafaqat; HAYAT, Noor; HASSAN, Taimoor Ul. How Tiktok Addiction Leads To Mental Health Illness?

Examining The Mediating Role Of Academic Performance Using Structural Equation Modeling. **Journal of Positive School Psychology**, vol. 6, n. 10, p. 1490-1502, 2022. Disponível em https://journalppw.com/index.php/jpsp/article/view/13392/8693. Acesso em: 27 maio 2023.

ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do right to privacy nos Estados Unidos. **Revista de Doutrina da 4ª Região**, Porto Alegre, n. 64, fev. 2015.

ZHANG, Xing; WU, You; LIU, Shan. Exploring short-form video application addiction: Socio-technical and attachment perspectives. **ScienceDirect**, v. 42, set. 2019. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0736585319303302. Acesso em: 14 jun. 2023.

ZIADY, Hanna. Europa lidera corrida para regulamentar a inteligência artificial; entenda como. CNN Brasil: Londres, jun. 2023. Disponível em: https://www.cnnbrasil.com.br/tecnologia/europa-lidera-corrida-para-regulamentar-a-inteligencia-artificial-entenda-como/. Acesso em: 30 jun. 2023.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder.** São Paulo: Intrínseca, 2021.